Crypto News

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

December 01, 2023

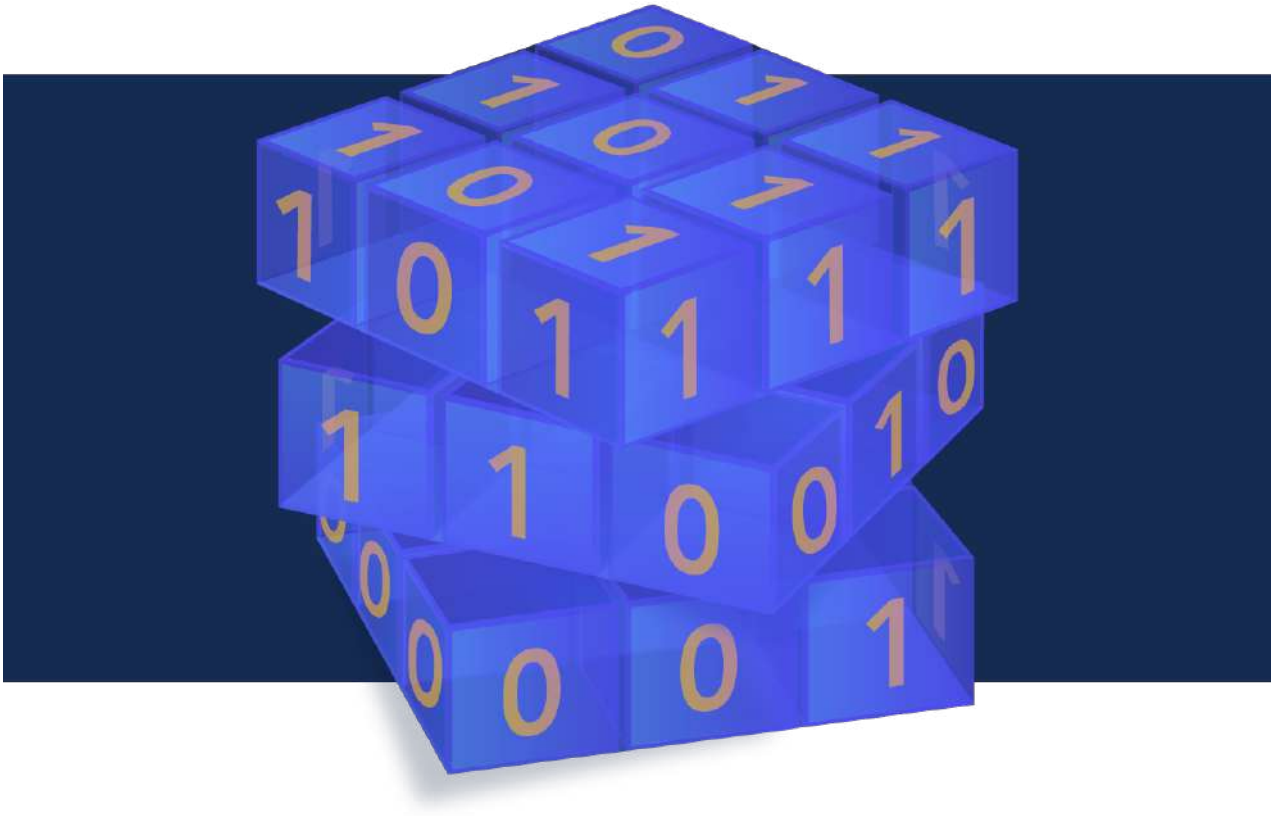


TABLE OF CONTENTS

Editorial

Let's start this edition by talking about two of our most impactful emerging technologies; Quantum Computing and AI. Quantum Computing and AI will, and already have, started to change the way we do things. Suffice to say, when two emerging technologies come together, there is an even greater impact. How will Quantum Computing and AI impact each other? One of the main impacts will be the use of Quantum Computers to exponentially expedite the "learning" step for AI which typically is the longest step. After that, AI running on a Quantum Computer will be able to learn new information almost instantly and process new inputs faster as well. That is, once we inevitably reach a quantum advantage (which is well on its way). For both Quantum Computers and AI to function effectively, cybersecurity is key. Though both technologies are a threat to cybersecurity, they themselves are vulnerable to it as well. Federal agencies including the NSA, NCSC-UK, US CISA, and others have come together to release guidance for AI security. To learn more about what they're saying, make your way to article 6.

If you work in the world of banking and/or finance, articles 18 and 21 will be of interest to you and your clients. Though the warnings about a Cryptographically Relevant Quantum Computer (CRQC) are not new to the industry, there is urgency for closer collaboration between the banking industry and the UK government. Article 18 walks through the specifics. It's not all doom and gloom though. Article 21 talks about the advantages of "Quantum Banking" which will increase the speed of banking. Navigate to the article to learn more about Quantum Banking along with other Quantum Computing use cases relevant to the banking industry.

Make sure to peruse the entire newsletter since it will definitely get your neurons firing! Happy reading and Happy Holidays! We'll see you in the new year!

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-CCP 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.Singtel tapped to build first quantum-safe network in Southeast Asia

by Gigi Onag
https://www.lightreading.com/network-technology/singtel-tapped-to-build-first-quantum-safe-network-in-southeast-asia

Singtel said today that it will develop Singapore's first National Quantum-Safe Network Plus (NQSN+) for enterprises in partnership with Geneva-based ID Quantique (IDQ).

Singaporean regulator IMDA appointed Singtel to build the network as part of the Digital Connectivity Blueprint, which outlines holistic plans for continuous enhancement of the city's digital infrastructure up to 2030.

"We are excited to kickstart the launch of Southeast Asia's first quantum-safe network infrastructure to help both businesses and government agencies tap on quantum-safe technologies. NQSN+ will help to realize Singapore's vision of a quantum-safe nation, building our nation's capabilities in this space," said Dr. Ong Chen Hui, assistant chief executive, BizTech Group, IMDA.

The network will employ modern quantum-safe technologies such as quantum key distribution, which is a secure method for distributing encryption keys only known between shared parties, and post-quantum cryptography, a new, advanced form of encryption algorithms that are secure against attacks from quantum computers.

''We are laying the foundation for becoming a regional hub for quantum computing as well as a launch-pad for new leading-edge innovations and applications," said Ng Tian Chong, chief executive officer, Singtel.

He added: "With Singtel's nationwide quantum-safe network for enterprises, we are securing our data networks from advanced quantum threats for our customers and giving them easy access to solutions to safeguard their critical data in the quantum age."

Launch expected next year

Singtel expects to launch the NQSN+ network in mid-2024.

The NQSN+ will incorporate Quantum Key Distribution and Quantum-Safe Key Management solutions from IDQ into Singtel's network and co-develop a bigger talent pool with deep expertise in design, solutions, engineering and operations of Quantum-Safe Networks.

The Quantum-Safe Network will leverage Singtel's managed network services and fiber network with selected exchanges stipulated as trusted nodes to establish a reliable, secure and resilient nationwide quantum key distribution network. This enables companies to secure their communications across the island and extends quantum-safe security to new use cases and applications such as identity, mobility and authentication.

"With quantum computing gaining traction and potentially used as a threat vector by malicious actors to attack classical (traditional) encryption, it is imperative that organizations update their assets to safeguard their information and boost their cyber resilience," said Ng.

2.Alibaba Shuts Down its Quantum Computing Effort

by John Russell
https://www.hpcwire.com/2023/11/30/alibaba-shuts-down-its-quantum-computing-effort/

In case you missed it, China's e-commerce giant Alibaba has shut down its quantum computing research effort. It's not entirely clear what drove the change. Reuters' reported earlier this week that Alibaba "cut a quantum computing laboratory and team from its research arm, donating both the lab and related experimental equipment to Zhejiang University."

Alibaba was a relatively early entrant among giant e-commerce/cloud providers into quantum computing research, placing the effort in its Alibaba's DAMO Academy research organization. There are reports it had invested on the order of $15 billion in the effort. According to the Reuters report, about 30 employees are being released with and effort under way to find positions for them at Zhejiang.

Rather than being tied to specific issues with the quantum research, the prevailing opinion seems to be that the quantum work was caught in the larger turmoil surrounding Alibaba and its ongoing reorganization. The company said its DAMO organization will deepen its work on AI and machining learning research which may be able to have a nearer-term impact on Alibaba's business.

Macro concerns, including recent U.S. semiconductor export restrictions, are also a likely factor. The Wall Street Journal reported earlier this month that Alibaba scrapped plans "to spin off and list its cloud-computing division, citing the impact of the export controls that took effect late last month. The restrictions "may materially and adversely affect" the cloud business's ability to offer products and services and to perform under existing contracts, Alibaba said, adding that it would focus on the division's growth."

It may be the quantum effort was seen as not likely to have a business impact soon enough while Alibaba sorts through core business issues and reorganization. Meanwhile, the big U.S.-based cloud providers – AWS, Azure, and Google – continue forging ahead with the quantum computing plans.

3.U.K. Conference Accelerates Post-Quantum Cryptography Standards Review Process

by Robert Huntley
https://www.eetimes.eu/u-k-conference-accelerates-post-quantum-cryptography-standards-review-process/

Industry readiness for post-quantum cryptography (PQC) took an important step forward in late summer when the U.S. National Institute of Standards and Technology (NIST) published three quantum-safe draft standards for public review. The University of Oxford's Mathematical Institute recently hosted the second Oxford Post Quantum Cryptography Summit to review and provide timely feedback on the published draft standards.

EE Times Europe spoke with three post-quantum cryptography experts at the conference to gain insight into the new standards and their potential impact on the development of embedded systems.

NIST's draft standards, covering quantum-secure public key encryption and digital signature algorithms, are FIPS 203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard), FIPS 204 (Module-Lattice-Based Digital Signature Standard) and FIPS 205 (Stateless Hash-Based Digital Signature Standard). More than 100 people from the international cryptographic community, representing the foremost post-quantum cryptography experts from universities, technology organizations and governments worldwide, attended the Oxford conference. Through a series of conference streams and workshops, delegates looked closely at the proposed standards with the aim of accelerating the standardization process through a collaborative technical review.

Adopting Arm Cortex-M4 as a PQC reference platform

While much work has gone into offering up post-quantum algorithm candidates and the four selection rounds, embedded developers may wonder whether the proposed options will be suitable for running on resource-constrained microcontrollers.

Peter Schwabe, research group leader of the Max Planck Institute for Security and Privacy (Bochum, Germany), addressed this issue when speaking with EE Times Europe about his work on recent post-quantum security initiatives.

"I've been involved in the PQC process as a co-author of seven proposals, and of the four algorithms that have now been selected for standardization, I'm a co-author of three," Schwabe said. "I've also been conducting research within a project funded by the EU called EPOQUE, which stands for engineering post-quantum cryptography, of which there are two main parts: One is on protocol integration and the other on achieving an efficient and secure implementation on microcontrollers."

Schwabe cited a project he'd been involved with before the draft PQC standards were announced. "We started on PQM4, which presented a testing and benchmarking framework for the Arm Cortex-M4 using some of the initial post-quantum encapsulation and signature schemes," he said. "The idea was to get the algorithms working on the Cortex-M4 platform so we could optimize them and benchmark them in terms of speed and memory consumption. I believe that with this project, we had a bit of influence on the NIST PQC standardization process since NIST also decided to make the Cortex-M4 a reference platform for implementations. Clearly, the algorithms are somewhat bigger than [the current] elliptic-curve cryptography [ECC] methods, but it's not that much slower."

Schwabe said that the computational speed depends on which platform you are looking at, but the new lattice-based cryptographic standards, such as Kyber, are about as fast as ECC and are not going to be a concern speedwise as long as they're in the ballpark. "If your design can afford ECC, then you can afford Kyber," he said.

Draft standards eight years in the making

PQShield (Oxford, U.K.) has played a crucial role in proposing and collaborating with NIST on post-quantum cryptography standards. As company CEO Ali El Kaafarani recalled, "In 2015, I was hired by

the University of Oxford to lead the post-quantum cryptography project. That was when it all started, and it was the same year that the NSA announced an international collaborative project to develop quantum-safe security algorithms. We quickly figured out with the stakeholders that this is not something that you can solve in an academic environment. It requires an industrial setting because it's related to standards, implementations, software, hardware and protocols. Mathematics is only one piece of that.

"The vision for PQShield is to have a safer world to live in, where everybody knows that every line of code they're writing and math problem they're solving has one purpose: to keep us all one step ahead of attackers," El Kaafarani added. "Perfect security does not exist, and every generation, every few years, a new tool will become available to attackers that they will use and leverage to break our cybersecurity methods."

While the challenge for the next 10 years is quantum computing, he said, it could well be something else in another 10 years. "It is quantum computing when it comes to the underlying mathematics of the security algorithms, but it's not quantum computing when it comes to side-channel resistance, for instance."

Keeping a watch on AI, machine learning

EE Times Europe asked El Kaafarani if there was anything on the far horizon that could require replacing post-quantum cryptography in the future. "The two things we see at the moment are quantum computing and AI," he said. "Quantum computing has a clear way to break existing algorithms, and we have a clear methodology to defend against it. However, AI still needs to be clarified [as to] what it can do, and this is something to keep an eye on. We need to use AI to our benefit to build more secure encryption methods and build better side-channel countermeasures."

PQShield has a team of cryptographic professionals engaged in playing the role of attackers, he said. "They're trying to attack our own post-quantum products with various methods. Post-quantum cryptography has been in an academic setting for decades now, but it hasn't been in an industrial environment for that time. There are many different industrial attack surfaces that adversaries can use, and that's how you can stay ahead of them—by building a group to do that work."

Side-channel attacks set to rise

It was clear from the discussions with El Kaafarani that there were real concerns over side-channel attacks. Coupling the power of AI to analyze vast amounts of data gathered from a side-channel attack method, such as differential power analysis, is something PQShield takes seriously, he said. "In terms of products, we also have the most advanced side-channel countermeasures that have been applied to our products and have been already licensed to customers."

EE Times Europe met PQShield's head of product innovation and security, Axel Poschmann, in his test lab in Oxford. Surrounded by a bank of embedded platforms, one of which was inside a Faraday cage, Poschmann explained the role of test vector leakage assessment (TVLA) methods in the test lab. He noted some of the countermeasures the researchers use to protect post-quantum cryptography products from side-channel attacks, such as masking.

"TVLA is widely recognized as a robust and reliable test methodology and is part of NIST FIPS 140-3 Security Certification requirements," Poschmann said. "At PQShield, we use it because it is very suitable for automation and easily integrated into our continuous integration and continuous deployment development environment. This allows us to run tests overnight and analyze them in the morning, enabling rapid improvement cycles that yield much more secure products."

Poschmann demonstrated a power analysis attack on an embedded system running a cryptographic algorithm without countermeasures (unmasked) and explained a screen-captured image: "The red line is the security assurance threshold set by the ISO 17825 standard, which NIST's FIPS 140-3 certification is

based on. This threshold is currently being raised, which PQShield has accounted for, but as the red line was exceeded in this test, the unmasked algorithm has failed."

4.Quantum Computing Is Coming Faster Than You Think

by Jim McGregor
https://www.forbes.com/sites/tiriasresearch/2023/11/28/quantum-computing-is-coming-faster-than-you-think/?sh=3405626c1d32

It seems for every proponent for quantum computing there is also a detractor. The detractors often refer to quantum computing as "a science project", "hype", "a hoax", even a "failed cause". If you look back through the history of the technology industry, it is littered with technologies that failed for various technical or business reasons. So, there is reason to be skeptical. However, there are just as many technologies that went on to chart the future direction of innovation because of major advancements that enabled the technology. Some have even had a similar level, if not more, of skepticism and of being "a science project" - technologies like artificial intelligence (AI). AI is a concept that had been theorized about long before the development of the first silicon transistor, but it wasn't until the past decade that it became a reality through advancements in silicon technology, processing architectures, and deep learning techniques. Similarly, quantum computing technology is real now and is on the verge of that breakout over the next decade.

Quantum Computing Is Not Easy

Even describing the concept of quantum computing is not easy. Classical computers use bits to represent a one (on state) or zero (off state), while quantum computers use qubits that can represent multiple states through superposition and links with other qubits through entanglement. The result is a computer that scales exponentially in terms of compute capacity. While this makes quantum computers ideally suited for large mathematical models, they are not suited for handling the simple overhead tasks associated with computing. As a result, quantum computing is better positioned as a new accelerator technology, similar to a Graphics Processing Unit (GPU), Digital Signal Processor (DSP), or Field-Programmable Gate Array (FPGA), but on a much larger scale in terms of computing performance. However, quantum computers require specialized control logic and memory because of the unique compute architecture on which quantum computing is based. Large refrigeration units are also required because they operate at near absolute zero, meaning zero degrees Kelvin or -273.15 degrees Celsius.

Quantum computing also faces two major challenges – accuracy and scaling. Errors are introduced through both the stability (or lack thereof) of qubits and potential interference from other qubits. Maintaining stability or lifespan of a qubit in a superposition state is challenging and may be limited to a few milliseconds or microseconds. Additionally, qubits can interfere with neighboring qubits. As a result, error suppression, correction, and mitigation techniques are being developed to work both individually and together to increase computation accuracy. Error suppression does front-end processing based on the knowledge of the system and circuits to offset potential errors, such as making alterations to the pulses that control the qubits. Error mitigation corrects errors in postprocessing based on a noise model. Error correction, on the other hand, requires many additional qubits, to correct errors during execution. While error correction may be the most effective way to eliminate errors, it comes at a significant cost. However, with error suppression and mitigation, quantum computing still allows for processing at a level that cannot be easily accomplished even on the largest classical supercomputers.

Scaling quantum computers is also a significant challenge. While there are several different quantum solutions, many do not use standard CMOS manufacturing processes, which means they do not scale with the advanced semiconductor processes used for other high-end processors or accelerators. Additionally, the entire system needs to scale with the number of qubits, which means more wires connecting each individual qubit to the control logic, plus the associated cooling elements. If you look at current quantum computers when they are not in a refrigerator, they look more like a jumble of tubes and wires than a silicon-based system. Scaling these systems is not an easy task.

Rapid Advances In Quantum Computing

If quantum computing is so fraught with challenges, the natural question is why do I think that we are on the cusp of major advances in quantum computing? One of the reasons is the level of investment in quantum computing. The benefits of having a single computer that can outperform many supercomputers is so valuable that the scientific community, technology industry, governments, and enterprises are investing billions into the development and use of quantum computing. This includes industry leaders like Alibaba, Amazon, IBM, Intel, Google, Honeywell, Microsoft, Nvidia, and Toshiba among many other companies. Likewise, the US Government has a National Quantum Initiative to "accelerate quantum research and development for the economic and national security of the United States." A key example of this investment is evident walking through the IBM quantum data center in Poughkeepsie, New York, which I had the opportunity to tour earlier this year.

Another reason is the continued advancements being made in quantum computing is improvements in quantum chips, control logic, systems, and software. These advancements are especially true of the development tools for error mitigation, suppression, and correction. As an example, IBM holds the lead in quantum scaling with the 433-qubit Osprey processor introduced in 2022 and is slated to introduce the 1121-qubit Condor processor later this year. If you consider IBM's quantum processor roadmap, the number of qubits will increase by approximately 2-3x every year. IBM is also networking quantum computers together to further increase the qubit capacity. IBM has stated that it has a goal of 100,000 qubit systems by 2033. Industry and academia are already working on practical applications with current quantum computers. This development will accelerate as qubit capacity increases in the latter half of this decade.

The final reason, and the one I believe will be critical to the next step in quantum computing, is artificial intelligence (AI). Thus far, the focus has been integrating classical computers with quantum computers. However, AI holds the potential to both improve the capabilities and performance of quantum computers and being improved by quantum computers but the work in this area is just beginning.

Quantum Timeline

When and how will quantum computing become available for practical applications? With thousands of universities, research organizations, and enterprises already learning and experimenting with quantum computing, the answer is *now*, for some limited applications. As published in the scientific journal Nature, IBM partnered with US Berkley to demonstrate the ability of quantum computers with just 127 qubits to outperform classical computers in material modeling. However, IBM believes that the 100k qubit capacity level will drive an inflection point for the industry. With quantum systems networked together, this threshold is rapidly approaching.

How the quantum computing industry will take shape is a little easier to predict. Because of the high investment in the supporting systems and infrastructure to support the systems, quantum computing is likely to be a cloud service provided by the leading hyperscalers and/or technology providers for the vast majority of the market – at least in the foreseeable future. There will be some university and enterprise installations, but these are likely to be few and far between.

The Quantum Era

Given the amount of quantum computing investment, advancements, and activity, the industry is set for a dynamic change, similar to that caused by AI – increased performance, functionality, and intelligence. This also comes with the same challenges presented by AI, such as security, as outlined in the recent Quantum Safe Cryptography article. But just like AI, quantum computing is coming. You might say that quantum computing is where AI was in 2015, fascinating but not widely utilized. Fast forward just five years and AI was being integrated into almost every platform and application. In just five years, quantum computing could take computing and humanity to a new level of knowledge and understanding.

5.Crypto Quantique partners with Blaitek enabling quantum secure chip-to-cloud connection

by Neil Tyler
https://www.newelectronics.co.uk/content/news/crypto-quantique-partners-with-blaitek-enabling-quantum-secure-chip-to-cloud-connection

This newly formed commercial alliance is set to leverage the advanced capabilities of Crypto Quantique's QuarkLink software, facilitating secure connectivity for businesses seeking to integrate IoT products and utilises Blaitek's WiFi technologies with cloud services.

The collaboration is intended to provide a streamlined approach for customers to seamlessly incorporate innovative features into their products and conduct secure over-the-air updates throughout the entire life cycle of their devices.

Notably, this is achieved without the need for substantial investment in engineering resources or acquiring in-depth knowledge of chip-to-cloud security.

Proactively anticipating the quantum computing era, Crypto Quantique is enhancing the resilience of QuarkLink through the integration of post-quantum cryptography. These quantum-resistant techniques are designed to ensure the sustained efficacy of security measures, even in the face of potential quantum-powered attacks.

In a landscape where over 20 countries worldwide are introducing stringent IoT security regulations, including the forthcoming EU Cyber Resilience Act, which mandates a baseline security level for compliance or risk financial penalties, Crypto Quantique's chip-to-cloud IoT security is being seen as an important solution.

It not only ensures compliance with evolving regulations but also mitigates risks across global supply chains.

6.Guidance for Securing AI Issued by NSA, NCSC-UK, CISA, and Partners

by NSA Media Relations
https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3598020/guidance-for-securing-ai-issued-by-nsa-ncsc-uk-cisa-and-partners/

The National Security Agency (NSA), UK National Cyber Security Centre (NCSC-UK), U.S Cybersecurity and Infrastructure Security Agency (CISA), and other partners have released "Guidelines for Secure AI System Development," a Cybersecurity Information Sheet (CSI).

The agencies are releasing the report to help developers, providers, and systems owners develop, deploy, and operate secure Artificial Intelligence (AI) systems, including those used in National Security Systems (NSS), by the Department of Defense (DoD), and by the Defense Industrial Base (DIB).

"We wish we could rewind time and bake security into the start of the internet. We have that opportunity today with AI. We need to seize the chance," said Rob Joyce, NSA Cybersecurity Director.

According to the CSI, AI systems are subject to security vulnerabilities that need to be considered alongside standard cyber threats. For example, AI systems are vulnerable to "adversarial machine learning" (AML) attacks, which exploit fundamental vulnerabilities in machine learning (ML) systems, including hardware, software, workflows, and supply chains. Prompt injection and training data poisoning are examples of AML attacks that could enable malicious cyber actors to compromise an ML model's classification or regression performance, perform unauthorized actions, or extract sensitive information.

The CSI indicates that secure by design principles are applicable to AI systems. Providers of AI components should implement security controls by design and default within their ML models, pipelines, and systems. Accordingly, the CSI focuses on four key areas of AI system development: secure design, secure development, secure deployment, and secure operation.

The UK National Cyber Security Centre (NCSC-UK) and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) co-authored the CSI with NSA and other partners.

The authoring agencies advise that this CSI does not replace general cybersecurity best practices and risk management programs. Recommendations in the CSI should be considered in conjunction with established cybersecurity, risk management, and incident response best practices. Read the full report here.

7.What is quantum advantage?

by Daniel Lidar
https://theconversation.com/what-is-quantum-advantage-a-quantum-computing-scientist-explains-an-approaching-milestone-marking-the-arrival-of-extremely-powerful-computers-213306

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

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

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

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

The source of quantum computing's power

Central to quantum computing is the quantum bit, or qubit. Unlike classical bits, which can only be in states of 0 or 1, a qubit can be in any state that is some combination of 0 and 1. This state of neither just 1 or just 0 is known as a quantum superposition. With every additional qubit, the number of states that can be represented by the qubits doubles.

This property is often mistaken for the source of the power of quantum computing. Instead, it comes down to an intricate interplay of superposition, interference and entanglement.

Interference involves manipulating qubits so that their states combine constructively during computations to amplify correct solutions and destructively to suppress the wrong answers. Constructive interference is what happens when the peaks of two waves – like sound waves or ocean waves – combine to create a higher peak. Destructive interference is what happens when a wave peak and a wave trough combine and cancel each other out. Quantum algorithms, which are few and difficult to devise, set up a sequence of interference patterns that yield the correct answer to a problem.

Entanglement establishes a uniquely quantum correlation between qubits: The state of one cannot be described independently of the others, no matter how far apart the qubits are. This is what Albert Einstein famously dismissed as "spooky action at a distance." Entanglement's collective behavior, orchestrated through a quantum computer, enables computational speed-ups that are beyond the reach of classical computers.

Applications of quantum computing

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

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

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

Another use of quantum information technology is quantum sensing: detecting and measuring physical properties like electromagnetic energy, gravity, pressure and temperature with greater sensitivity and

precision than non-quantum instruments. Quantum sensing has myriad applications in fields such as environmental monitoring, geological exploration, medical imaging and surveillance.

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

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

Staying coherent and overcoming errors

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

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

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

Quantum advantage coming into view

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

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

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

8.An RFC on IoCs - playing our part in international standards

by Andrew S

https://www.ncsc.gov.uk/blog-post/rfc-indicators-of-compromise-for-ietf

The NCSC has published a new RFC on Indicators of Compromise to support cyber security in protocol design - and hopes to encourage more cyber defenders to engage with international standards.

In August 2023, the IETF published the document Indicators of compromise (IoCs) and their role in attack defence as RFC9424. There are a lot of terms to unpack in that sentence, and we'll get to that later. The headline point is that, working with partners from UK industry – Kirsty Paine, James Sellwood and Ollie Whitehouse, before he became our new CTO – the NCSC have written an IETF RFC. It's the first document the NCSC has authored in the IETF, a major international standards body, and it details one of the most important tools in a cyber defender's arsenal – indicators of compromise.

This is the culmination of over three years of work, and we think it's a really valuable reference and set of considerations on these vital techniques for internet protocol designers and the wider community.

More about 'standards'

First things first, what are 'standards' in this context? I'm referring here to documents, agreed between different parties, that define how things should be made, or that lay out the best practice.

The world of standards is vast. There are standards for *everything* from charging cables and paper sizes to dishwashers. Not all standards are relevant to cyber security of course, but standards for how the internet works most certainly are. Internet standards don't just ensure interoperability and easy communication – the design decisions that standards bodies take have significant consequences for computer and network security.

IETF and RFCs

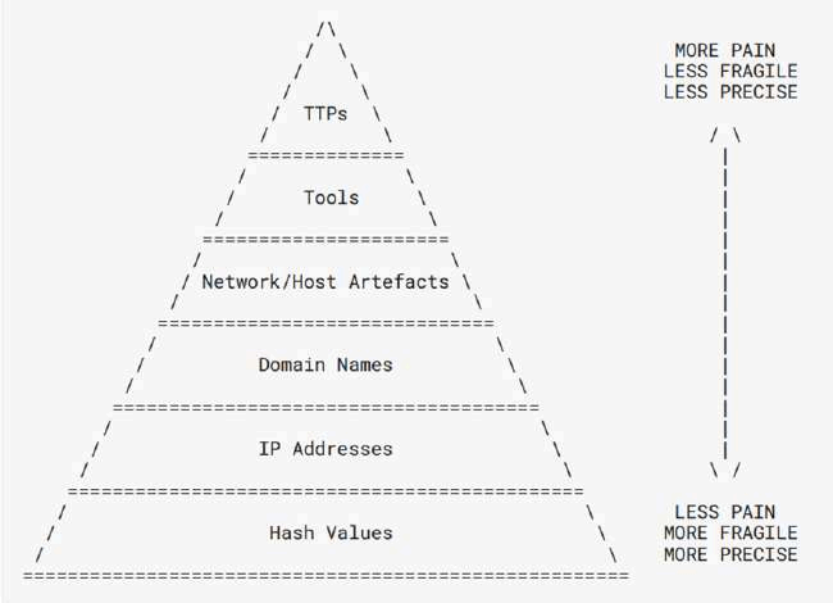
Now to unpack some of that first sentence! The IETF is the Internet Engineering Task Force – the international standards body responsible for designing the most important protocols on the internet today. This includes IP (Internet Protocol), TLS (Transport Layer Security), QUIC (which stands for, um, QUIC) and many, many others.

Anyone can participate in the IETF. Most participants are from industry, but academia, government and not-for-profit groups are all represented too. The IETF publishes standards called RFCs, which can define protocols or provide an informative reference, as our document does. Taking an IETF document from a first draft to a published RFC can be a long process. The authors carry out many rounds of revisions and improvements based on feedback until the document is deemed to have 'rough consensus' from the IETF community. It can then be published as an RFC.

More about *our* RFC

Our document is an introduction to indicators of compromise, or as we define them in the RFC, 'observable artefacts associated with an attacker'. They can be things like domain names for phishing sites, IP addresses of malware command and control servers, or cryptographic hashes of malicious executables. They provide a relatively simple way to detect malicious activity and tie it to a specific actor, while also being very easy to share quickly between organisations.

In the document, we cover the IoC lifecycle from discovery to deployment, through to end of life, while the 'pyramid of pain' shows on a scale how different types of IoC are more or less painful for an attacker to change in order to evade detection. We also include some real examples of how IoCs were used to respond to threats and cover *how* IoCs are used as part of a defence-in-depth strategy, and outline some considerations for their use.



An example of a TTP might be if an attacker always uses phishing as the initial access vector, and then pivots to other machines on the internal network. The TTP doesn't guarantee that it's the same attacker, but is robust against changes to the phishing email, or exploits used to move laterally. Whereas, towards the bottom of the pyramid, an attack coming from the same IP address as previously seen is very likely to be the same attacker; but it is much easier to lose track of if the attacker moves to a new service provider (or even reboots their router!)

This is a topic that will be bread and butter to those of you working in network defence and sharing threat intelligence. But it's a topic that not everyone involved in the IETF and designing the future internet will be hugely familiar with.
We hope our document will go some way to changing that.

Why standards bodies matter in cyber resilience

Standards bodies like the IETF are where the design decisions that will define the internet of the future are made. Getting involved is a great opportunity not only to see these new ideas long before they're deployed, but, more importantly, a chance to be part of the design process. This could mean bringing your own technology or idea to the table, or applying your expertise to improve other standards. Going to standards meetings is also just a great way to meet some really smart people and talk about the future of technology.

The NCSC has been participating in the IETF for a number of years now, contributing in a range of working groups and research groups – we're now also writing a draft on terminology for the use of post-quantum cryptography in internet protocols. We've found participating in standards bodies really useful to help us understand the future of the internet. It's also very rewarding to be able to contribute our cyber security and cryptographic expertise to something bigger.

Call to get involved

This is far from the only work the NCSC is doing in the world of international standards, across far more topics than just internet protocols. From the Internet of Things (IoT) to 5G, industrial control systems and AI, standards are vital to both the NCSC and UK national security. So we really want to encourage more subject matter experts and stakeholders from UK academia and industry to engage in relevant standards

bodies.

Bringing technical experience of real-world attack and defence considerations to these forums, along with operational insights, are important bedrocks to achieve and maintain UK cyber resilience.

9.From PKI to PQC: Devising a strategy for the transition

by Zeljka Zorz
https://www.helpnetsecurity.com/2023/11/16/transition-post-quantum-cryptography/

Quantum computers capable of breaking currently used encryption algorithms are an inevitability. And since the US, China and Europe are sprinting to win that arms race, we know that day is coming sooner rather than later.

Will organizations be ready to counter this threat to their data, though?

The Ponemon Institute recently canvassed 1426 IT and IT security practitioners knowledgeable about their organizations' approach to post-quantum cryptography, and found that 61% of them worry that their organization will not be ready to address the security implications of post-quantum computing.

As they see it, the main challenges are lack of time, money, and skilled personnel, but also:

- Uncertainty about the implications of post-quantum cryptography (PQC),
- The fact that post-quantum algorithms are still in the process of being standardized, and
- The fact that there is no clear ownership of the transition process within the organization.

Obstacles to remove for a successful transition to post-quantum cryptography

Before starting, organizations should know the answers to the following questions: Who holds the budget for the transition to post-quantum cryptography? Who is going to drive the effort? And where does the responsibility lie?

“Independently of PQC as a topic, one of the challenges often voiced by our customers is that public key infrastructure (PKI) can exist in a company in a broad range of departments, making it difficult centralize the responsibility for and ownership of it,” Jason Sabin, Chief Technology Officer at digital security company DigiCert, told Help Net Security.

Companies are solving that problem in different ways. In some cases, they centralize their cryptographic activity under one department and one head. In other cases, they create an acting committee, with stakeholders across the company who influence the direction of their programs.

“The companies that have already started to centralize management have an organizational method to request that budget and schedule the activity. But for the organizations that have not, there’s a little bit of an organizational design challenge present. And that’s where, I think, the technology leaders need to partner with the business leaders to come up with the best organizational path forward,” he remarked.

Quantum-resistant algorithms still not having been standardized is not an insurmountable challenge: Draft standards are available, the algorithms can be explored and tested on different systems, and the results can help organizations devise the right implementation plan in advance.

Finally, a change in mindset around quantum cryptography is needed. Executives must realize that the threat to data privacy and confidentiality exists even if cryptographically relevant quantum computers are not yet at hand.

"Threat actors can employ **Harvest Now, Decrypt Later** strategies to steal data, sit on it, and then decrypt it once quantum computers are around," Sabin pointed out.

"The other vector are software or devices that will be deployed in the field for a long time. They need to be secured with quantum-safe keys now, so that they can still protect the data and the users employing them when quantum computers become a reality."

All of this makes it obvious that a certain degree of urgency IS warranted.

A lot is at stake

Good relationships – whether business or personal – are based on trust. Unfortunately, trust that has been built over a long period of time can be lost quickly, leading customers and business partners to walk away.

"As a customer, I want to know which companies are investing in getting ready for a post-quantum future, and especially which are not! And companies will care whether their vendors and suppliers are 'quantum-safe'," Sabin pointed out.

From that perspective, a timely transition to post-quantum cryptography equals shoring up business resiliency.

"I think this transition should not be viewed just as a technology requirement or something that's happening deep in the weeds in the technology organization, but also something that needs to be at the forefront of business strategy into the next decade," he added.

And if, while transitioning the algorithms, companies make the effort to adopt a more efficient and secure approach to managing their cryptographic assets, they can end up with a better security posture overall.

The question now is to what degree are companies prepared to invest in maintaining trust with their partners, customers, and employees?

Know what you have and prioritize what needs to be prioritized

The good news is that there's a global concerted effort aimed at mitigating the data confidentiality risks associated with post-quantum computing ahead of time. For once, security is not an afterthought: we know what's coming and we can prepare for it.

To start, senior leadership must be made to understand the threats to data security caused by post-quantum computing, and they must make sure that resources are allocated to prepare for it.

(Ponemon's study revealed that currently only 30% of respondents say that their organization is allocating any budget for PQC readiness. 22% say that their company has no plans at the present time to allocate budget.)

Ideally, the organization already has a "central hub" that deals with all internal PKI matters, and the allo-

cated budget can be used to – among other things – engage experts that will test post-quantum algorithms and generally work on the transition to post-quantum cryptography.

They will first create and keep updated an inventory of cryptography keys in use. This activity must reveal the keys' characteristics, where they are located and for what they are used.

(Ponemon found that 52% of organizations have already invested in creating a centralized crypto-key inventory and gained operational benefits from this. But with PQC on the horizon, such an inventory will become a necessity.)

This information will allow them to:

- Identify priorities (e.g., protection of intellectual property, customer data) and answer questions that need to be answered (e.g., "How long does the data need to be protected?")
- Create a detailed plan of action (by consulting guidance such as NIST's Migration to Post-Quantum Cryptography),
- Establish a centralized crypto-management strategy that will be applied across the entire enterprise.

"Companies can then look at how to streamline the operations of managing the transition, by putting in place systems that deliver crypto-agility, i.e., automated certificate and key management. This will enable them to respond quickly and in sequence to their needs as the pressures on the cryptographic landscape change," Sabin concluded.

10.The new frontier in online security: Quantum-safe cryptography

by Monash University
https://techxplore.com/news/2023-11-frontier-online-quantum-safe-cryptography.html

A team of experts led by Monash University researchers, in collaboration with Australia's national science agency CSIRO, has created an algorithm that can help strengthen online transactions that use end-to-end encryption against powerful attacks from quantum computers.

Cryptography researchers from Monash University's Faculty of Information Technology and CSIRO's data and digital specialist arm Data61 have developed the most efficient quantum-secure cryptography algorithm, called "LaV," to enhance the security of end-to-end encryption, with potential application across instant messaging services, data privacy, cryptocurrency and blockchain systems.

End-to-end encryption is a way to secure digital communication between a sender and receiver using encryption keys. Mobile messaging services like WhatsApp and Signal use end-to-end encryption so that no one, including the communication system provider, telecom providers, internet providers or hackers can access the information being transmitted between the sender and the receiver.

It would take millions of years for a normal computer or even a supercomputer to hack into and gain access to data protected by end-to-end encryption. But a large-scale quantum computer could break current encryption within minutes and gain access to encrypted information more easily.

Lead researcher of the collaborative quantum security project, Dr. Muhammed Esgin, said the new cryptography tool will help make end-to-end encryption more secure, so online services can withstand hacks or interference from the most powerful quantum computers in the future.

"While end-to-end encryption protocols are quite well established and are used to secure data and messaging in some of the most popular instant messaging applications across the world, currently they are still vulnerable to more sophisticated attacks by quantum computers," Dr. Esgin said.

"This new cryptographic tool can be applied to various mobile applications and online transactions that use end-to-end encryption and is the first practical algorithm that can be used to fortify existing systems against quantum computers."

Co-author of the research and quantum-safe cryptography expert Associate Professor Ron Steinfeld said software for current technology is not being developed, keeping in mind the advent of much more powerful computing devices.

"Over the past few years we have seen many significant cyberattacks and data leaks in Australia alone, clearly showing that we need to pay much more attention to cybersecurity and mitigate vulnerabilities in our systems before such vulnerabilities are exploited by attackers," Associate Professor Steinfeld said.

"Government and Standards organizations worldwide are preparing for the possibility that large scale quantum computers, which can threaten the security of currently deployed encryption systems, could become a reality within the next decade or so.

"Our past experience has shown the process of updating encryption algorithms deployed in existing online systems can also take a decade or more to complete. This means that we need to urgently start updating our cybersecurity infrastructure to use quantum-safe cryptography, to ensure our systems are protected before the approaching quantum threat is realized," Associate Professor Steinfeld added.

This research was conducted in collaboration with researchers Dr. Dongxi Liu and Dr. Sushmita Ruj (now at the University of New South Wales) from CSIRO's Data61, and was presented at Crypto 2023, the 43rd International Cryptology Conference held earlier this year in Santa Barbara, U.S..

"The National Institute of Standards and Technology has been standardizing methods like encryption and digital signatures to protect basic internet security in a post-quantum world. However, these measures are not enough to protect advanced security applications. Our research is filling this gap," said Dr. Liu. "Our new algorithm has been implemented into code by Dr. Raymond Zhao from CSIRO's Data61 and is available open source."

As the next step, the research team is working on building a full quantum-secure key transparency protocol which can be readily deployed in encryption applications.

11.Cybersecurity Threats Just Got Worse

by Skip Sanzeri
https://www.forbes.com/sites/forbestechcouncil/2023/11/14/cybersecurity-threats-just-got-worse/?sh=7e4af810ceeb

If you have seen any of my previous Forbes articles, you will know that I write about the quantum computing threat to the encryption we all use to keep our data safe and private. Quantum computers, be-

cause they operate differently than our standard computers, have been mathematically proven to eventually break the internet's encryption. Called public-key Infrastructure (PKI), this is the cryptography that protects us as we are exchanging data online. The current gold standard, or commonly applied highest level of encryption is RSA (Rivest Shamir Adleman) 2048. So, to date, quantum computers have not been powerful enough to crack RSA 2048. However, there is a process called SNDL (Steal Now, Decrypt Later) wherein data stolen today is then stored on remote servers (in other countries) for decryption later. Since adversarial nation-states are storing this data, there is an exceptionally good reason for enterprises and government organizations to start moving to advanced cryptography now.

However, on September 18, the cybersecurity community was shocked to learn about a development from San Diego-based MemComputing (Mem) regarding a new, more imminent danger. Mem was asked by the US Air Force to use their technology to see if there was a way to easily crack PKI. Mem did the work and then published a white paper on how they used in-memory processing ASICs (Application Specific Integrated Circuits) to simulate breaking RSA *in real time*. The paper called "Scaling up prime factorization with self-organizing gates: A MemComputing Approach" describes how they used software emulation focusing on factorization test problems from 30 to 150 bits: "Results showed that the circuit generated the appropriate congruences for benchmark problems up to 300 bits, and the time needed to factorize followed a 2nd-degree polynomial in the number of bits."

In other words, Mem's findings estimate their ASIC chip can crack RSA 2048 in two years or less using classical, not quantum, computing**.** Compare this to our best estimates for supercomputers that would take millions of years to do the same. If Mem is right, their development demonstrates a fundamental breakthrough: A bad actor could threaten the world's public key encryption including *all data* traveling over the internet.

Previously we were more worried about quantum computers breaking public-key encryption. Commonly referred to as "Q-day," this depicts the time when quantum computers are powerful enough to break RSA 2048. The current estimates are anywhere from 5 to 10 years, and all believe that it will take an extremely powerful quantum computer to break public-key encryption.

The Mem breakthrough shows that this is no longer just about quantum computing but about how there are other clever methods to crack encryption. We can bet that if we know about this advancement, our adversaries know as well.

We Are Not Standing Still

Fortunately, our federal government has been hard at work. NIST (National Institute of Standards and Technology) has been working on this problem for over seven years and has nearly finalized recommendations of new cryptography that can be tested now. The new algorithms (also called quantum-resilient) are based on new and different cryptographic infrastructures using math problems different from the current prime factoring problems we use today for cryptography. They are tested to be quantum-resilient and should hold up against decryption methods such as Mem's and other developments.

On December 21, 2022, President Biden signed into law Public Law 117-260—the "Quantum Computing Cybersecurity Preparedness Act"—"An act to encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes." It is the first step in mandating that our entire federal government upgrade from our existing standard cryptography to new, quantum-resistant cryptography.

What To Do

It is now even more vital that enterprises and federal government organizations start the upgrade process to new encryption. Even if large organizations initiated a cryptographic upgrade today, it is going to take years, or even a decade, to complete the process. With Mem's development, and powerful quan-

tum computers on the way, we have zero time left to be safe.

Here are some steps organizations can take right now:

- **Learn About New Cryptography**: Business leaders should stay informed about the progress of new, available cryptography via NIST. These new quantum-resilient algorithms use different math and are not based on factoring large numbers like our existing encryption.
- **Act Now—Test New NIST Algorithms Right Away**: There is insignificant risk in testing quantum-resilient algorithms. By bringing this new cryptography into the network, enterprises and government organizations will quickly gain valuable hands-on experience, thus getting a jump on the larger, permanent upgrade that will be necessary.
- **Stay Crypto-Agile**: Companies should start planning for a transition to advanced cryptography with the ability to change cryptography on the fly. At the same time, we expect the new algorithms to go through difficulties. Some will fail, some will need adjustment, some will work. So being crypto-agile is a way organizations can use new cryptography without worrying about committing to one new algorithm.
- **Ease Of Deployment:** Deployment of new cryptography algorithms will take time and organizations can reduce risk by finding partners who can install these algorithms over the existing cryptography: so, no rip and replace.
- **Address Your Entire Network:** Any outdated or vulnerable cryptography provides an attack vector. Think of servers, switches, phones, laptops, cloud-based servers and even satellites.
- **Scalability**: Look for partners that can deploy quantum-resilient algorithms without installing anything on edge devices. This will make it much easier and quicker to secure your organization as there is no change to the endpoint or user experience.
- **Hybrid Approach While Transitioning**: While quantum-safe cryptography is being standardized, organizations should use a hybrid approach. Finding a solution that leaves existing encryption to remain in place while transitioning to quantum-resilient algorithms is key.

With the Mem breakthrough, the reason to test and deploy advanced, quantum-resilient cryptography has intensified. Make no mistake, if public-key cryptography starts breaking, this will prove to be an existential threat to our nation, allies and the free world.

12.Key Takeaways from the Second PKI Consortium Post-Quantum Cryptography Conference

by Casey Crane
https://www.thesslstore.com/blog/key-takeaways-from-the-second-pki-consortium-post-quantum-cryptography-conference/

In early November, public and private cybersecurity and cryptography experts worldwide gathered in

Amsterdam to share their insights and updates about quantum-resistant (quantum-safe) cryptography at the PKI Consortium's latest conference. Some presentations focused on the technical details of PQC cryptographic algorithms and schemes, while others talked about the considerations surrounding the implementation of quantum-safe cryptography in specific environments.

The PKI Consortium is a non-profit organization comprising 100+ public and private member organizations (governments, certificate authorities, auditors, service providers, consultants, etc.) from around the world. This event marked the PKI Consortium's second PQC conference, the first of which was hosted in Ottawa in Ontario, Canada.

Since we figured most of our readers didn't get to make the trip to the Netherlands or want to get up as early as 3 a.m. to tune in remotely, we've put together a breakdown of some of the key takeaways and lessons we learned from this year's sessions.

Let's hash it out.

An Overview of the Top Concerns Haunting Organizations Regarding PQC Implementation

Before we dive into all of the top takeaways from this year's conference, let's quickly go over some of the key challenges that industry experts say organizations face when preparing for post-quantum cryptography.

Of course, this is only a handful of the challenges that public and private sector organizations may experience in the journey to a post-quantum world. Now, it's time to explore some of the takeaways global industry leaders shared during the 2023 PQC conference.

Top 9 Takeaways For Public and Private Sector Stakeholders

1. We Need to Stop Calling It "Post-Quantum" Cryptography

Using a term like "post-quantum cryptography" doesn't drive home the urgency of transitioning from quantum-insecure to quantum-resistant cryptography. The actual verbiage is still contested within the industry, though, as some experts refer to it as *PQC* while others call it "quantum-resistant" or "quantum-safe" cryptography.

Chris Hickman, Chief Security Officer at KeyFactor who presented and participated in one of the conference's panel discussions, described the term "post-quantum" cryptography as the biggest disservice industry professionals did to themselves. "This is an evolution of security, and we really need to start thinking of it in those terms," said Hickman, who said that organizations need to start thinking through the security needs regarding these vastly different technologies now and not when quantum computers are widely available. He pointed out that the industry has been relying on the same technologies for several decades and that enough is enough. "What else has lasted for 40 years in IT, period? Not a lot. Security-wise, not a lot."

"So, I think, yeah, things are going to take on their own life cycle and their own trajectory because organizations are going to start to realize that this is simply an evolution. This is the next step.

No, we've never been through this; yes, it's going to be painful. Are we going to stumble along the way? Organizations will stumble along the way, that's without question. But the thing that we can do here is help explain the best ways to do that, the ways to mitigate the risk, how to look at it from risk management standpoint. I think that's a very smart way to look at it."

— Chris Hickman, Chief Security Officer at KeyFactor

Hickman's sentiments are shared by other industry experts, including Tim Hollebeek, DigiCert's Industry Technical Strategist. He recommends referring to it as "quantum-safe cryptography" instead.

"*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.*"

— Tim Hollebeek, Industry Technical Strategist at DigiCert

2. Quantum Computing Is Something to Start Planning & Preparing for Now using Hybrid Cryptography

A theme that was repeated throughout the two-day conference is that you can (and should) start planning and preparing for PQC rather than waiting. If you wait, you'll already be too late. While saying companies should start planning and preparing is all well and good, but it leaves us with two important questions:

1. How do we start preparing?
2. And how soon do we need to do so?

One of the things highlighted by many speakers was having a hybrid quantum security strategy. The benefit of using PQC hybrid algorithms in your approach is that they still support the "classical" algorithms that are necessary to fight modern threats while also using PQC algorithms to protect data against "harvest now, decrypt later" attacks.

This means bad guys would have to break two cryptosystems in order to compromise data. This protects you while in the transition period when we're not sure about whether the new PQC algorithms will work as intended. (After all, we've seen a number of NIST candidate algorithms being broken over the past several years using modern computers.)

We'll talk more about the answer to the first question in just a moment. But as far as the answer to question #2 is concerned: start planning now. Quantum computers are becoming more advanced, and companies are working on "noise reduction" to help facilitate more powerful machines that require fewer qubits to operate. So, what does this mean for organizations with regard to when they need to start getting their ducks in a row?

"*The main thing is, don't wait. Well, we **do** want you to wait for the final standards. So, you can test out the algorithms now. You can get ready. Wait for the final standards to begin actually putting these into products. But for planning purposes, don't wait to think about your migration – start getting ready for that.*"

– Dustin Moody, Mathematician & Project Lead, Post-Quantum Cryptography at the National Institute of Standard and Technology (NIST)

3. A Cryptographic Inventory and Risk Analysis Are the First Steps to PQC Readiness & Agility

By and large, organizations are clueless about where and how they're using cryptography within their networks and IT infrastructure. In some cases, the uses are internal; other times, they're provided through third-party services and software.

But the key thing to remember is that if you don't know what cryptographic assets you have or where they are, then you can't identify your risks, and if you can't do that, then you don't know

what you need to mitigate them.

- **Creating an inventory of cryptographic assets and vulnerabilities.** This involves using automated scanning tools and manual scanning methods to catch what they miss.

- **Perform quantum risk analysis on top of your standard risk analysis.** This will provide you with greater insights into the PQ vulnerabilities within your network and IT environment.

The next step is to prioritize where you want to start taking action and make preparations for "**Q Day**." But how do you do that if you don't know where your organization currently stands? This question is one Tom Patterson, Quantum Security Global Lead at Accenture, says he wants to help organizations globally figure out via a Quantum Security Maturity Index.

Patterson said the concept is similar to the Capability Maturity Model Integration (CMMI) in that it gives company boards and executives a way to measure where they are and see how far they still have left to go. If they're at level 2 and want to be at level 3, what money and time would they need to invest?

His company is working with organizations across the world in multiple sectors to create standardized definitions relating to PQC adoption and maturity. The PQC journey the company has outlined currently has eight PQC maturity tiers that are part of Accenture's program.

"I'm just trying to drive the process so that there's standardized definitions about adoption and maturity," said Patterson. "If you can't measure it, you can't protect it.'"

Where Does PKI Come Into Play in All of This?

That's a good question — one Patterson hopes organizations will help him answer. After all, having a robust and PQC-safe PKI requires more than just swapping out a few existing assets.

"Because PKI is so robust in its current state, you can't just tinker with it," says Tom Patterson. Instead:

"We talk about how it is highly sophisticated and highly integral to their operations today, and just changing over from one HSM to another, and from one piece to another, from one certificate to another certificate. That's not the answer. That's not how it's going to work."

Changing the underlying foundation of internet security — all of the technologies, protocols, policies, and other components that make up public key infrastructure (PKI) — is a process Patterson says will take place over "many years going forward." But if an agreed-upon maturity index is created through collaboration across organizations in various sectors, it'll improve the overall quantum defenses of the world as a whole.

He put out a call for "volunteers" of sorts; organizations that want to participate in the process and help identify areas and specific steps to build out. Accenture is planning to unveil the results of this collaborative effort to the world at the World Economic Forum in January 2024.

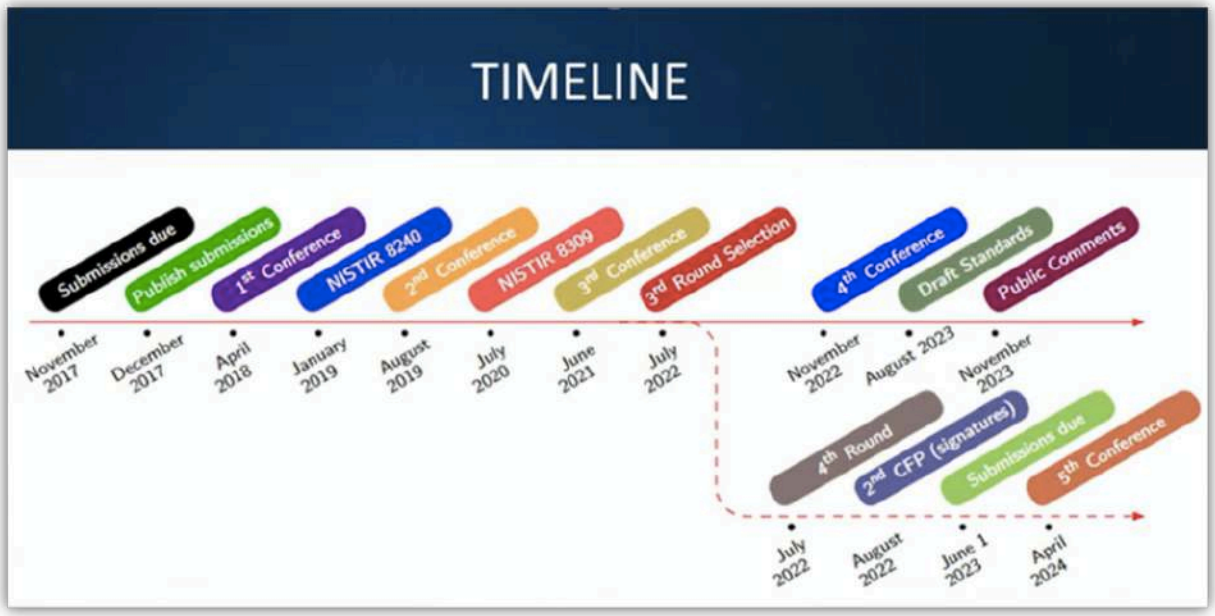
4. NIST's First PQC Standards Are Coming in Early 2024

Since 2016, the National Institute of Standards and Technology (NIST) has been engaged with the cryptographic community in a "competition" to create quantum-resistant cryptographic algorithms. (This isn't a new approach, as RSA and other algorithms have been created in similar scenarios.) Although NIST has released drafts of the first three PQC algorithms for public comments, the federal standards organization is looking to publish the first official PQC standards early next

year (2024).

Two experts from NIST — Dustin Moody, Mathematician & Project Lead, Post-Quantum Cryptography and Bill Newhouse, Cybersecurity Engineer & Project Lead, National Cybersecurity Center of Excellence (NCCoE) — shared the ongoing process regarding the selection of PQC algorithms. Their update offered insights into the NIST PQC standardization process, how it's coming along, and practices to make migrating from quantum-vulnerable public-key cryptography to quantum-resistant cryptography a bit easier.

Here's a quick timeline of the NIST PQC process:



As of the writing of this article:

- NIST has completed four evaluation rounds for cryptographic algorithms.
- NIST opened a request for public comments in August (which are open until Nov. 22, 2023) on the first three drafts of the Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography:
  - FIPS 203: ML-KEM (Kyber)
  - FIPS 204: ML-DSA (Dilithium)
  - FIPS 205: SLH-DSA (SPHINCS+)
- **Additional signature schemes are still being considered.**

This "small call" for additional signatures, ideally based on code-based algorithms rather than lattice problems, aims to create greater diversity amongst the pool of PQC algorithms. The idea here is to have additional general-purpose signature schemes and those that have faster verification and shorter signatures for different use cases.

5. Being Crypto-Agile Is Crucial and Is Everyone's Responsibility

Crypto-agility is described by Germany's Federal Office for Information Security (BSI) as a principle of keeping cryptographic mechanisms 'as flexible as possible in order to react to develop-

ments, implement upcoming recommendations and standards, and possibly replace algorithms in the future that no longer guarantee the desired level of security.'" This also entails being able to use existing secure hardware and systems to meet the needs of new cryptographic algorithms and protocols without hindering performance.

But what do the experts say about crypto-agility in terms of what it represents and how it should be perceived?

"Crypto-agility begins with agile standards," said Jaime Gomez Garcia, Head of Quantum and Architecture at the Crypto and Blockchain CoE, Banco Santander, who emphasized that it's constantly adapting and changing through collaboration. "Our new cryptography standard isn't built as a Word document; it is built on GitHub."

Bill Newhouse from NIST describes crypto-agility as a dream for public and private sector organizations alike. "It's a desire, and some of you have mapped out schemes to support this within your technologies to support this."

The overarching idea that many presenters reiterated is that everyone needs to keep cryptographic agility in mind when evaluating solutions. But Robert Hann, Global Vice President of Sales, Cryptographic Center of Excellence at Entrust, says that being crypto-agile is more than having the right tools in place:

"Crypto-agility is not just about tech; it involves people and processes. It's a process of change, and many organizations aren't good at changing cryptography because we've never had to try. We haven't really been tested hard. We now are about to, so you've absolutely got to build that in, in the solutions you buy, the software you develop."
— Robert Hann, Global Vice President of Sales, Cryptographic Center of Excellence at Entrust

6. By and Large, CISOs Won't Adopt PQC Until They Have To

It's no secret that organizations are seemingly dragging their feet when it comes to dedicating the time, people, and resources to preparing for the quantum threats to come. But when you consider the high amounts of stress and short tenures of most CISOs, it's easy to see why they view quantum threats as things to put off until "later," even though they're not. Banco Santander's Garcia says that there's a growing need for a change of mindset and approach.

In his presentation on Comparing Strategies for Quantum-Safe Cryptography Adoption in Organizations, Garcia cited research from KMPG and Germany's (BSI) that shows the overwhelming majority of CISOs are waiting to take any real action until there are standards (89%) or regulatory requirements (96%) in place that force their hands. People are burned out on the "sky-is-falling" messages they've been hearing for decades.

"People are going to act when they're required to act. My conclusion is that risk-based messages do not work. They have not worked so far, and they will not work because we are talking about a threat that happens far in the future. So, we need to explain in a different way why things need to be done now."

So, what's the alternative? Garcia pointed to an executive action that came out of the U.S. White House as an example (a memorandum on "Migrating to Post-Quantum Cryptography"). The document breaks down specific requirements that must be met within set periods. For example: "Within 30 days of the memorandum, agencies will designate a cryptographic inventory and migration lead for their organization."

The point is to create a sense of urgency and to show a way forward by outlining the preparatory steps that must be outlined within a limited period.

Consider the high levels of stress amongst CISOs for all of the urgent items on their to-do lists that have short timespans. It's understandable (in some ways) why quantum preparations aren't at the top of the list. After all:

- 94% of CISOs admit to being stressed at work, and 65% say it compromises their job capabilities;
- Three in four (77%) CISOs admit that job-related stress is taking a toll on their physical and mental health; and
- CISOs are in their roles for a median period of 4 years — meaning they'll be out of their roles significantly sooner than quantum computers are expected to arrive.

7. Take a Stealth Approach to Get Funding and Support of Your PQC Initiatives

One of the key challenges I'd mentioned earlier when organizations face when planning for and implementing PQC-focused initiatives is that they often lack the financial support of their boards and c-suite execs. Although CISOs and other IT/cybersecurity professionals largely agree that quantum cryptography represents an opportunity to invest in new technologies and divest legacy systems, many of their organizations' leaders don't necessarily share that same opinion when it comes to supporting PQ initiatives with the companies' checkbooks.

"Many organizations are struggling to justify a project with no end date. Most projects have a compelling event: 'I have to go live by January 2024.' PQ's different. We don't know when we don't have to be live; we know roughly that we have to be ready by, probably, 2028, 2027 if we want to be a couple of years ahead of our adversary.

"[…] so if it's that kind of timeline, try justifying that to a board member by saying 'I think it's near the end of the decade' and they say, 'well, this other project is going to generate us more revenue, reduce our risks more, and so on' and they'll put their money there."
— Robert Hann, Global Vice President of Sales, Cryptographic Center of Excellence at Entrust

Even though boards often view quantum computing as a priority, protecting their organizations against quantum-based threats doesn't seem to garner as much interest.

So, what's the solution? Hann suggests taking a stealthy approach: start combining key aspects of your organization's PQC initiatives into other more timely and profitable priorities your execs favor. For example, tie it in with your zero-trust strategy or AI strategy. Doing this helps the board set the goals and priorities they think matter most while enabling you to do what needs to be done to prepare for the quantum threats to come.

8. Businesses Want Financial Incentives to Become Early Adopters

One of the most interesting points discussed at the conference was brought up by one of the audience members during an open forum discussion by Anita Wehmann, Senior Advisor Information Security at the Ministry of the Interior and Kingdom Relations (BZK) of the Netherlands and Germain van der Velden: Being a "first mover" is a risky venture.

You're bound to make mistakes that will cost your business money. If organizations and businesses are expected to take on the risks associated with being early adopters, shouldn't there be

some financial incentive(s) for them to do so?

"As this is such a global problem, there needs to be at least some clear incentive for 'first movers,'" said the unnamed forum participant.

"I think we need to at least get some clarity on that – whether there will be possibilities to support each other also in the form of financial perspective. So, not only knowledge and things like that, but really, enterprises have a financial aspect as well. […] The financial part should not be forgotten if you want to enfold enterprises into this integration path."

Regarding the concept of being an early adopter, Wehmann separately brought up an interesting point and question in a panel discussion near the end of the two-day conference: If the expectation from governments and industry leaders is that critical infrastructure organizations be among early adopters of PQC, isn't that, in some ways, counterintuitive to critical infrastructure security?

Critical infrastructure organizations have a longstanding history of being risk-averse. But if those organizations are among the first adopters of PQC, then they'll be the ones making the mistakes that could have potentially devastating results.

It seems to be a *damned if you do, damned if you don't* kind of situation. But what's the solution? As of right now, no one seems to have a definitive answer.

9. PQC Progress Requires Significant Collaboration Between Global Regions and Industries

Quantum readiness requires the best and brightest from around the world to come together for this shared cause. There have been significant collaborations between various agencies and research institutes across Europe, as well as with North America (U.S. and Canada). But even with those collaborations, there are different perspectives in terms of how we should approach this overarching goal, and even which algorithms should be used.

While many presenters agree that there's already good collaboration going on between different countries' cryptographic experts, there's always room for growth and improvement. We need to connect more, coordinate better, and share more information.

Every initiative is valuable and has its own merits. We agree on many points, but there are nuances where different countries differ in terms of prioritizations and approaches.

Final Thoughts on the Insights Shared at the PKIC PQC Forum

We hope that you've found this article useful. From a non-cryptographer perspective, it was interesting to hear the different perspectives and earnest discussions that took place. Although some of the presentations left me with more questions than answers — for example, the intricacies of lattice-based algorithms — it's opened up a wealth of information and ideas that I (and possibly you) had not considered. Did you attend the conference (either in person or remotely, like me) and have additional takeaways to share? If so, we'd love for you to share them in the comments below!

13.Security Agency Publishes Post-Quantum Guidance For Firms

by Phil Muncaster

https://www.infosecurity-magazine.com/news/security-agency-postquantum/

The UK's National Cyber Security Centre (NCSC) has released more information designed to help organizations migrate their systems to post-quantum cryptography (PQC).

Quantum computing promises to open the door to boundless innovation, but also the threat of effectively breaking public key cryptography (PKC); specifically, the algorithms used for key establishment and digital signatures, the agency warned.

"For key establishment and encryption, there is a risk from an attacker collecting and storing data today and decrypting it at some point in the future," it said.

"This means that for organisations that need to provide long-term cryptographic protection of very high-value data, the possibility of a CRQC [cryptographically-relevant quantum computer] in the future is a relevant threat now."

Attackers could theoretically also used quantum computers to forge digital signatures to impersonate the legitimate private key owner or tamper with information protected by a digital signature, the NCSC warned.

Fortunately, the US National Institute of Standards and Technology (NIST) has been busy selecting and establishing new algorithms that will be immune to quantum cracking.

The NCSC's new guidance features several important points for enterprise IT and security bosses:

PQC upgrades can be planned to take place within regular technology refresh cycles

The ML-KEM (Kyber) and ML-DSA (Dilithium) algorithms selected for standardization by NIST are suitable for general purpose use. All proposed parameter sets provide an acceptable level of security for personal, enterprise and Official-tier government information

The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases

Operational systems should only use implementations based on final standards

Combining a PQ key establishment algorithm with a traditional key establishment algorithm to drive a PQ/T hybrid key establishment scheme should only be used as a stepping stone to PQC

Although viable quantum computers are still some years away, lawmakers and industry have been preparing the way. Last December a US Quantum Computing Cybersecurity Preparedness Act was signed into law, and in September 2023, a new tech consortium launched with a mission to drive adoption of PQC.

Axel Poschmann, head of product innovation and security at PQShield, welcomed the new NCSC guidance.

"Previously, a key barrier to migration to post-quantum cryptography has been questions around exactly how and when the new algorithms would be finalized. These new draft [NIST] standards and the NCSC's recommendations provide this assurance and a framework that allows everyone to move forward in protecting our cryptography systems against the quantum threat," he added.

"This is a testament to the expertise of our world-leading researchers and engineers as well as the col-

lective dedication of the entire post-quantum cryptography community."

14.Next steps in preparing for post-quantum cryptography

https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

This guidance helps system and risk owners in commercial enterprises, public sector organisations and critical national infrastructure providers to think about how to best prepare for the migration to post-quantum cryptography.

Background

In our 2020 white paper, Preparing for Quantum Safe Cryptography, we set out the threat that quantum computers pose to current cryptography, and the work by organisations such as the US National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI) to counter this threat.

Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today's digital, 'classical', computers. They are, theoretically, capable of performing certain computations that would not be feasible for classical computers. Although advances in quantum computing technology continue to be made, quantum computers today are still limited, and suffer from relatively high error rates in each operation they perform.

In the future, it is possible that error rates can be lowered such that a large, general-purpose quantum computer could exist. It is, however, impossible to predict when this may happen as many engineering and physical challenges must be overcome first. If such a computer could exist in the future, most traditional public key cryptography (PKC) algorithms in use today will be vulnerable to attacks from it. A quantum computer that will be able to run these attacks is referred to as a cryptographically-relevant quantum computer (CRQC).

These traditional PKC algorithms include:

- algorithms based on integer factorisation such as RSA
- algorithms based on the discrete logarithm problem such as Finite Field Diffie-Hellman, ECDH, DSA, ECDSA, EdDSA

These algorithms are primarily used for key establishment (used to agree a shared cryptographic key for secure communication) and digital signatures (used to underpin proof-of-identity and trust on a network).

For key establishment and encryption, there is a risk from an attacker collecting and storing data today and decrypting it at some point in the future. Given the cost of storing vast amounts of old data for decades, such an attack is only likely to be worthwhile for very high-value information. This means that for organisations that need to provide long-term cryptographic protection of very high-value data, the possibility of a CRQC in the future is a relevant threat now.

The threat to digital signatures is that an adversary in possession of a CRQC could forge signatures to impersonate the legitimate private key owner, or tamper with information whose authenticity is protected

by a digital signature. This attack should be considered before a CRQC exists, particularly when deploying keys for high-value trust anchors that are intended to have a long operational lifetime.

In contrast with PKC, the security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with at least 128-bit keys (such as AES) can continue to be used. The security of hash functions such as SHA-256 is also not significantly affected, and secure hash functions can also continue to be used.

The NCSC advice remains that the best mitigation against the threat of quantum computers to traditional PKC is post-quantum cryptography (PQC), also called quantum-safe cryptography or quantum-resistant cryptography. PQC algorithms will replace the vulnerable PKC algorithms used today for both key establishment and digital signatures. The security of PQC algorithms is based on mathematical problems that are believed to be intractable for both classical and quantum computers. These algorithms will not necessarily be drop-in replacements for the current PKC algorithms in protocols or systems, so system owners should begin planning for the migration to PQC.

Implications of PQC migration for users and system owners

For users of commodity IT, such as those using standard browsers or operating systems, the switchover to PQC will be delivered as part of a software update and should happen seamlessly (ideally without end-users even being aware). To ensure devices are updated to PQC when it is available, system owners should ensure they follow the NCSC's guidance on keeping devices and software up to date.

System owners of enterprise IT, such as those who own IT systems designed to meet the demands of a large organisation, should communicate with their IT system suppliers about their plans for supporting PQC in their products.

For a minority of systems with bespoke IT or operational technology, such as those that implement PKC in proprietary communications systems or architectures, choices will need to be made by system and risk owners as to which PQC algorithms and protocols are best to use.

Technical system and risk owners of both enterprise and bespoke IT should begin or continue financial planning for updating their systems to use PQC. PQC upgrades can be planned to take part within usual technology refresh cycles once final standards and implementations of these standards are available.

Towards PQC standardisation

Since 2016, NIST has been running a process to standardise PQC algorithms, backed up by academic scrutiny from the international cryptography community. This process has been followed closely by standards-defining organisations including:

the Internet Engineering Task Force (IETF), who have been working on updating their protocols to be resistant against a quantum computer

ETSI, who have been producing migration and deployment guidance

NIST has selected one algorithm for key establishment:

- ML-KEM (CRYSTALS-Kyber)

and three algorithms for digital signatures:

- ML-DSA (CRYSTALS-Dilithium)
- SLH-DSA (SPHINCS+)

- FALCON

There are also two already standardised stateful hash-based signature algorithms, which also offer protection against a quantum computer but can only be used in a subset of use cases. These are Leighton-Micali Signatures (LMS) and eXtended Merkle Signature Scheme (XMSS).

The draft standards for ML-KEM, ML-DSA and SLH-DSA were released in August 2023. Final standards for these algorithms are expected in 2024. The draft standards for FALCON will be released in the future.

The NIST draft standards will allow developers to test these algorithms in their systems and develop plans for deploying these algorithms when the final standards are released. The draft standards are subject to changes before the final standards are released, so there is a risk that implementations based on draft standards may not be compatible with the final standards. **For this reason, the NCSC strongly advises that operational systems should only use implementations based on the final NIST standards**.

These algorithms will need to be implemented in protocols before they can be used on the internet and in other networks. The IETF is in the process of updating the most widely-used security protocols. This includes ensuring that PQC algorithms can be incorporated into key exchange and signature mechanisms in existing protocols such as TLS and IPsec. IETF implementations of post-quantum protocols are subject to change until they are published as RFCs. The NCSC strongly advises that operational systems should use protocol implementations based on RFCs, and not on Internet Drafts.

Choosing algorithms and parameters for your use cases

The following table gives the NCSC recommended algorithms, their functions, and specifications:

Algorithm	Function	Specification
ML-KEM	Key establishment algorithm	NIST Draft - FIPS 203
ML-DSA	Digital signature algorithm	NIST Draft - FIPS 204
SLH-DSA	Digital signature algorithm for use cases such as signing firmware and software	NIST Draft - FIPS 205
LMS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208
XMSS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208

The above algorithms support multiple parameter sets that offer different levels of security. The smaller parameter sets generally require less power and bandwidth, but also have lower security margins. Conversely, the larger parameter sets provide higher security margins, but require greater processing power and bandwidth, and have larger key sizes or signatures. The level of security required can vary according to the sensitivity and the lifetime of the data being protected, the key being used, or the validity period of

a digital signature. The highest security level may be useful for key establishment in cases where the keys will be particularly long lived or protect particularly sensitive data that needs to be kept secure for a long period of time. It may also be useful for digital signatures where the keys have a particularly long lifetime, such as in a root of trust.

Note that:

- **All of these parameter sets provide an acceptable level of security for personal, enterprise and OFFICIAL-tier government information.**
- ML-KEM and ML-DSA are algorithms suitable for general purpose use. **The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases**.
- Users may wish to use the smaller parameter sets in situations where key/signature size is a consideration, or where it may help address performance issues, such as in constrained devices.

Hash-based signatures

Hash-based signatures such as SLH-DSA, LMS and XMSS rely on different security assumptions than ML-DSA and FALCON. They are **not** suitable for general purpose use as the signatures are large and the algorithms are much slower than ML-DSA. However, these algorithms may be a good fit for use cases such as signing firmware and software where speed is not a bottleneck.

For LMS and XMSS, the security of these algorithms critically depends on users correctly managing the state (that is, knowing which one-time keys have been used for signing so it can be guaranteed that they are never used again). Cases where state management is a more tractable problem include firmware and software signing. ETSI have created advice on how to do this in their Technical Report TR 103 692 v1.1.1 . LMS and XMSS should only be used in situations where it is possible to manage state in a trusted manner for the lifetime of the signing key.

SLH-DSA provides a more robust alternative for situations where it may be difficult or impossible to guarantee a one time key is not re-used, as state management is not straightforward and mistakes can be detrimental to security. This increased robustness comes with significantly larger signature sizes and greater signing time than either LMS or XMSS, although the verification performance is similar.

LMS and XMSS are available as final standards, whereas, as of August 2023, SLH-DSA is available as a draft standard.

Post-quantum traditional (PQ/T) hybrid schemes

A PQ/T hybrid scheme (as defined in this IETF Draft) is one that combines one (or more) PQC algorithms with one (or more) traditional PKC algorithms where all component algorithms are of the same type (for example, a PQC signature algorithm combined with a traditional PKC signature algorithm to give a PQ/T hybrid signature).

There are greater costs to PQ/T hybrid schemes than those with a single algorithm. PQ/T hybrid schemes will be more complex to implement and maintain and will also be less efficient. However, there may sometimes be a need for a PQ/T hybrid scheme, due to **interoperability**, **implementation security**, or constraints imposed by a **protocol** or system:

Interoperability

In a large network, it will be necessary to adopt a phased approach to the introduction of PQC.

This will lead to a period where both PQC and traditional PKC algorithms need to be supported simultaneously. Flexible protocols incorporating PQ/T hybrid schemes will make it possible for systems with different security policies to interoperate, and should also allow for a migration to a PQC-only future.

Implementation security

PQC is an emerging technology and, while NIST has a robust process to ensure the security of the PQC algorithms, it will take time for assurance in implementations of these algorithms within protocols and systems to be developed. Therefore, users may wish to consider using PQC in combination with traditional PKC with the aim of building a system which remains secure, even if one of the implementations is insecure.

Protocol constraints

Some protocols may have technical constraints that mean it is difficult to remove the traditional PKC algorithm when adding support for PQC. An example of this is the need to avoid IP layer fragmentation in IKEv2.

Additional considerations for PQ/T hybrid schemes

There are many ways to combine a PQ key establishment algorithm with a traditional key establishment algorithm to obtain a PQ/T hybrid key establishment scheme. For example, using a PQ/T hybrid key establishment mechanism such as in the draft for Hybrid TLS (draft-ietf-tls-hybrid-design-09) or at the protocol level such as in the design for IKE (RFC 9370). These two protocols have been modified to incorporate PQ/T hybrid schemes in a relatively simple and backwards-compatible way.

PQ/T hybrid key establishment mechanisms should be designed carefully to ensure the hybridisation mechanism does not allow additional attacks. As of November 2023, advice on how to do this is currently in development by ETSI.

Proposed PQ/T hybrid schemes for authentication can be significantly more complex than those used for confidentiality, due to the need to make sure both signatures verify in a robust way. There has also been significantly less research activity into PQ/T schemes for authentication than for confidentiality, and there is not yet guidance or a consensus on how to do this in a secure way.

Public key infrastructures (PKIs) make use of authentication algorithms to create, store, verify and revoke digital certificates. Within a PKI, it is difficult to change an individual signature algorithm in isolation. PQ/T hybrid authentication within a PKI requires either a PKI which can generate and sign traditional and post-quantum digital signatures, or two parallel PKIs (one for traditional and one for post-quantum digital signatures). This additional complexity and the difficulty in migrating PKIs mean that a single migration to a fully post-quantum PKI is preferred to adopting an intermediate PQ/T hybrid PKI.

Recommendations on PQ/T hybrid schemes

In the future, if a CRQC exists, traditional PKC algorithms will provide no additional protection against an attacker with a CRQC. At this point, a PQ/T hybrid scheme will provide no more security than a single post-quantum algorithm but with significantly more complexity and overhead. **If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure, and it should be used within a flexible framework that enables a straightforward migration to PQC-only in the future**.

With this in mind, technical system and risk owners should weigh the reasons for and against PQ/T hybrid schemes including interoperability, implementation security, and protocol constraints, as well as the complexity, cost of maintaining a more complex system, and the need to complete the migration twice

(once to a PQ/T hybrid scheme and again to PQC-only algorithms as a future end state).

Summary

- Most PKC algorithms in use today will be vulnerable to a CRQC. The best mitigation against the threat of quantum computers to traditional PKC is PQC.
- The security of symmetric cryptography is not significantly impacted by quantum computers, and existing symmetric algorithms with appropriate key sizes can continue to be used.
- PQC upgrades can be planned to take place within usual technology refresh cycles.
- ML-KEM (Kyber) and ML-DSA (Dilithium) are algorithms selected for standardisation by NIST that are suitable for general purpose use. All proposed parameter sets provide an acceptable level of security for personal, enterprise and OFFICIAL-tier government information. The NCSC recommends ML-KEM-768 and ML-DSA-65 as providing appropriate levels of security and efficiency for most use cases.
- The NCSC strongly advises that operational systems should only use implementations based on final standards.
- If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure that allows a straightforward migration to PQC-only in the future.

15.UK agency warns post-quantum cryptography migration will be 'very complicated'

by Alexander Martin
https://therecord.media/post-quantum-cryptography-migration-uk-ncsc

New guidance published Friday by the United Kingdom's National Cyber Security Centre (NCSC) has cautioned that the migration to post-quantum cryptography will be "a very complicated undertaking."

As explained in the NCSC's blog post, more than just mathematics will be necessary to meet the threat that quantum computers pose to traditional public-key cryptography, as some systems — such as those controlling critical national infrastructure — would simply not be capable of running the resource-heavy software used in post-quantum cryptography.

Ultimately, the security of public key cryptographic systems relies on the mathematical difficulty of factoring very large prime numbers — something that traditional computers find exhaustingly difficult.

However, research by American mathematician Peter Shor published in 1994 proposed an algorithm for finding these prime factors with far more ease, undermining some of the key assumptions about what makes public-key cryptography secure.

The good news, according to NCSC, is that while advances in quantum computing are continuing to be

made, the machines that exist today "are still limited, and suffer from relatively high error rates in each operation they perform," writes the agency's head of crypt research, John H. (Surnames are not published for most of its staff.)

But the agency warns that "in the future, it is possible that error rates can be lowered such that a large, general-purpose quantum computer could exist," but it is "impossible to predict when this may happen."

That does not mean that the risk doesn't exist today, as contemporary attackers could be collecting and storing data today for decryption "at some point in the future."

"Given the cost of storing vast amounts of old data for decades, such an attack is only likely to be worthwhile for very high-value information," states the NCSC blog.

As such, at least for the subset of organizations that have access to this kind of very high-value data, the possibility of a cryptographically-relevant quantum computer (CRQC) existing at some point in the future is a relevant threat right now.

To that end, numerous organizations and researchers have been attempting to develop a new kind of cryptography that would not be broken by a quantum computer — including the Dilithium standard proposed by Google.

Known as post-quantum cryptography (PQC), the work to develop a standard has continued at pace since 2016 when the U.S. National Institute of Standards and Technology (NIST) started soliciting comments on what such a cryptographic system could look like, resulting in draft standards being published in August of this year.

But even if a standard achieved universal acceptance as something that would be unbreakable by a quantum computer, that wouldn't be enough to completely solve the issue. As NCSC writes: "Migration to PQC requires more than just new algorithms."

Whole "protocols and services need to be re-engineered, because PQC typically places greater demands on devices and networks than traditional [public-key cryptography]."

Upgrading major internet services is likely to be one of the easier aspects of the transition, but legacy and sector-specific protocols such as those used in critical national infrastructure (CNI) is likely to be a significant challenge, because PQC requires more resources than public-key cryptography and much CNI is dependent on "devices with constrained resources, and on legacy systems that are hard to upgrade."

The owners of these systems will need to plan for the PQC transition "as a part of scheduled technology refresh cycles," but the good news is that for the majority of individuals and organizations relying on major service providers, the transition is largely expected to happen behind the scenes "because of the years of work already done by cryptographers, software engineers, hardware designers, security architects, and many other cyber security specialists worldwide."

16.UK NCSC issues new guidance on post-quantum cryptography migration

by Michael Hill

https://www.csoonline.com/article/658650/uk-ncsc-issues-new-guidance-on-post-quantum-cryptography-migration.html

The UK National Cyber Security Centre has refreshed its guidance to help system and risk owners plan their migration to post-quantum cryptography (PQC).

The UK National Cyber Security Centre (NCSC) has published updated guidance to help system and risk owners plan their migration to post-quantum cryptography (PQC). The guidance builds on the NCSC 2020 white paper Preparing for Quantum-Safe Cryptography and includes advice on algorithms choices and protocol considerations following the availability of draft standards from the US National Institute of Standards and Technology (NIST).

The point at which quantum computers will be capable of breaking existing cryptographic algorithms such public-key cryptography (PKC) - known as "Q-Day" - is approaching. It's a juncture that's been discussed for years, but with advancements in computing power, post-quantum threats are becoming very real. Some security experts believe Q-Day will occur within the next decade, potentially leaving all digital information vulnerable under current encryption protocols.

PQC is therefore high on the agenda as the security community works to understand, build, and implement cryptographic encryption that can withstand post-quantum threats and attacks of the future. There have been multiple notable initiatives, programs, standards, and resources launched this year to help the creation/development of and migration to PQC.

In August, NIST published draft PQC standards that are designed as a global framework to help organizations protect themselves from future quantum-enabled cyberattacks. The standards were selected by NIST following a seven-year process that began when the agency issued a public call for submissions to the PQC Standardization Process. NIST again called for public feedback on three draft Federal Information Processing Standards (FIPS), which are based upon four previously selected encryption algorithms.

Migration to PQC requires more than just new algorithms

Migration to PQC requires more than just new algorithms - protocols and services need to be re-engineered, because PQC typically places greater demands on devices and networks than traditional PKC, wrote John H, head of crypt research at the NCSC. "This is especially true of the amount of data that needs to be communicated between parties using PQC to secure their communications." International bodies have been working to update protocol standards in parallel with the development of algorithm standards, which is enabling test deployments of PQC by major service providers to understand the potential impacts of the transition, John H added.

While not straightforward, upgrading many major internet services (and the apps that access those services) will likely be one of the "easier" parts of PQC transition, John H said. "Many legacy and sector-specific protocols, including those used in critical national infrastructure (CNI) will also need to transition to PQC. Additional challenges in these use cases include having to run cryptography on devices with constrained resources, and on legacy systems that are hard to upgrade."

Implications of PQC migration for users and system owners

For users of commodity IT, such as those using standard browsers or operating systems, the switchover to PQC will be delivered as part of a software update and should happen seamlessly (ideally without end-users even being aware), the NCSC's updated guidance stated. To ensure devices are updated to PQC when it is available, system owners should ensure they keep devices and software up to date. "System owners of enterprise IT, such as those who own IT systems designed to meet the demands of a

large organisation, should communicate with their IT system suppliers about their plans for supporting PQC in their products," it added.

For a minority of systems with bespoke IT or operational technology, such as those that implement PKC in proprietary communications systems or architectures, choices will need to be made by system and risk owners as to which PQC algorithms and protocols are best to use, the NCSC said. "Technical system and risk owners of both enterprise and bespoke IT should begin or continue financial planning for updating their systems to use PQC. PQC upgrades can be planned to take part within usual technology refresh cycles once final standards and implementations of these standards are available."

Choosing algorithms and parameters for your use cases

The following table gives the NCSC recommended algorithms, their functions, and specifications:

Algorithm	Function	Specification
ML-KEM	Key establishment algorithm	NIST Draft – FIPS 203
ML-DSA	Digital signature algorithm	NIST Draft – FIPS 204
SLH-DSA	Digital signature algorithm for use cases such as signing firmware and software	NIST Draft – FIPS 205
LMS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208
XMSS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208

"The above algorithms support multiple parameter sets that offer different levels of security," The NCSC wrote. The smaller parameter sets generally require less power and bandwidth, but also have lower security margins, it added. "Conversely, the larger parameter sets provide higher security margins, but require greater processing power and bandwidth, and have larger key sizes or signatures. The level of security required can vary according to the sensitivity and the lifetime of the data being protected, the key being used, or the validity period of a digital signature." The highest security level may be useful for key establishment in cases where the keys will be particularly long lived or protect particularly sensitive data that needs to be kept secure for a long period of time. The NCSC strongly advised that operational systems should only use implementations based on final standards.

Post-quantum traditional (PQ/T) hybrid schemes

Post-quantum traditional (PQ/T) hybrid scheme is one that combines one (or more) PQC algorithms with one (or more) traditional PKC algorithms where all component algorithms are of the same type, the NCSC wrote. For example, a PQC signature algorithm could be combined with a traditional PKC signature algorithm to give a PQ/T hybrid signature.

There are greater costs to PQ/T hybrid schemes than those with a single algorithm. "PQ/T hybrid

schemes will be more complex to implement and maintain and will also be less efficient. However, there may sometimes be a need for a PQ/T hybrid scheme, due to interoperability, implementation security, or constraints imposed by a protocol or system," according to the NCSC.

"If a PQ/T hybrid scheme is chosen, the NCSC recommends it is used as an interim measure, and it should be used within a flexible framework that enables a straightforward migration to PQC-only in the future. Technical system and risk owners should weigh the reasons for and against PQ/T hybrid schemes including interoperability, implementation security, and protocol constraints, as well as the complexity, cost of maintaining a more complex system, and the need to complete the migration twice, the NCSC added.

17.The Future of Encryption: Navigating Change with Crypto-Agility

by The Gurus
https://www.itsecurityguru.org/2023/11/03/the-future-of-encryption-navigating-change-with-crypto-agility/

“Agility” has been quite a buzzword recently. You will likely find it on most companies’ 5-year plan slide decks. Yet, there is one area where the ability to adapt quickly and efficiently makes a lot of sense-cryptography. In an age where the methods employed by cyber attackers are becoming increasingly sophisticated and the specter of quantum computing looms, the importance of encryption cannot be overstated. This has led to the rise of a concept enabled by technical capabilities, known as “crypto-agility,” or the ability to quickly adapt to an alternative cryptographic standard without making significant infrastructure changes.

Embracing Crypto-Agility

With advancements in encryption come new challenges. As encryption methods evolve, older algorithms may become susceptible to attacks. Crypto-agility, therefore, has emerged as the antidote to this vulnerability. At its core, crypto-agility empowers organizations to transition seamlessly between encryption techniques. Rather than relying solely on one method, crypto-agility advocates for strategic flexibility, allowing the swift adoption of newer, more secure crypto libraries. However, large organizations can have hundreds or thousands of keys, digital certificates, encryption, and other cryptographic assets that can expire or suddenly break. Most security teams are unaware of the types of encryptions they use, let alone which applications use them. They implicitly trust that embedded cryptographic systems will protect their networks. This strategy has proven to fail as the headlines pile up. It is time to extend zero-trust principles into the cryptographic ecosystem to know if the most fundamental layer of protection and confidentiality can fulfil its purpose when called upon. The first step to address these risks is to discover where the current cryptographic assets reside and assess their ability to withstand decryption attempts. Cryptographic discovery tools have been developed to create accurate inventories of all cryptographic instances, known and unknown, and analyze systems relying on cryptography to protect sensitive assets, including web servers, hosts, applications, networks, and cloud systems.

Proactive Resilience

The use cases of crypto-agility have soared in recent years. We could argue that it has even become a buzzword in the cybersecurity industry, although it is often misused. Even once impregnable encryption algorithms have succumbed to the relentless march of technological progress and ingenious hacking

techniques. Organizations lacking crypto-agile strategies were exposed to preventable attacks, prompting industry juggernauts to partner with crypto-agility solution providers. Steering away from static cryptographic management models requires robust tooling capable of integrating with a comprehensive set of environments such as networks, servers and applications but also with certificate management solutions, threat management suites and EDR technologies, among others. Crypto-agility platforms are being developed to empower cybersecurity teams to add crypto-agility capabilities to their security tech stack. For example, large financial institutions are increasingly integrating InfoSec Global Crypto-Agility Management Platform with industry-leading agent management tools like Microsoft Sentinel or CrowdStrike Falcon. Adopting a crypto-agility framework allows organizations to accommodate future changes but also comply with strict standards, like the Payment Card Industry Data Security Standard (PCI DSS), guiding payments industry stakeholders to ensure safe payments worldwide.

Emerging Encryption Trends

Encryption technology is on a transformative journey, reflecting the need for robust data protection. Traditional symmetric and asymmetric encryption techniques now share the stage with ground breaking innovations such as homomorphic and post-quantum encryption. However, switching from legacy encryption to recommended algorithms tends to be exceedingly expensive and error prone. After a year OpenSSL experienced an implementation error that led to the Heartbleed vulnerability, half of U.S. organizations still had not patched all their OpenSSL instances. This is because cryptographic assets are deeply embedded into software, rendering them extremely difficult to change.

Another growing segment comes from the proliferation of Internet of Things devices. Securing IoT devices throughout their lifespan can be particularly challenging as their encryption is baked in when manufactured. With crypto-agility, your new electric car will be updated to mitigate risks thanks to a crypto-agile middle layer at the chip level allowing it to update its cryptographic assets.

Conclusion

Without crypto-agility, applications must either be reconfigured locally or recoded to enable the implementation of new quantum-safe algorithms. Neither one is a good option. To prevent security issues that can halt major networks' operations and cause Global 1000 to shell out millions to ransomware attackers, leading standard bodies are working hard to identify which digital signature schemes, hash algorithms, block ciphers, and other encryption methods to approve for standardization. Legislators worldwide are also increasingly promulgating their own encryption standards, which puts additional pressure on organizations to become crypto-agile to comply to different market regulations.

18.UK Banks Warn Quantum Will Imperil Entire Payment System

by Phil Muncaster
https://www.infosecurity-magazine.com/news/uk-banks-quantum-imperil-entire/

The UK finance industry has warned that quantum computing could unravel the security used to protect the country's entire payment system.

Banking body UK Finance issued the warning in a new report published this week: *Identifying and Minimising the Risks Posed by Quantum Technology.*

Quantum computing is still in development, but if viable computers can be built using the technology, they could use Shor's algorithm to crack the asymmetric (PKI) encryption used by the finance industry, rendering it practically useless.

These warnings are not new, but the banking industry is now lending them an added urgency, calling on industry and government to collaborate more closely on a post-quantum future.

"We cannot ignore the risks … and the reality that when a Cryptographically Relevant Quantum Computer is developed, it could break the encryption underpinning all payments and electronic commerce," warned Jana Mackintosh, managing director of payments, innovation & resilience at UK Finance.

"We must be ready. Industry and government must work together now to secure the financial services industry against these threats, and put the UK at the head of the pack to seize the opportunities."

Other quantum risks highlighted by UK Finance include:

- Possible market instability caused by unequal access to the technology
- Insufficient skills in the UK
- The technological debt accrued from legacy systems
- Multiple environmental considerations associated with quantum technology

However, the industry body released a second report in tandem with the first, outlining the multibillion-pound opportunity that quantum technology offers the financial services sector.

To address both opportunity and risk, UK Finance set out seven recommendations for government:

- Establish a quantum-safe taskforce to help the transition to technology capable of withstanding security threats in the new quantum era
- Be vigilant of other nations' work to develop quantum technology, and encourage the private sector to transition to quantum-safe technologies
- Grow the quantum workforce
- Encourage UK supervisory authorities to start their quantum-safe journey now
- Develop targeted sector-specific roadmaps with support from the National Cyber Security Centre (NCSC)
- Establish a quantum computing taskforce for monitoring advances in the technology and identifying relevant use cases
- Encourage firms to invest in quantum computing training and education for their workforce

19.Keeping secrets in a quantum world

by Neil Savage
https://www.nature.com/articles/d41586-023-03336-4

In July 2022, a pair of mathematicians in Belgium startled the cybersecurity world. They took a data-encryption scheme that had been designed to withstand attacks from quantum computers so sophisticated they don't yet exist, and broke it in 10 minutes using a nine-year-old, non-quantum PC.

"I think I was more surprised than most," says Thomas Decru, a mathematical cryptographer, who worked on the attack while carrying out postdoctoral research at the Catholic University of Leuven (KU Leuven) in Belgium. He and his PhD supervisor Wouter Castryck had sketched out the mathematics of the approach on a whiteboard, but Decru hadn't been sure it would work — until the pair actually ran it on a PC. "It took a while for me to let it sink in: 'Okay, it's broken.'"

The encryption scheme, dubbed SIKE, was designed for the ambitious purpose of keeping secrets secret. It was one of four finalists chosen in 2022 for potential adoption by the US National Institute of Standards and Technology (NIST) in its Post-Quantum Cryptography standardization process. The aim is to find algorithms that can safeguard private information from the looming threat of quantum computers.

The world's digital information relies on encryption to keep it secure. Hard drives containing medical data are encrypted, as are the secrets held by national militaries and intelligence agencies. Online credit-card payments, digital signatures, readings from smart meters, the computers in driverless cars and the chips in passports all depend on algorithms, developed in the 1970s, that turn easy-to-read data into encrypted ciphers accessible only to those with a mathematical 'key' to unlock them. Those algorithms, in turn, depend on mathematical functions that are straightforward to use to create keys, but difficult to run in reverse to reveal them: the mathematical equivalent of frying an egg.

If practical quantum computers arrive, however, these hard-to-solve problems will suddenly become child's play. RSA, an encryption scheme that allows systems to share keys, could take a classical computer most of the lifetime of the Universe to reverse-engineer. A quantum computer, researchers estimate, could do the same job in 8 hours. The Diffie–Hellman key exchange, another widely used cryptographic method, named after its two inventors, could also be easily reversed by a quantum machine. A different type of scheme, the Advanced Encryption Standard, is not considered to be under serious threat by computational advances, but it's often used in conjunction with the other methods and can't replace their secret-keeping abilities.

Whereas classical computers work on ordinary digital bits of ones and zeros, quantum computers use quantum bits, or qubits. These units take advantage of a quantum-mechanical property called superposition, which allows a qubit to be, for example, 70% '1' (on) and 30% '0' (off) at the same time. The ability to be in many states of partially on and partially off at once lets a quantum computer perform complicated mathematical operations much faster than even the most sophisticated classical computer could. This characteristic brings eon-spanning calculations within easy reach.

Existing quantum computers contain a handful of qubits — a few hundred at most — and have limited capabilities. The global technology firm IBM plans to release a chip with 1,121 qubits sometime this year, and says it will have a computer with more than 4,000 qubits by 2025. Scientists from Google and the Swedish National Communications Security Authority estimated in 2021 that 20 million qubits would be necessary to crack an RSA key of 2,048 bits, a commonly used key length. "The big question is, of course, whether all of the efforts to make quantum computing practical will have any cryptanalytic benefits," says Ronald Rivest, a computer scientist at the Massachusetts Institute of Technology in Cambridge — and the R in RSA, which he developed with fellow computer scientists Adi Shamir at the Weizmann Institute of Science in Rehovot, Israel, and Leonard Adleman at the University of Southern California in Los Angeles. "It still is very much an open question."

But even if practical quantum computers aren't built for another 20 years, the problem is urgent today, researchers say. "Your data could already be lost to a future quantum computer, even though one hasn't

been built," explains Dustin Moody, a mathematician in NIST's Computer Security Division, who leads the Post-Quantum Cryptography project. Spy agencies or cybercriminals could collect encrypted data now and simply wait for the technology to catch up. Many researchers think that countries such as China and the United States are doing just that.

In case practical quantum computers do arrive, cryptographers and standards bodies around the world are working to come up with a set of encryption techniques that will be as hard for a quantum computer to unravel as existing schemes are for classical computers. To do that, many researchers are putting the latest algorithms to the test.

Broken keys

Breaking SIKE earned Decru and Castryck a US$50,000 reward from Microsoft for winning the SIKE Cryptographic Challenge. Once the pair had announced their findings, other groups quickly found ways to unscramble the codes even faster. This wasn't the first futuristic algorithm of NIST's to fall. Another candidate, called Rainbow and based on a different mathematical approach, had been broken five months earlier — in a single weekend — by Ward Beullens, a postdoctoral researcher at IBM Research Zurich in Rüschlikon, Switzerland.

Testing such potentially quantum-resistant algorithms to their breaking point is the aim of a multi-year competition that NIST has been running to develop post-quantum cryptography schemes. "The strongest will survive," says Moody. "Sometimes they look promising, but over the years, they wither out and we say, 'Okay, we've gone as far as we can in that direction. We have to have some new ideas.'"

Of 69 candidate algorithms chosen in late 2017, between 25 and 30 have either been broken entirely or suffered some significant attack, Moody says. In late August this year, NIST published draft standards for three of the remaining algorithms and invited public comment. The agency plans to finalize the standards sometime in 2024.

Of these three algorithms, one — CRYSTALS-Kyber — is designed for general-purpose encryption and the exchange of public keys that protect shared data. The other two, CRYSTALS-Dilithium and SPHINCS+, are used to secure digital signatures, which ensure that a person providing a document is who they say they are. A draft standard for another algorithm for digital signatures, Falcon, is also set to be published by NIST in 2024, and 40 more digital-signature candidates were collected in July, after the agency sent out a call for a new round of submissions. "They are sort of sending the message that they are not happy with the three that they have," says Tanja Lange, a cryptographer who heads the coding theory and cryptology group at Eindhoven University of Technology in the Netherlands, and who contributed to the development of SPHINCS+.

Tapping extra information

Any cryptography system has to be more than just a hard-to-solve mathematical problem. It also has to allow some way of sharing information about the problem with the person who needs to decode it. And that introduces vulnerability. "There's this game that always has to be played in cryptography," Castryck explains. You have to have a hard problem on which to build a crypto system, "but there's always extra information that is passed along just to make the scheme work".

The SIKE system was based on an isogeny, which is a map showing how points on an elliptic curve correspond to points on another such curve. Unlocking SIKE requires finding the right map between 2 random curves out of at least 2^{434} such curves — a number so huge there's no word for it in English, and something that should be almost impossible without a key, even for quantum computers. To share a key with the recipient of an encoded message, each sender has to provide information about two points along one of the curves. Castryck and Decru were able to use that extra information about the points to

reconstruct the map, and could therefore break the code without actually solving the hard mathematical problem.

Isogeny as the basis for a cryptographic scheme is not dead, but it's on shaky ground, says Decru, now at the Université Libre de Bruxelles in Belgium. The pair's attack on SIKE does not affect NIST's other proposed standards, which use different mathematical approaches. Two are based on structured lattices, a kind of repeating grid. The hard mathematical problem is to determine how parts of the grid relate to each other. SPHINCS+ is based on hash functions, which take a string of numbers and convert it into a shorter string that forms a recognizable fingerprint of the original. Hash functions are not reversible, so they're easier to create than other approaches are, but because of their one-way nature, they can only be used for signature verification, not for trading cryptographic keys.

Putting cryptographic algorithms to use in a way that balances the competing demands of security and efficiency is another challenge when it comes to making data safe in a quantum world, Castryck says. Longer keys are more secure, because there are more possible solutions to a problem, thus increasing the difficulty of finding the right one. But that also increases the time and computing bandwidth required to generate and transmit the key. "Industry is not asking for a very secure crypto system that takes one hour for a single key exchange," Castryck says.

Attacks from the side

Peter Schwabe, a cryptographic engineer at the Max Planck Institute for Security and Privacy in Bochum, Germany, is investigating how to protect cryptographic schemes from side-channel attacks. In an attack of this kind, an adversary gathers information from a computer that is not part of the key itself but could provide hints to it. In classical computing, for instance, sending messages to a server and measuring the time it takes to get a response could reveal whether a given bit is a '1' or a '0', or the power usage might vary according to the structure of the cryptographic key. The attacker can use these clues to piece the key together. Or, if the attacker can place some spyware on a server, they might be able to learn what this server is doing by measuring its demand on resources such as memory.

In August, the multinational tech giant Intel released a firmware patch for several brands of chip it has sold since 2015, after Daniel Moghimi, a security researcher at Google in San Diego, California, discovered what he named the Downfall vulnerability. It exploits the way in which the chips speed up the process of gathering data scattered through their memory. An attacker with access to the chip sends requests to encrypt random data, then collects some low-level information that leaks from the process. The attacker can analyse that information and look for patterns, which can eventually be used to piece together the encryption key the system is using.

Although the specifics of the attack will vary with the particular encryption scheme, there is nothing in post-quantum cryptography that inherently rules out such attacks. "One goal of this project is to figure out how we can systematically protect these new crypto systems against these kinds of attacks," Schwabe says.

NIST isn't the only group that is working on cryptographic standards. The German Federal Office for Information Security also provides recommendations about which systems to use. These include two standards that didn't make NIST's final cut. One is FrodoKEM, a key- encapsulation scheme based on lattices. The other is Classic McEliece, which uses error-correction codes that are hard to reverse. Both are considered to be more secure than the NIST proposals, but they involve longer keys, and are thus slower to use.

Other standards organizations are likely to weigh in as well. For example, the Internet Engineering Task Force does not recommend particular cryptography standards, but will have a say in the protocols that incorporate them. Between 2018 and 2019, the Chinese Association for Cryptologic Research held its own competition for new algorithms. The submissions involved the same families of mathematical prob-

lems as those in the NIST proposals, and the chosen winner was based on structured lattices.

In the end, there will have to be a small set of internationally agreed standards. “The simple reason is that when you want to do Internet communication, both ends need to speak the same cryptography,” Schwabe says. And large international companies will also have a role. For instance, Google announced in August that it was incorporating Kyber into its Chrome browser. “If Google implements key agreement with Kyber, then everybody who wants to speak to Google needs to speak Kyber, no matter where they’re sitting in the world,” Schwabe says.

It will take time to implement the NIST standards and to spread them, or similar approaches, to computer systems around the world. Meanwhile, cryptographers will keep trying to develop algorithms, and attempting to break those that already exist. But the threat that data could be collected now and decrypted at a later stage means that the issue is urgent, and the sooner the world adopts post-quantum cryptography, the better, Decru says. “Whether the quantum computer exists in 20, 30 or 40 years, we don’t know,” he says. “But I don’t think there’s time to waste on that front, really.”

20.Six Steps to Prepare for Post-Quantum Cryptography

by Christian Simko
https://www.appviewx.com/blogs/6-steps-to-prepare-for-post-quantum-cryptography/

Preparing for post-quantum cryptography is essential to ensure the security of digital communications and data ahead of when quantum computers can potentially break current today’s cryptographic algorithms. Here are six steps to help you to start preparing for post-quantum cryptography:

1. **Assessment and Awareness**: Start by assessing your organization’s current cryptographic infrastructure and understanding the potential risks posed by quantum computing. Use the assessment to build an inventory of cryptographic assets to raise awareness among key stakeholders about the importance of post-quantum cryptography and potential impact on your security posture.

2. **Stay Informed**: Keep up-to-date with the latest developments in post-quantum cryptography. The field is rapidly evolving, and new algorithms and techniques are continually being researched and progressing through standardization efforts. Participate in relevant conferences, read research papers, and engage with the cryptographic community to stay informed.

3. **Identify Critical Systems and Data**: Identify the critical systems and data that may be at risk from quantum attacks. This includes assessing the cryptographic protocols used to protect sensitive information, such as SSL/TLS for securing web applications and providing encryption. Determine which systems and data need to be prioritized and protected using post-quantum cryptography.

4. **Implement Transition Plans**: Develop a transition plan for upgrading your cryptographic infrastructure to post-quantum algorithms. This may involve replacing or updating existing encryption methods with quantum resistant algorithms. Be prepared to update hardware and software systems, as well as Public Key Infrastructure (PKI) protocols and policies, to accommodate these new cryptographic algorithms.

5. **Engage with Standards Bodies**: Participate in standards development organizations (SDOs) and

consortia that are working on standardizing post-quantum cryptographic algorithms. For example, NIST (National Institute of Standards and Technology) is leading efforts in this area. By engaging with SDOs, you can help shape the standards and ensure interoperability with other organizations.

6. **Implement Crypto-Agility:** The ability to quickly switch between cryptographic algorithms will be essential to ensure a rapid response against cryptographic threats. Choosing an enterprise certificate lifecycle management automation solution to provide visibility and control can provide a path to crypto-agility today.

Here are some additional things to consider:

- **Quantum-Safe Certificate and Key Management**: Explore quantum-safe certificate and key management solutions to protect these cryptographic assets from quantum attacks. This may involve using quantum-resistant key exchange algorithms and implementing robust certificate and key management practices.

- **Education and Training**: Invest in educating your IT and security teams about post-quantum cryptography. Ensure that your staff is well-versed in the principles and best practices associated with quantum-resistant cryptographic algorithms.

- **Testing and Validation**: Conduct thorough testing and validation of any new cryptographic solutions before implementing them in production. Ensure that they provide the expected level of security, do not introduce vulnerabilities, and do not break existing processes.

- **Budget and Resource Allocation**: Start allocating the necessary budget and resources to support the transition to post-quantum cryptography. This may include funding for research, development, and infrastructure upgrades. Do not let this slip to the last minute when it is harder to request emergency funding.

Preparing for post-quantum cryptography is a long-term effort, and it's essential to start early to ensure the security of your organization is properly protected from the impending threats quantum computing will expose with today's encryption algorithms.

21.How quantum computing could transform the banking sector

by Alex Clere
https://fintechmagazine.com/articles/how-quantum-computing-could-transform-the-banking-sector

It's an emerging technology often overlooked in favour of en vogue innovations like AI and cloud. How might quantum banking change the financial system?

Quantum banking is, perhaps, one of the least championed trends within financial services today – yet it still has the potential to have a significant impact on the financial system.

It revolves around quantum computing and blockchain to build a faster payments mechanism that is also cheaper to operate, because it removes the so-called middlemen who have often been needed in traditional peer-to-peer payments.

What is quantum computing and how does it work?

Suhail Bin Tarraf, Group Chief Operations Officer at First Abu Dhabi Bank, says: “Computers today use bits to run operations, however a quantum computer uses qubits to perform multidimensional algorithms in real time. Just like classical bits, a quantum bit must have two separate states: one representing 0 and one representing 1.

“However, a quantum bit can also exist in states of superposition, be subjected to incompatible measurements, and be intertwined with other quantum bits – creating a multitude of unique combinations. The recent developments in harnessing these unique traits makes qubits much more powerful than classical bits.”

Duke Munoz, Sales Representative at TechEniac, continues: “In quantum computing, 0 and 1 can coexist, or even intertwine, leading to a multitude of calculations even with the same input.

“This revolutionary technology has enabled a more secure, efficient, and counterfeit-resistant financial system, making it a promising development in the world of finance.”

Indeed, so promising is it that MarketsandMarkets forecasts the global quantum computing market to reach US$1.77bn by 2026, up significantly from US$472m in 2021, recording a compound annual growth rate in excess of 30%. If adopted correctly, financial services could be one of the biggest proponents of quantum computing, benefitting from this value creation in the process.

Speed a considerable advantage of quantum banking

One of the most considerable advantages that quantum banking provides over alternative methods of banking and moving money is the increased speed. Quantum computing can process data 10 million times faster even than supercomputers, highlighting the astounding capacity that this emerging technology possesses.

The authors of an IBM report into quantum banking explain the technical advantages that lurk beneath the hood: “The solution space of a quantum computer is orders of magnitude larger than traditional computers – even immensely powerful ones. That’s because doubling the power of a classical computer requires about double the number of transistors working on a problem. The power of a quantum computer can be approximately doubled each time only one qubit is added.”

This system in turn provides powerful advantages to financial institutions and other players within the banking space – and it’s not going unnoticed by the industry. A recent report published by Temenos surveyed 300 executives across retail, commercial and private banking around the world. Among other things, it found that 63% of executives thought new technologies – including quantum computing – would have the biggest impact on banks in the next five years, compared to just 34% for the next most popularly cited trend: changing customer behaviours.

This figure is a couple of percentage points lower than it was two years ago, suggesting a slight COVID-19 tempering of expectations, but significantly higher than it was in 2019 – the last full year unaffected by the pandemic – with just 42% of executives surveyed as part of Temenos’ 2019 research saying that these technologies would be the biggest driver of change.

Speaking at the time the research was released, Jonathan Birdwell, Global Head of Policy and Insights for Economist Impact, which conducted this survey on behalf of Temenos, claimed that banks were aware of the onus that these expectations placed upon them: “New technology and customer demands are the top two trends expected to impact banking in the next five years. To maintain their direct connection with the consumer, banks are recognising that they must become true digital ecosystems.”

Risk management among other quantum use-cases

Another significant use-case for quantum banking lies around risk, which continues to be an operational tug-of-war for banks of all sizes. Quantum computing can perform operations magnitudes quicker, meaning complex financial information – such as the data that goes into assessing credit risk, for example – can be analysed quickly and with more accuracy.

A study published earlier this year by Ernest & Young (EY) highlights the complex risk landscape that banks are operating in: it claims that CROs face an extraordinary volume and variety of risks, both traditional and emerging, which all seem to be growing in urgency. Yet their biggest challenge lies in understanding how these risks intersect with each other to create potential points of failure within their organisation, even when traditional risk management metrics look stable.

“Cyber risk is the top risk priority for the next 12 months, according to CROs,” the study says. “But credit risk may soon become more of a focal point if economic conditions worsen.” Clearly, then, this necessitates improved technology to help financial institutions manage the plethora of risks they face on a daily basis. Could quantum banking be a solution?

First-movers will secure an early advantage

Authors of a report from UK Finance previously wrote: “Quantum computing will have applications across financial services, transforming the way we approach investment, risk, AI and security and offering financial services firms that seize the opportunities an early advantage.

“Financial services firms should be considering how they prepare for the quantum computing technology that looks certain to transform the market. Failing to do so risks others developing the ability to move faster in the short term and to attract the resources that will be essential for long-term success.”

Suhail Bin Tarraf, Group Chief Operations Officer at First Abu Dhabi Bank, continues: “Outside of risk management, quantum supercomputing will lead to a range of banking capabilities, such as analysing large areas of unstructured data to make financial predictions or simulate investment portfolios. It will lead to a greater understanding of financial markets and economic booms or busts as well as management of asset allocation.

“Experts believe that the commercialised use of quantum computing is still about a decade away. Scalability, cost, maintenance, legacy technology, and regulatory scrutiny are a few of the challenges in store for banks. However, early movers are likely to have an advantage and the chance for gaining a competitive foothold will not be free for long.”