Crypto News

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

September 05, 2024

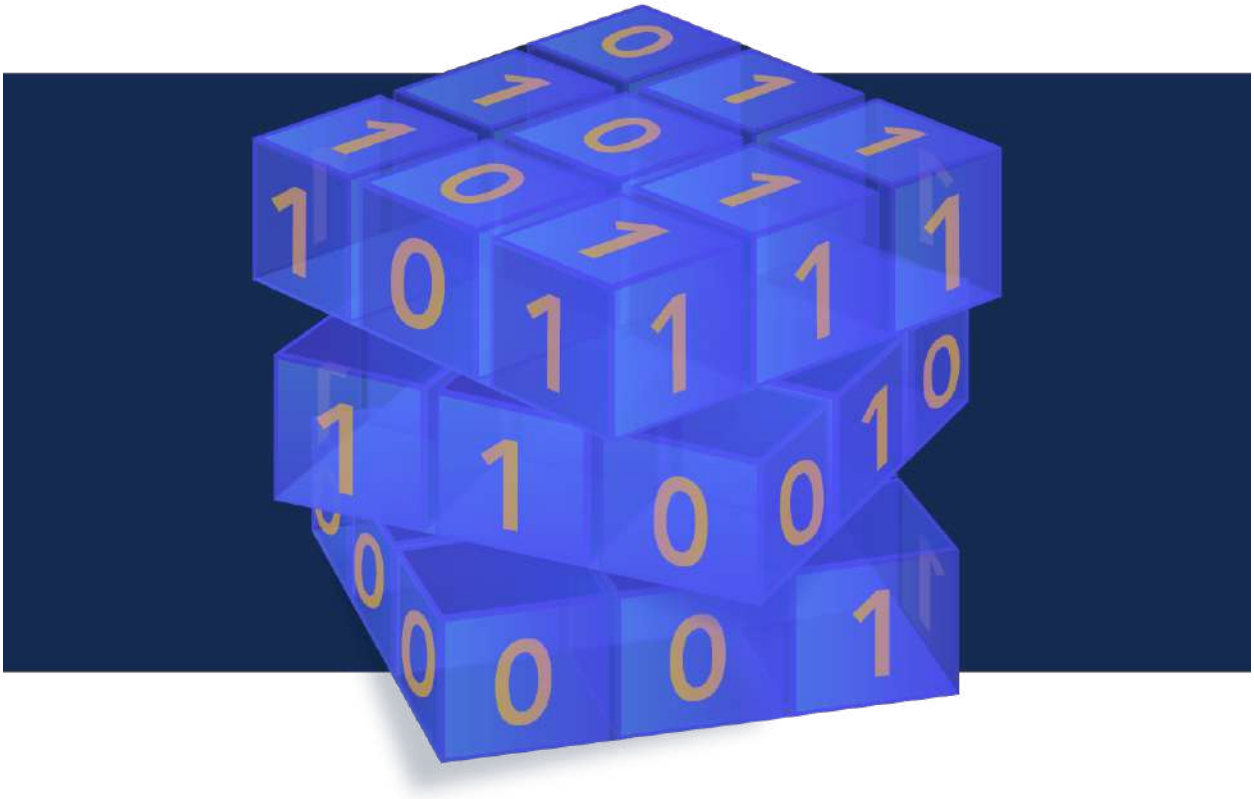


TABLE OF CONTENTS

Editorial

This month it's all about Post-Quantum Cryptography (PQC) and rightfully so. With the release of NIST FIPS 203, 204, and 205 on August 13th, organizations now have guidance on the quantum-safe cryptography their organizations can start implementing based on their business needs. However, this will not be an easy migration. Unlike the upgrades of the 1990's and 2000's where one algorithm was being upgraded such as DES to 3DES to AES or SHA-1 to SHA-2, this time it's two. Organizations will need to upgrade the asymmetric algorithms AND the hashing function. If you were in this space during those upgrades of the 1990's and 2000's mentioned above, you'll remember that those upgrades were far from simple in terms of manual labor and the staff with the right skillset to make it all happen. Is your organization crypto-agile enough to take on such a monumental upgrade? If you're not sure, make your way to article 1 to learn more about what's coming with Cryptographically Relevant Quantum Computers (CRQCs) and if you're ready to take on the challenge. Heed this warning, "if you fail to prepare, you will prepare to fail."

You'll also want to read the article I released with the CSA on August 15th here (https://lnkd.in/d5Nng4dM) to get an overview of FIPS 203, 204, and 205 along with a brief history of how we got here and next steps your organization can take to kick off your post-quantum journey.

Still not convinced your organization needs to implement PQC? Apple and Google are already moving towards it. Apple made its move concerning quantum-safe cryptography by introducing iMessage with PQ3 earlier this year. Google then released a quantum-resistant encapsulation mechanism to protect Chrome TLS traffic. The concern now is that the supply chains, vendors, and others in the tech world will also need to adopt PQC timely. Otherwise, there can and will be compatibility issues. Your business will not want to be one of those businesses who didn't start preparing soon enough and is left in the dust. Navigate to article 23 to learn more about what's coming. There are so many other articles of note in this edition that you won't want to miss so make sure you find a comfortable chair and take it all in in this edition of Crypto News. Until next time readers!

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.

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.Quantum Computing and the Risk to Classical Cryptography

by Dr. Angelique Faye Loe
https://www.appviewx.com/blogs/quantum-computing-and-the-risk-to-classical-cryptography/

The recent standardization of first three post-quantum cryptography (PQC) encryption and digital signature algorithms by the U.S. National Institute of Standards and Technology (NIST) has officially kicked off the race to PQC readiness. In its PQC press release, NIST cites predictions that within the next decade, a cryptographically-relevant quantum computer (CRQC) capable of running Shor's algorithm will pose a significant risk to classical cryptography because it will have the ability to efficiently solve problems that are currently infeasible for classical computers.

Shor's algorithm running on a CRQC will be capable of factoring large integers and computing discrete logarithms over finite fields and elliptic curves. This capability will undermine the security of widely-used asymmetric cryptographic algorithms used for encryption and digital signatures such as ECDH, RSA, ECDSA, and EdDSA.

Currently, classical cryptographic algorithms are ubiquitous and have a function to protect the confidentiality and integrity of digital data in code, development pipelines, network protocols, and applications running on end-user system and servers.

To address the risks posed by a CRQC, the three PQC standards approved by NIST provide algorithms to handle encryption and digital signatures which are considered quantum-resistant. However, due to the extensive use of classical asymmetric algorithms across various use cases and complex systems, the transition will require the correct engagement of people, processes, and tooling to be successful. The scale and complexity of this transition to quantum-resistant algorithms will be several orders of magnitude greater than previous cryptographic algorithm upgrades.

In this article we provide the relevant background and motivation to why PQC migration is now an essential consideration for CISOs and we also demonstrate how this migration strategy dovetails into other competing priorities.

Crypto-Agility vs 'Crypto-Fragility'

Crypto-agility is an organization's ability to transition to new cryptographic standards and algorithms in response to new security threats.

Historical cases point to crypto-agility being an overly optimistic property for a system to possess. One of the largest cryptographic upgrades in the late 1990s and early 2000s was the replacement of IBM's Data Encryption Standard (DES).

DES was broken in the late 1990s mainly through the use of brute-force attacks. The upgrade to Triple DES (3DES) allowed certain configurations to be backward-compatible with DES through the reuse of the secret key. Furthermore, in 2001 the Advanced Encryption Standard (AES) was standardized by NIST and was promoted to be the preferred replacement for DES.

DES was widely used in Automated Teller Machines (ATMs) – often implemented in hardware. Therefore, 'crypto-agility' in certain use cases meant physical hardware replacements of susceptible hardware.

More recently, the Secure Hashing Algorithm 1 (SHA-1) was no longer accepted on commercial web browsers using TLS certificates in 2017. TLS certificates were required to use the SHA-2 algorithm as a replacement to SHA-1. The motivation behind this hashing algorithm upgrade was due to a clear risk of a plausible attack on SHA-1 known as a collision attack being identified in 2011. A seasoned CISO will recall the resource intensive task of replacing these certificates throughout their organizations.

The commercial web browser vendors were not crying wolf. In 2017, a collision attack was realized by researchers at CWI and Google on two PDF files, SHAttered.

In both instances of DES replacement and SHA-1 replacement, crypto-agility was not feasible in practice. With DES, labor intensive hardware upgrades were needed in various use cases. With SHA-1, without highly mature Certificate Lifecycle Management (CLM) at the time, the task of identifying and upgrading TLS certificates was manual, slow and resource intensive.

Without crypto-agility CISOs are faced with the opposing reality of 'crypto-fragility'. **Crypto-fragility is marked by two characteristics:**

1. Not having clarity about the systems which host the vulnerable cryptography (lack of measurement)

2. Not having the people, processes, and tooling to upgrade the cryptography efficiently (lack of management)

Why PQC Migration is Inherently More Complex

There are many more algorithms to upgrade across machines, applications, workloads and cloud services across more complex hybrid multi-cloud environments.

The DES upgrade to 3DES and ultimately to AES was the replacement of a symmetric algorithm. The SHA-1 upgrade to SHA-2 was the replacement of a hashing algorithm. With the new NIST PQC standards, there are requirements to replace not only the asymmetric algorithm, but also auxiliary functions, such as the hashing function.

Therefore, for PQC migration, two algorithms will need upgrading, namely the main asymmetric algorithm and the hashing algorithm, as compared to one algorithm in the case of DES, namely the replacement of a symmetric algorithm, and SHA-1, namely the replacement of the hashing algorithm.

Size Requirements

When DES was first upgraded to 3DES, the key size went from 56-bits to 112-bits or 168-bits. This marked a two or three times larger key size for an upgrade. This step change in key sizes, made adoption in the field challenging. When SHA-1 was upgraded to SHA-2 the key size went from 160-bits to 256-bits, a 1.6 times increase in size.

By way of example, let us consider the upgrade of the ECDSA algorithm to ML-DSA. Upgrading a 32-byte public key would require at minimum for the ML-DSA-44 algorithm a 1312-byte public key. This is a 41 times increase in

Furthermore, if we chose to adopt the SLH-DSA-SHAKE-128s algorithm, although the public key size is comparable to the ECDSA key size, the minimum signature size is 7856-bytes, this is a 123 times size increase when compared to an ECDSA 64-byte signature.

Clearly the scale and complexity of a PQC migration must not be underestimated. Even less complex historical examples of cryptographic algorithm updates presented challenges. Therefore, it is a fair assumption to make that PQC migrations will pose greater difficulties than previously encountered.

If You Fail to Prepare, You Will Prepare to Fail

The key to any successful migration project is preparation. In this section, we provide insight to why early preparation for successful PQC migrations is essential.

The Importance of Mosca's Theorem

Mosca's Theorem provides a simple formula to identify the timeframe required to adopt quantum-resistant algorithms to reduce the risks to confidentiality and integrity of your digital data. Learn more about Mosca's Theorem here.

The formula is as follows: if $x + y > z$, then you have a risk of your confidential data being exposed due to the risk of a CRQC. Where x is the number of years you need to keep the organizations data safe, y is the number of years required to adopt quantum-resistant algorithms, and z is the number of years for a CRQC to be accessible.

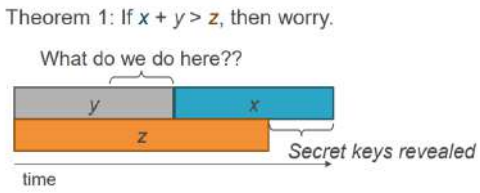


Figure 1: Illustration of Mosca's Theorem from page 21 of Mosca's 2015 presentation: Cyber security in a Quantum World: Will We be Ready?

This less mathematical example is more practical approach to demonstrate the urgency of a PQC migrations to other decision makers within you organization

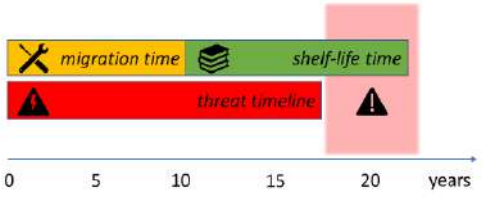


Figure 2: Illustration of *Mosca's Theorem* reproduced from Figure 1 of the Global Risk Institute's 2021 full Quantum Threat Timeline Report by Mosca and Piani.

As a CISO, you are the custodian of your organization's data. Therefore, you have very little control over variable x. Also, unless you are working for a leading research and development company focusing on the advancements in quantum-computing, you also have very little control over variable z. However, where you do have control is on variable y, the time it will take to adopt PQC for the relevant digital data assets in your organization.

Accordingly, it is in your organization's best interest with you as the leader of the cybersecurity team and strategies, that you progress with the planning and preparation for migrating to quantum-resistant algorithms as soon as possible. Budgets, processes and resources will need to be in place to make this project a success.

Benefits of Starting PQC Migrations Now

In the NIST Cybersecurity Framework's (CSF) Five functions of Identify, Protect, Detect, Respond, Recover (IPDRR) (The CSF 1.1 Five Functions), early adoption of PQC fits into the Identify and Protect functions.

By measuring and identifying the systems vulnerable to a CRQC, you can then begin to understand the rough order of magnitude that will be required for migrating to quantum-resistant algorithms. This will also provide you with the ability to prioritize the correct systems and data for remediation based on Mosca's Theorem.

Also, by ensuring that protective controls are in place for the critical digital systems and assets in your organization, this can greatly mitigate the resources and costs associated with the Detect, Respond, and Recover functions. A proper defense-in-depth strategy focuses heavily on the initial first line of defense protection of assets.

To get started, crypto-agility is key and the first step is to gain full visibility into your crypto landscape. Without knowing what you have, it will be impossible to properly scope and plan your PQC migration strategy. An effective certificate lifecycle management (CLM) solution that can enable crypto-agility is a must for visibility, automation and control of all crypto assets in your PKI landscape.

To learn more about crypto-agility and certificate lifecycle management, request a demo of the AppViewX AVX ONE CLM solution.

2.India's DRDO Scientists Complete Testing of 6-Qubit Superconducting Quantum Processor

by Matt Swayne
https://thequantuminsider.com/2024/08/29/indias-drdo-scientists-complete-testing-of-6-qubit-superconducting-quantum-processor/?utm_source=newsletter&utm_medium=email&utm_term=2024-09-01&utm_campaign=TQI+Weekly+Newsletter+--+Google+Surfaces+QEC+Strategy+Juniper+Ventures+Quantum+Bridge+Plus+More+Quantum+News+Industry+Updates

Scientists from Defence Research and Development Organisation — DRDO — Young Scientists Laboratory for Quantum Technologies (DYSL-QT), Pune and Tata Institute of Fundamental Research (TIFR), Mumbai have completed end-to-end testing of a 6-qubit quantum processor based on superconducting circuit technology.

The demonstration was carried out in front of the apex committee overseeing the DYSL-QT. This included submitting a quantum circuit from a cloud-based interface, the execution of the programme on the quantum hardware and updating the cloud interface with computed results.

The project being executed at TIFR Mumbai's Colaba campus is a three-way collaboration between DYSL-QT, TIFR and Tata Consultancy Services (TCS). The DYSL-QT scientists put together the control and measurement apparatus using a combination of commercial off-the-shelf electronics and custom-programmed development boards. The qubits were designed and fabricated at TIFR and the quantum processor architecture is based on a novel ring-resonator design invented at TIFR. The cloud-based interface to the quantum hardware is developed by TCS.

The scientists are now working on optimising various aspects of the system performance before it becomes ready for operation. Plans are underway to provide wider access to this system for education, research and eventually as a test bed for testing superconducting quantum devices for analysis.

The next development target is to scale up the number of qubits and assess the scaling trends with respect to technology challenges, development effort/time and monetary resources required for development, operations & commercialisation of various sizes of quantum computers. This will involve a holistic view from the quantum theory to engineering to business feasibility.

3.FBI Wants More Access to Everything, Can't Be Bothered to Protect The Stuff it Already Has

by Tim Cushing
https://www.techdirt.com/2024/08/28/fbi-wants-more-access-to-everything-cant-be-bothered-to-protect-the-stuff-it-already-has/

The FBI has been pulled right up to the national security table for years. Having switched from regular law enforcement agency to being a major player in the counter-terrorism field has seen it avail itself of vast collections of data obtained by the NSA. While its own contributions to combating terrorism have been questionable at best, only recently was its access to NSA data seriously challenged.

But nothing came of that and things go on as they have for the past two decades. As if that wasn't enough, the FBI's directors constantly complain about encryption getting in the way of slurping up communications and scraping seized phones of all their data.

Well, all of the stuff the FBI currently collects, obtains, or has access to has to be stored somewhere. And it wants to add to these haystacks. But when the haystacks needs to be rotated out due to device failure or hardware updates, the FBI apparently believes no precautions should be taken to make sure classified and sensitive data doesn't end up in the hands of others.

That's what DOJ Inspector General Michael Horowitz has highlighted in his recent memo to the agency, which points out its extremely careless handling of discarded computer hardware.

> *We found the FBI does not always account for its loose electronic storage media, including hard drives that were extracted from computers and servers, thumb drives, and floppy disks. For example, the FBI instructs field offices to remove hard drives slated for destruction from Top Secret computers to be couriered separately to save on shipping costs. However, extracted internal hard drives are not tracked, and the FBI does not have the ability to confirm that these hard drives that contained SBU and/or NSI information were properly destroyed. The lack of accountability of these media increases*

> *the risk of loss or theft without possibility of detection.*

Not great! There are small companies that handle device and data destruction more responsibly than this and their overriding concern is maintaining market share, rather than, say, securing a nation.

The FBI also handles classified data almost as carelessly as a former president. While servers and drives might be marked to indicate the presence of classified or top secret data, data extracted for disposal is placed on other devices that do not bear these markings, making it that much easier for top secret data to be treated as carelessly as trash from the office break room.

On top of that, the FBI tends to take its time destroying hardware, which results in warehouses full of components that are potentially full of extremely sensitive information. This long-term storage is overseen by … nobody.

> *Non-accountable assets slated for destruction were stored on pallets without sufficient internal physical security for an extended period of time. For example, a pallet containing extracted internal hard drives marked non-accountable had been stored for 21 months and had wrapping that was torn and left open. This facility is shared with other FBI operations, such as logistics, mail, and information technology equipment fulfilment, and had almost 400 persons with access as of May 2024, including 28 task force officers and 63 contractors from at least 17 companies. Both the FBI supervisor and contractor confirmed that they would not be aware if someone was to take hard drives from the pallets because these assets are not accounted for or tracked.*

I'm tempted to believe "non-accountable assets" is a reference to FBI employees. But even if it's meant to designate devices that most likely do *not* contain classified or top secret information, there's no way the FBI itself can say for sure because of the previous two problems the IG discovered: top secret/classified info isn't always accounted for and some devices containing sensitive info get placed on the "please destroy" pile without proper external labeling.

Ignoring every requirement along the way to destruction results in stuff like this, which doesn't exactly instill confidence in the FBI's ability to stay on task, be detail-oriented, or many other basic levels of competency one would hope to find in the nation's largest law enforcement agency.

Walmart takes more care securing its Black Friday pallets than the FBI does with its pallets full of sensitive info. Keep that in mind the next time the FBI's complaining it simply doesn't have enough access to data or top secret information. It doesn't secure what it already has. It definitely shouldn't be entrusted with anything more until it can handle this very basic part of internal security.

4.Crypto wars: Why weakening encryption misses the mark

by Rashmi Dahiya
https://www.crowe.com/cybersecurity-watch/crypto-wars-why-weakening-encryption-misses-the-mark

Weakening encryption does more harm than good in the fight against cyberthreats.

Under the auspices of combating cybercrime, governments around the world have pushed for access to encrypted communications because they see these secure channels as potential havens for illicit activity. At the same time, privacy advocates and tech specialists warn that weakening encryption exposes

everyone to risks and undermines the trust that forms the backbone of digital interactions. This tension, generally referred to as the crypto wars, raises an important question: Is sacrificing privacy the price for security, or can security and privacy coexist in a solution that protects safety without eroding the freedoms that encryption was designed to protect?

Organizations don't exist outside of this larger, theoretical context. Indeed, by understanding this tension, they can play an important role in establishing a secure and transparent digital environment for their business and their customers.

A brief history of the crypto wars

Asymmetric encryption emerged in the 1970s against the backdrop of heavy government surveillance used to weaponize information against domestic and foreign enemies. Since then, law enforcement and government intelligence agencies have argued that widespread private use of encryption can hamper criminal investigations and national security efforts. For many cryptographers and privacy activists, however, this surveillance was the primary threat that made widespread use of cryptography a moral necessity in the first place.

One pivotal moment in this history was the prosecution of Phil Zimmerman by the U.S. federal government for distributing his encryption software, Pretty Good Privacy (PGP), without a munitions export license. In the 1990s, U.S. arms control regulators treated cryptography software like a munition, and as a result, exporting such a program overseas by posting it on the internet was in violation of these regulations. The case dragged on for three years before eventually being dropped, and export control laws were rewritten after it became obvious that software couldn't be contained like rocket motors.

Fast forward to 2021, when a presidential executive order charged the National Institute of Standards and Technology (NIST) with setting standards requiring the encryption of data to protect software supply chains. What's more, NIST's Federal Information Processing Standards have included forms of PGP software for more than two decades. This shift illustrates how the federal government eventually recognized the importance of strong encryption and that, despite the different shapes and forms it has taken over the decades, the conflict between the security and privacy advocates reflects a lag in governmental adaptation to technological advancements.

While the overarching debate generally remains the same, the crypto wars now primarily revolve around end-to-end encryption (E2EE). Widespread public access to E2EE means that criminals can also use it with impunity, making it harder to detect and investigate the transmission of illegal content, such as child sexual abuse material and terrorist plots. Law enforcement officials are challenged with investigations going dark because they are unable to conduct investigations due to a lack of access to communications and data. This situation is a surveillance and security problem and a content moderation problem. In addition, E2EE makes it harder for platforms to defend users from spam, abuse, and harassment, and encrypted communications can become vectors for abusive harassment and misinformation campaigns.

Computer scientists and privacy advocates, in turn, counter these criticisms with the argument that strategies for content moderation go beyond merely reading messages, with automated data analysis, user reporting workflows, and message flagging mechanisms as some available tools. Further, with ongoing research in this field, E2EE isn't necessarily the roadblock to content moderation that many think it is.

Why targeting E2EE is fundamentally flawed

Opponents of encryption oversimplify this challenge by assuming a middle-ground approach can allow for strong encryption with exceptional access for law enforcement. As straightforward as it might sound, this approach is a fundamentally flawed solution for three main reasons:

- **Weakened security.** Regardless of how it is implemented, exceptional access jeopardizes citizens' privacy, and it can also lead to the unintended consequence of imperiling national security. One of the biggest technical challenges here is ensuring that the back door itself does not become a weak point that can be exploited by malicious actors who could potentially attack the system's vulnerabilities, steal the keys held by law enforcement, and move their communications to non-U.S. platforms that are outside the reach of U.S. law enforcement.

- **First Amendment violation.** If mandated by the federal government, exceptional access would violate the First Amendment under the compelled speech doctrine. By requiring companies to create back doors in their encryption, the federal government is compelling them to express a message contrary to their commitment to user privacy and security. This coerced speech violates the principles of free expression and undermines the integrity of both the products and the companies that create them.

- **Potential abuse of power.** The entire argument in favor of weakening encryption rests on the assumption that governments around the world are sacrificing user privacy for the greater good in order to combat serious crimes. But what is stopping them (or even other entities) from misusing back-door access for purposes beyond the intended scope, such as unauthorized surveillance or political repression? Without adequate checks in place, exceptional access holds the potential to cause more harm than the good it seeks to offer.

Where to go from here?

Achieving the balance between security and privacy in digital communications, particularly in the context of E2EE, remains a daunting task. Despite ongoing research in this field, security specialists are far from securing a robust solution to tackle this challenge. However, following are several promising approaches that offer steps in the right direction.

- **Homomorphic encryption** is a form of encryption that enables computations on encrypted data without decryption, allowing operations such as keyword filtering and pattern matching while maintaining data confidentiality.

  - **Pro:** Supports complex analysis without exposing data

  - **Cons:** High computational overhead; cross-platform compatibility issues

- **Metadata-based moderation** allows platforms to analyze message metadata attributes such as frequency and size to identify patterns indicative of harmful content without accessing message contents. It complies with privacy regulations by focusing on noncontent data and strikes a balance between user privacy and security.

  - **Pros:** Preserves message confidentiality; complies with privacy regulations

  - **Cons:** Might miss sophisticated threats; subject to legal concerns over metadata usage and storage

- **Source tracking** is a way to integrate the original sender's identity into message metadata, allowing platforms to trace the dissemination of harmful content across networks. Source tracking enhances moderation capabilities while preserving user anonymity and confidentiality.

  - **Pro:** Preserves user anonymity by only using metadata

  - **Con:** Complex to implement in decentralized systems

- **Client-side moderation** is another way of minimizing user data exposure in content moderation. It keeps tasks such as spam filtering and malware detection on the user's device. By processing sensitive data locally, client-side moderation enhances user privacy and reduces server-side exposure, thereby mitigating risks associated with centralized data storage.

  - **Pro:** Sensitive data remains encrypted and within the user's control

  - **Cons:** Limited by user devices' processing power; requires constant updates to client software

- **Perceptual hashing** is a technique that can be used to generate unique fingerprints of media files, facilitating efficient comparison against databases to detect known harmful content, thus enhancing content moderation capabilities across diverse media formats while preserving the encryption of original files.

  - **Pros:** Effectively identifies illicit materials without breaking encryption; works across diverse media formats

  - **Cons:** Needs regular database updates; might struggle with new or sophisticated threats

The bottom line is that continued advancements in encryption technologies and regulatory frameworks will play pivotal roles in shaping the future landscape of digital communication and can help protect privacy as a fundamental right in the face of evolving security threats.

The crypto wars and business

The crypto wars hold significant implications for organizations operating in the digital space. Balancing these elements is crucial for compliance and for building and sustaining user trust. Strong encryption is a cornerstone of user trust because customers need to feel confident that their communications and data are secure. Weakening encryption can erode this trust, leading to reputational damage and potential loss of business.

One action that organizations can take is to prioritize incorporating E2EE into their operational frameworks. To do so, they can take the following steps:

- **Develop and implement policies.** Organizations should have policies in place to mandate the use of E2EE for all internal and external communications. These policies should align with regulatory requirements and industry best practices.

- **Prioritize E2EE in acquisitions.** When acquiring new software or services, prioritizing vendors that offer strong E2EE capabilities is essential. Encryption standards should meet or exceed industry benchmarks to safeguard sensitive data.

- **Train employees.** Because employees are the first line of defense for any organization, they must be trained on the importance of E2EE and how to use encryption tools effectively.

- **Evaluate regularly.** Regularly evaluating and updating encryption practices to keep pace with evolving threats and technological advancements is vital, as conducting security audits can help identify potential vulnerabilities and address them promptly.

Long story short

Security and privacy aren't two sides of the same coin. Rather, they are overlapping functions within society's technological framework. Prioritizing one over the other fails to respect the balance necessary for good public policymaking. With the world no longer being divided between the physical and the digital, the crypto wars aren't a state versus citizen or security versus privacy conflict but rather a societal risk management challenge.

As the Zimmerman story highlights, governmental understanding can evolve, albeit slowly. The ongoing struggle underscores the need for governments and businesses to keep pace with technological advancements and adapt their policies accordingly. Organizations must understand the critical role of encryption in securing data and fostering customer trust, adapt to regulatory changes, and invest in innovative solutions that balance security and privacy.

Looking ahead, continued research and technological innovation will lead to the development of more robust encryption methods and effective moderation strategies. This progression can enhance security measures and reinforce user trust in digital platforms. Aligning such advancements with global privacy regulations will be crucial in fostering a secure and transparent digital environment.

5.PQShield and Si-Five collaborate to advance post-quantum cryptography in RISC-V

by PQShield
https://www.prnewswire.com/news-releases/pqshield-and-si-five-collaborate-to-advance-post-quantum-cryptography-in-risc-v-302232038.html

PQShield, a leading quantum-safe cryptography provider, and RISC-V processing pioneer SiFive have partnered to deliver post-quantum cryptography on SiFive's Essential and Performance high-performance processor families, protecting critical aerospace, consumer, defense, and automotive systems from quantum attacks and accelerating the adoption of NIST post-quantum cryptography standards on RISC-V technologies.

Powerful quantum computers are soon expected to be able to easily crack the current encryption standards used to protect software and hardware applications globally. This also presents the immediate threat of "harvest now, decrypt later" attacks (where attackers steal data today, to crack into later with a quantum computer). As governments and institutions prepare for the quantum threat, a new cybersecurity benchmark has emerged through NIST's standardization of post quantum cryptography (PQC) algorithms, which are designed to resist quantum attacks.

To ensure they are leveraging the best security and staying one step ahead of the hackers, hardware and software manufacturers are migrating their products to PQC encryptions in line with **NIST's new standards** for post-quantum cryptography.

RISC-V is rapidly emerging as the system architecture of the future, crucial to sectors as diverse as IoT, aerospace, defense, and automotives that increasingly require greater compute density and to handle greater workloads. There is a need to modernize RISC-V cryptography to ensure it can operate in these

harsh environments in a quantum-safe manner that is secure and cost-effective - without diminishing speed or performance.

Integrating PQShield's PQPlatform-CoPro technology with SiFive's Essential RISC-V processors overcomes this challenge and delivers the highest level of protection and trust for automobiles, consumer devices, and defense and aerospace applications. The combination of PQShield's cutting-edge security IP and SiFive's world-leading processor IP yields a future-proof hardware security solution that can be deployed immediately to establish a quantum-resistant hardware Root-of-Trust - arguably the foundation of any secure system, and recently determined the highest priority use case by the NSA.

As a result, product designers leveraging SiFive's RISC-V processors can build products that comply with NIST's recently published standards for post-quantum cryptography without compromising performance or lifecycle.

This partnership will also allow PQShield's cryptographic libraries to utilize RISC-V vector extensions for the very first time. Through this, developers can maintain post-quantum protection while taking advantage of the performance benefits of RISC-V vector extension implementations in SiFive Performance P470 CPUs.

Graeme Hickey, PQShield's VP of Engineering, said: "*Partnering with SiFive is a perfect match for PQShield as we co-authored NIST's PQC standards and have contributed extensively to the RISC-V instructions extensions for cryptography. SiFive is revolutionizing RISC-V computing with its high-performance processors, and we are proud to partner with them to protect the aerospace, military, automotive, and consumer device technologies they are powering and help RISC-V innovators stay one step ahead of the attackers.*"

Yann Loisel, Principal Security Architect at SiFive, said: "*Implementing post-quantum protection is a major step for our Essential and high-performance processors and a strong benefit to our customers. This collaboration ensures that designers of RISC-V vector extensions will be working with the latest generation of cybersecurity. We're pleased to help the growth of PQC across the RISC-V community following the publication of NIST's standards*."

6.D(HE)at Attack – 20-Yr-old Flaw Let Attackers Exploit Diffie-Hellman Protocol To Over-Heat Your CPU

by Balaji N
https://cybersecuritynews.com/dheat-attack/#google_vignette

Researchers uncovered a new type of denial-of-service (DoS) attack, known as the D(HE)at attack, exploits the computational demands of the Diffie-Hellman key agreement protocol, particularly its ephemeral variant (DHE), to overwhelm servers with minimal effort from the attacker.

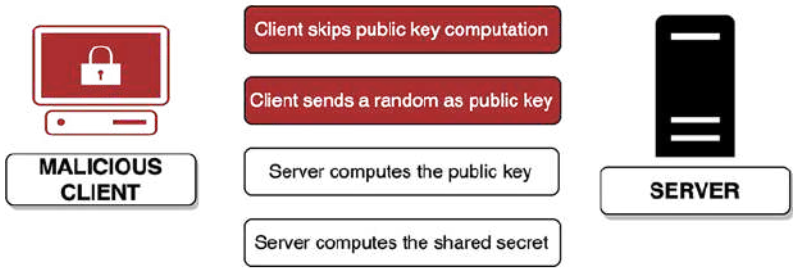
The attack is named for its ability to overheat the CPU by making the victim perform the heavy computation of modular exponentiation, which is used in the Diffie-Hellman key exchange within cryptographic protocols like TLS, SSH, IPsec, and OpenVPN.

Here's a detailed look at how this attack works and its implications.

How Does D(HE)at Attack Works

The Diffie-Hellman key agreement protocol is widely used to exchange cryptographic keys securely over public channels.

Under normal circumstances, the client and server perform similar operations, including public key generation and shared secret calculation, which involves computationally intensive modular exponentiation. Theoretically, this means both parties share the computational burden equally.



However, the D(HE)at attack takes advantage of a protocol flaw, particularly in older versions of protocols like TLS (Transport Layer Security) prior to version 1.3. In these versions, a malicious client can initiate a handshake by pretending to support only the ephemeral variant of Diffie-Hellman.

This forces the server to generate a public key without the client having to reciprocate with its own computational effort.

Once the server completes this task, the attacker terminates the connection, leaving the server to bear the computational cost.

Exploiting Protocol and Implementation Weaknesses

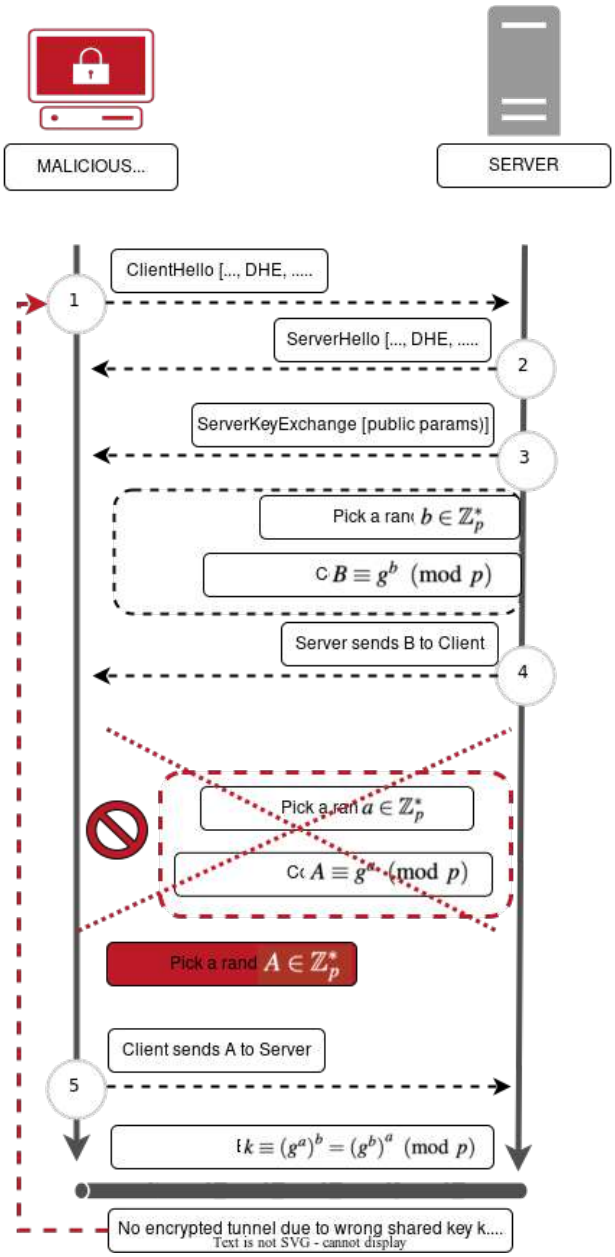
The client must send its public key in protocols like TLS 1.3 or SSH. However, a malicious client can send an arbitrary number as its public key, avoiding the need for modular exponentiation.

Unaware of this deception, the server calculates the shared secret, performing a second modular exponentiation. Although the key agreement eventually fails, the server has already expended significant computational resources.

According to the report, Certain implementation flaws and protocol configurations exacerbate the attack:

1. **Exponent Lengths**: Some cryptographic libraries use long exponents, leading to more expensive calculations (CVE-2022-40735). The resource requirement for modular exponentiation grows nonlinearly with the size of these parameters, making larger key sizes particularly vulnerable.

2. **Public Key Validation**: To prevent small subgroup confinement attacks, servers should validate the order of the peer's public key. However, some libraries perform this validation regardless of whether a safe-prime group is used, triggering unnecessary computational effort (CVE-2024-41996).



3. **Parameter Sizes**: Larger parameter sizes, such as ffdhe6144 or ffdhe8192, can significantly increase the attack's impact. Some libraries, like OpenSSL, default to the largest available parameter size, which can be exploited if not properly configured by application servers.

The D(HE)at attack is not merely a flaw in cryptographic library implementations that can be patched with a software update.

It is a protocol-level vulnerability that requires a more strategic approach to mitigation. Servers cannot easily distinguish between a legitimate modular exponentiation result and a random number, as there is no proof-of-work required from the client.

Researchers also released an FAQ detailing some of the most relevant questions about D(HE)at attack.

D(HE)at Attack Mitigation

To mitigate the risk of a D(HE)at attack, organizations should consider:

- **Updating Protocols**: Transitioning to newer protocol versions like TLS 1.3, which require mutual public key exchange before server-side computations.
- **Configuring Libraries**: Adjusting cryptographic library settings to use shorter exponents and smaller parameter sizes where possible.
- **Implementing Rate Limiting**: Applying rate limits to the number of handshake requests a server processes from a single client.
- **Monitoring and Alerts**: Setting up monitoring systems to detect unusual patterns of handshake requests that could indicate an ongoing attack.

7.Is Telegram really an encrypted messaging App?

by Matthew Green
https://blog.cryptographyengineering.com/2024/08/25/telegram-is-not-really-an-encrypted-messaging-app/

This blog is reserved for more serious things, and ordinarily I wouldn't spend time on questions like the above. But much as I'd like to spend my time writing about exciting topics, sometimes the world requires a bit of what Brad Delong calls "Intellectual Garbage Pickup," namely: correcting wrong, or mostly-wrong ideas that spread unchecked across the Internet.

This post is inspired by the recent and concerning news that Telegram's CEO Pavel Durov has been arrested by French authorities for its failure to sufficiently moderate content. While I don't know the details, the use of criminal charges to coerce social media companies is a pretty worrying escalation, and I hope there's more to the story.

But this arrest is not what I want to talk about today.

What I do want to talk about is one specific detail of the reporting. Specifically: the fact that nearly every news report about the arrest refers to Telegram as an "encrypted messaging app." Here are just a few examples:

> The arrest was made by investigators from the National Anti-Fraud Office, part of the French Customs Department, according to the reports. Durov, who has been criticized for alleged insufficient moderation on the encrypted Telegram app, is accused of refusing to cooperate with authorities, according to the reports.

This phrasing drives me nuts because in a very limited technical sense it's *not wrong.* Yet in every sense that matters, it fundamentally misrepresents what Telegram is and how it works in practice. And this mis-

representation is bad for both journalists and particularly for Telegram's users, many of whom could be badly hurt as a result.

Now to the details.

Does Telegram have encryption or doesn't it?

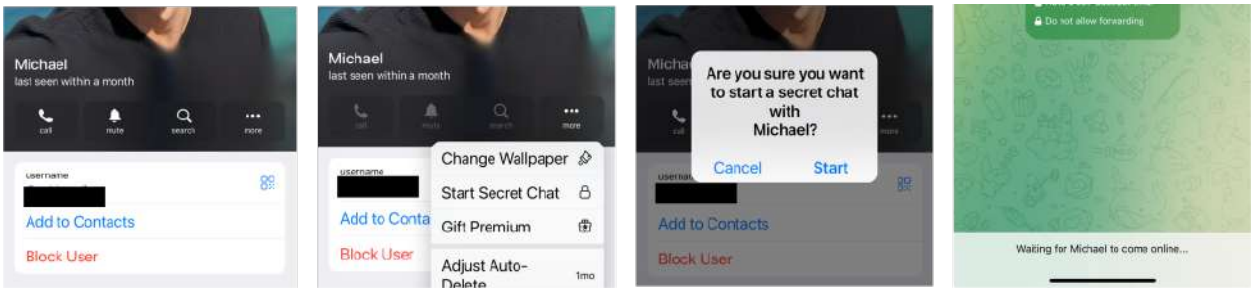
Many systems use encryption in some way or another. However, when we talk about encryption in the context of modern private messaging services, the word typically has a very specific meaning: it refers to the use of default end-to-end encryption to protect users' message content. When used in an industry-standard way, this feature ensures that every message will be encrypted using encryption keys that are only known to the communicating parties, and not to the service provider.

From your perspective as a user, an "encrypted messenger" ensures that each time you start a conversation, your messages will only be readable by the folks you intend to speak with. If the operator of a messaging service tries to view the content of your messages, all they'll see is useless encrypted junk. That same guarantee holds for anyone who might hack into the provider's servers, and also, for better or for worse, to law enforcement agencies that serve providers with a subpoena.

Telegram clearly fails to meet this stronger definition for a simple reason: it does not end-to-end encrypt conversations by default. If you want to use end-to-end encryption in Telegram, you must manually activate an optional end-to-end encryption feature called "Secret Chats" for every single private conversation you want to have. The feature is explicitly not turned on for the vast majority of conversations, and is only available for one-on-one conversations, and never for group chats with more than two people in them.

As a kind of a weird bonus, activating end-to-end encryption in Telegram is oddly difficult for non-expert users to actually do.

For one thing, the button that activates Telegram's encryption feature is not visible from the main conversation pane, or from the home screen. To find it in the iOS app, I had to click at least four times — once to access the user's profile, once to make a hidden menu pop up showing me the options, and a final time to "confirm" that I wanted to use encryption. And even after this I was not able to actually have an encrypted conversation, since *Secret Chats only works if your conversation partner happens to be online* when you do this.



Starting a "secret chat" with my friend Michael on the latest Telegram iOS app. From an ordinary chat screen this option isn't directly visible. Getting it activated requires four clicks: **(1)** to get to Michael's profile (left image), **(2)** on the "…" button to display a hidden set of options (center image), **(3)** on "Start Secret Chat", and **(4)** on the "Are you sure…" confirmation dialog. After that I'm still unable to send Michael any messages, because Telegram's Secret Chats can only be turned on if the other user is also online.

Overall this is quite different from the experience of starting a new encrypted chat in an industry-standard modern messaging application, which simply requires you to open a new chat window.

While it might seem like I'm being picky, the difference in adoption between default end-to-end encryption and this experience is likely very significant. The practical impact is that the vast majority of one-on-one Telegram conversations — and literally *every single group chat* — are probably visible on Telegram's servers, which can see and record the content of all messages sent between users. That may or may not be a problem for every Telegram user, but it's certainly not something we'd advertise as particularly well encrypted.

(If you're interested in the details, as well as a little bit of further criticism of Telegram's actual encryption protocols, I'll get into what we know about that further below.)

But wait, does default encryption really matter?

Maybe yes, maybe no! There are two different ways to think about this.

One is that *Telegram's lack of default encryption is just fine for many people*. The reality is that many users don't choose Telegram for encrypted private messaging at all. For plenty of people, Telegram is used more like a social media network than a private messenger.

Getting more specific, Telegram has two popular features that makes it ideal for this use-case. One of those is the ability to create and subscribe to "channels", each of which works like a broadcast network where one person (or a small number of people) can push content out to millions of readers. When you're *broadcasting* messages to thousands of strangers in public, maintaining the secrecy of your chat content isn't as important.

Telegram also supports large public group chats that can include thousands of users. These groups can be made open for the general public to join, or they can set up as invite-only. While I've never personally wanted to share a group chat with thousands of people, I'm told that many people enjoy this feature. In the large and *public* instantiation, it also doesn't really matter that Telegram group chats are unencrypted — after all, who cares about confidentiality if you're talking in the public square?

But Telegram is not limited to just those features, and many users who join for them will also do other things.

Imagine you're in a "public square" having a large group conversation. In that setting there may be no expectation of strong privacy, and so end-to-end encryption doesn't really matter to you. But let's say that you and five friends step out of the square to have a side conversation. Does *that* conversation deserve strong privacy? It doesn't really matter what you want, because *Telegram won't provide it*, at least not with encryption that protects you from sharing your content with Telegram servers.

Similarly, imagine you use Telegram for its social media-like features, meaning that you mainly consume content rather than producing it. But one day your friend, who also uses Telegram for similar reasons, notices you're on the platform and decides she wants to send you a private message. Are you concerned about privacy now? And are you each going to manually turn on the "Secret Chat" feature — even though it requires four explicit clicks through hidden menus, and even though it will prevent you from communicating immediately if one of you is offline?

My strong suspicion is that many people who join Telegram for its social media features also end up using it to communicate privately. And I think Telegram knows this, and tends to advertise itself as a "secure messenger" and talk about the platform's encryption features precisely because they know it makes people feel more comfortable. But in practice, I also suspect that very few of those users are actually *using Telegram's encryption*. Many of those users may not even realize they have to turn encryption on manually, and think they're already using it.

Which brings me to my next point.

Telegram knows its encryption is difficult to turn on, and they continue to promote their product as a secure messenger

Telegram's encryption has been subject to heavy criticism since at least 2016 (and possibly earlier) for many of the reasons I outlined in this post. In fact, many of these criticisms were made by experts including myself, in years-old conversations with Pavel Durov on Twitter[1].

Although the interaction with Durov could sometimes be harsh, I still mostly assumed good faith from Telegram back in those days. I believed that Telegram was busy growing their network and that, in time, they would improve the quality and usability of the platform's end-to-end encryption: for example, by activating it as a default, providing support for group chats, and making it possible to start encrypted chats with offline users. I assumed that while Telegram might be a follower rather than a leader, it would eventually reach feature parity with the encryption protocols offered by Signal and WhatsApp. Of course, a second possibility was that Telegram would abandon encryption entirely — and just focus on being a social media platform.

What's actually happened is a lot more confusing to me.

Instead of improving the usability of Telegram's end-to-end encryption, the owners of Telegram have more or less kept their encryption UX unchanged since 2016. While there have been a few upgrades to the underlying encryption algorithms used by the platform, the user-facing experience of Secret Chats in 2024 is almost identical to the one you'd have seen eight years ago. This, despite the fact that the number of Telegram users has grown by 7-9x during the same time period.

At the same time, Telegram CEO Pavel Durov has continued to aggressively market Telegram as a "secure messenger." Most recently he issued a scathing criticism of Signal and WhatsApp on his personal Telegram channel, implying that those systems were backdoored by the US government, and only Telegram's independent encryption protocols were really trustworthy.

While this might be a reasonable nerd-argument if it was taking place between two platforms that both supported default end-to-end encryption, Telegram really has no legs to stand on in this particular discussion. Indeed, it no longer feels amusing to see the Telegram organization urge people away from default-encrypted messengers, while *refusing to implement essential features that would widely encrypt their own users' messages*. In fact, it's starting to feel a bit malicious.

What about the boring encryption details?

This is a cryptography blog and so I'd be remiss if I didn't spend at least a little bit of time on the boring encryption protocols. I'd also be missing a good opportunity to *let my mouth gape open in amazement*, which is pretty much what happens every time I look at the internals of Telegram's encryption.

I'm going to handle this in one paragraph to reduce the pain, and you can feel free to skip past it if you're not interested.

According to what I *think* is the latest encryption spec, Telegram's Secret Chats feature is based on a

[1] I will never find all of these conversations again, thanks to Twitter search being so broken. If anyone can turn them up I'd appreciate it.

custom protocol called MTProto 2.0. This system uses 2048-bit[2] finite-field Diffie-Hellman key agreement, with group parameters (I think) chosen by the server. (Since the Diffie-Hellman protocol is only executed interactively, this is why Secret Chats cannot be set up when one user is offline.) MITM protection is handled by the end-users, who must compare key fingerprints. There are some weird random nonces provided by the server, which I don't fully understands the purpose of — and that in the past used to actively make the key exchange totally insecure against a malicious server (but this has long since been fixed.) The resulting keys are then used to power the most amazing, non-standard authenticated encryption mode ever invented, something called "Infinite Garble Extension" (IGE) based on AES and with SHA2 handling authentication.

If you ask me to guess whether the protocol and implementation of Telegram Secret Chats is secure, I would say *quite possibly.* To be honest though, it doesn't matter how secure something is if people aren't actually using it.

Is there anything else I should know?

Yes, unfortunately. Even though end-to-end encryption is one of the best tools we've developed to prevent data compromise, it is hardly the end of the story. One of the biggest privacy problems in messaging is the availability of loads of meta-data — essentially data about who uses the service, who they talk to, and when they do that talking.

This data is not typically protected by end-to-end encryption. Even in applications that are broadcast-only, such as Telegram's channels, there is plenty of useful metadata available about *who is listening to a broadcast.* That information alone is valuable to people, as evidenced by the enormous amounts of money that traditional broadcasters spend to collect it. Right now all of that information likely exists on Telegram's servers, where it is available to anyone who wants to collect it.

I am not specifically calling out Telegram for this, since the same problem exists with virtually every other social media network and private messenger. But it should be mentioned, just to avoid leaving you with the conclusion that encryption is all we need.

8.Chinese Researchers Perform Space-To-Ground Communications with Lightweight Quantum Satellite

by Matt Swayne
https://thequantuminsider.com/2024/08/24/chinese-researchers-perform-space-to-ground-communications-with-lightweight-quantum-satellite/

A team of Chinese researchers report that the successfully developed and demonstrated a compact quantum microsatellite that can performing space-to-ground quantum key distribution (QKD) using lightweight, portable ground stations, according to a study published on the preprint server ArXiv.

---

[2] It is a point where expert cryptographers would, in the context of something like a professional security audit, raise their hands and ask *a lot* of questions. I'm not going to go further than this. Suffice it to say that Telegram's encryption is unusual.

The microsatellite, weighing in at just slightly over 20 kilograms, represents a major cut in size and weight compared to previous quantum satellites, enabling more flexible and rapid deployment. The team reports the system achieved real-time secure communication, sharing up to 0.59 million bits of secure keys in a single satellite pass, marking a major step toward a global quantum network.

While challenges lie ahead, this achievement could be a step toward realizing a global quantum network, a technology that could offer secure communications and other advanced computing applications. The portable nature of the network would also offer several critical national security and defense advantages.

Microsatellite Innovation

The research team, which included members from the University of Science and Technology of China (USTC), the Chinese Academy of Sciences (CAS), and Quantum CTek Co., designed the quantum microsatellite with a payload weighing about 23 kilograms — that's approximately 50 pounds, or about the weight of a large bag of dog food. This is a substantial reduction compared to the previously developed Micius satellite, with a payload that weighed more than ten times more — around 250 kilograms. The microsatellite, dubbed Jinan-1, was launched into a 500-kilometer Sun-synchronous orbit in July 2022, according to the paper, and has since demonstrated its ability to securely share quantum keys between space and ground stations.

Quantum key distribution (QKD) is a method that leverages quantum mechanical principles to securely share encryption keys between two parties. Unlike traditional encryption methods, which rely on complex mathematical algorithms, QKD ensures that any attempt to intercept the key would be immediately detectable. This makes QKD an attractive option for securing sensitive communications against potential cyber threats.

Lightweight Ground Stations

In addition to the satellite, the research team developed portable ground stations, each weighing approximately 100 kilograms. This represents a significant reduction from traditional optical ground stations, which can weigh upwards of 13,000 kilograms.

The portability of these ground stations opens the possibility of deploying them in diverse and challenging environments, from urban areas to remote mountainous regions. In terms of military applications, a 100 kilograms is about the same weight of full combat gear of a soldier, opening up possibilities for use by militaries that are constantly moving through rugged terrains.

The ground stations are equipped with telescopes and specialized detectors that can receive quantum signals from the satellite. The researchers designed these stations to be easily assembled and rapidly deployed, requiring only three to five hours for full setup. This flexibility could make the technology accessible to a wide range of users, including governments, businesses, armed forces and scientific institutions.

Real-Time Secure Communication

Perhaps the most significant achievements reported in the study is the ability to perform real-time secure communication. According to the paper, the research team implemented a system of multiplexed bidirectional — sending and receiving — satellite-ground optical communication, which allowed for the simultaneous transmission of quantum keys and classical data. The setup enabled the researchers to achieve key distillation — an essential process for generating secure encryption keys — during a single satellite pass, with the sharing of up to 0.59 million bits of secure keys in one instance.

The satellite-ground communication was made possible by using a high-precision tracking system,

which kept the satellite and ground stations perfectly aligned during key transmission. This system uses a combination of satellite attitude control and advanced optics to maintain a precise link between the satellite's payload and the ground station's telescope.

Challenges And Future Prospects

While the development of the quantum microsatellite and portable ground stations is a significant technological achievement, several challenges remain before a global quantum network can be fully realized. One of the main hurdles is scaling the technology to create a constellation of quantum satellites capable of providing continuous global coverage.

The study's authors suggest that future efforts could focus on integrating quantum key distribution systems into photonics chips, further miniaturizing the payloads and making them even more accessible. Additionally, they propose exploring the feasibility of daytime satellite-to-ground QKD, which would enable round-the-clock secure communication services. The combination of satellites at different altitudes and orbit types could also enhance the performance and reliability of the quantum network.

Another avenue for future research is the development of satellite-based quantum repeaters, which would extend the range of QKD beyond the limitations of a single satellite pass. An advance like that could pave the way for a truly global quantum network, providing unprecedented levels of security for communications, computing, and sensing applications.

Broader Implications

The successful demonstration of satellite-based QKD with a lightweight, portable system has broad implications for the future of secure communications, the researchers write. As cyber threats continue to evolve, the ability to securely transmit information across long distances without the risk of interception could become increasingly valuable. Governments, military organizations, financial institutions and healthcare providers are just a few of the sectors that would likely line up to take advantage of quantum communication technologies.

Going a step in the scientific direction, the development of a quantum satellite constellation could be important for the broader field of quantum information science. By establishing a global quantum network, researchers could explore new possibilities in quantum computing and quantum sensing, potentially leading to advances that are currently unimaginable.

In addition to USTC, CAS and Quantum CTek Co., other key contributors include the Hefei National Research Center for Physical Sciences at the Microscale, Shanghai Research Center for Quantum Science, CAS Center for Excellence in Quantum Information and Quantum Physics, Hefei National Laboratory, Key Laboratory of Space Active Opto-Electronic Technology, Shanghai Institute of Technical Physics, Innovation Academy for Microsatellites of the Chinese Academy of Sciences, Jinan Institute of Quantum Technology, CAS Quantum Network Co., Ltd., and the Beijing Electronics Science and Technology Institute.

9.NIST Hands Off Post-Quantum Cryptography Work to Cyber Teams

by Becky Bracken
https://www.darkreading.com/cyber-risk/nist-post-quantum-cryptography-work-cyber-teams

No longer relegated to post-doctorate physics academia and sad Schrödinger's cat thought experiments, post-quantum computing remediation has arrived in the real world.

Quantum computing is expected to emerge in earnest a decade from now, with the power to crack existing public key infrastructure (PKI) cryptography schemes like RSA. And with NIST's recent release of three final quantum encryption standards, security teams are now racing against that 10-year clock to update vulnerable cryptography before quantum algorithms go into production that are capable of crushing them and unlocking reams of secret data.

With NIST effectively handing off the work of post-quantum encryption remediation planning and execution to cybersecurity teams around the world with the release of the standards, the time is now for rank-and-file cybersecurity professionals to get "hands on" with post-quantum cryptography (PQC), according to Jason Soroko, senior vice president of product at Sectigo.

"For regular cybersecurity practitioners who have been saying, 'I'm waiting for NIST,' there is no longer reason to wait," Soroko says.

Major information technology (IT) players like Akamai, and browsers including Google Chrome, have already initiated large-scale efforts to shore up their post-quantum cryptographic cybersecurity. But, individual organizations will need to handle the security of data both in-transit and at-rest after it's handed off to their networks from the edge and content delivery networks (CDNs). And unfortunately, the sheer scale of the problem is gargantuan, so they need to start now.

"Transitioning to post-quantum cryptography is a complex, multi-year process that requires careful planning to minimize disruption and ensure continued security," Soroko explains. "Early planning allows for a smoother transition when PQC standards become widely available."

Time is of the essence, too: there are already worries about "steal now, decrypt later" adversaries harvesting sensitive encrypted data and storing it for future decryption via quantum computers.

Transitioning to NIST's New Post-Quantum Cryptography Standards

Philip George, executive technical strategist at Merlin Cyber, characterizes the release of the new NIST post-quantum cryptography standards as a "pivotal moment for cybersecurity practitioners and general technology consumers alike," but notes that considerable time and effort will be needed to get arms around the scope of the PQC migration. And the complexity starts with the fact that all communications rely on cryptography for essential authentication functions, as well as privacy and security.

"There isn't one single area across the IT domain that does not rely on cryptography — whether it's encrypting data, securing connectivity to a bastion host, or providing validation checks for software," George says.

Thus, as a first practical PQC step, cryptography's sheer ubiquity requires a fulsome, automated asset inventory to prepare for any transition to quantum. To that end, "conduct a comprehensive audit of all cryptographic assets and protocols in use within the organization," Soroko advises. "This includes identifying where cryptographic algorithms are used for data protection, authentication, digital signatures, and other critical security functions."

There are scanning tools available to assist companies with the work of gathering evidence of cryptography across the organization, as well as from data from public key infrastructure logs and certificates, certificate management tools, cryptographic hardware keys, and more, he notes.

Further, these tools can maintain that cryptographic inventory as the organization's infrastructure changes, and integrate into ongoing development processes.

PQC Asset Inventory & Building a Remediation Plan

Once the cryptography asset inventory is complete, a remediation plan can be put into place, which involves determining which assets are most vulnerable to quantum attacks and need upgrading to post-quantum algorithms first, Soroko suggests.

For instance, when it comes to defending against the "harvest now and decrypt later" threat, Soroko suggests immediately identifying the organization's critical secrets protected by legacy algorithms and prioritizing those for PQC transition.

Meanwhile, PQC migration plans should be as detailed as possible, including the 'how' and 'when' the transition will take place, Soroko explains.

"Identify legacy and vulnerable cryptography, focusing on algorithms susceptible to quantum attacks (e.g., RSA, ECC)," he says, adding that cyber teams should also assess the "lifespan of critical data to determine the urgency of migration."

He also advocates that organizations set up a cross-functional team that includes IT, security, legal, and other business units, in order to centralize the PQC migration effort.

"This approach ensures all areas are covered and reduces duplication, leading to significant cost savings," Soroko says. "Crucially, adopt a top-down approach, ensuring that executives who own the risk champion the initiative, rather than leaving it to IT staff to assess risk. This alignment ensures that PQC migration is treated as a strategic priority, backed by the necessary resources and authority."

A joint NIST and Department of Homeland Security post-quantum roadmap explains that each organization will have its own particular set of requirements. It recommends determining where to start by asking these questions:

1. Is the system a high value asset based on organizational requirements?
2. What is the system protecting (e.g. key stores, passwords, root keys, signing keys, personally identifiable information, sensitive personally identifiable information)?
3. What other systems does the system communicate with?
4. To what extent does the system share information with federal entities?
5. To what extent does the system share information with other entities outside of your organization?
6. Does the system support a critical infrastructure sector?

7.How long does the data need to be protected?

The Role of Vendors & Partners

Creating a PQC remediation plan should also be done in close coordination with partners and vendors with whom organizations share data, to help guarantee a smoother transition.

"Collaboration ensures that the transition aligns with industry standards, minimizing risks," Soroko says. "Partners can also offer ongoing support, keeping the cryptographic infrastructure secure against evolving quantum threats."

Getting perspective on the entire enterprise ecosystem is critically important, and can't be achieved without engaging partners and vendors.

"Vendors can assist in identifying and securing critical secrets that may be targeted for 'harvest and decrypt' attacks, ensuring these are protected with quantum-resistant algorithms," he adds.

Including vendors in PQC transition planning early can also let cyber teams tap into specialized expertise that can ultimately help them stay ahead of quantum threats, too, according to Adam Everspaugh, cryptography expert with Keeper Security.

"Successfully transitioning to quantum-resistant cryptography will require a combination of expertise in cryptography, IT infrastructure and cybersecurity," he explains. "Security teams will need to collaborate closely with cryptographers who understand the new algorithms, as well as IT professionals who can manage the integration with existing systems. Given the uniqueness of these algorithms, expertise is still developing."

Vendors and partners should also continue to work with cyber teams through the research and testing phase, once planning is complete, Soroko says.

"Begin testing and integrating NIST-approved post-quantum cryptographic algorithms within your organization's infrastructure," he explains. "This includes participating in pilot programs, collaborating with vendors, and engaging in ongoing research to stay informed about the latest developments in PQC."

Don't Drag Your Feet on Quantum

It may seem daunting, but the need to implement PQC standards ahead of the next imminent quantum computing breakthrough means cyber professionals and network defenders everywhere can no longer just think about quantum — they need to act.

"The challenges for IT and security teams are significant, from ensuring compatibility with existing systems, to managing the transition of cryptographic keys," Everspaugh says. "However, the urgency of this shift cannot be overstated."

And indeed, organizations which take on the PQC project early will be far better positioned to successfully defend their networks from the impending quantum revolution, Soroko adds.

"Early adoption and testing will help organizations identify potential challenges and refine their implementation strategies," he says. "Engaging in research ensures the organization remains at the forefront of PQC advancements and is prepared to implement secure algorithms as they become standardized."

10.Toward a code-breaking quantum computer

by Adam Zewe
https://news.mit.edu/2024/toward-code-breaking-quantum-computer-0823

The most recent email you sent was likely encrypted using a tried-and-true method that relies on the idea that even the fastest computer would be unable to efficiently break a gigantic number into factors.

Quantum computers, on the other hand, promise to rapidly crack complex cryptographic systems that a classical computer might never be able to unravel. This promise is based on a quantum factoring algorithm proposed in 1994 by Peter Shor, who is now a professor at MIT.

But while researchers have taken great strides in the last 30 years, scientists have yet to build a quantum computer powerful enough to run Shor's algorithm.

As some researchers work to build larger quantum computers, others have been trying to improve Shor's algorithm so it could run on a smaller quantum circuit. About a year ago, New York University computer scientist Oded Regev proposed a major theoretical improvement. His algorithm could run faster, but the circuit would require more memory.

Building off those results, MIT researchers have proposed a best-of-both-worlds approach that combines the speed of Regev's algorithm with the memory-efficiency of Shor's. This new algorithm is as fast as Regev's, requires fewer quantum building blocks known as qubits, and has a higher tolerance to quantum noise, which could make it more feasible to implement in practice.

In the long run, this new algorithm could inform the development of novel encryption methods that can withstand the code-breaking power of quantum computers.

"If large-scale quantum computers ever get built, then factoring is toast and we have to find something else to use for cryptography. But how real is this threat? Can we make quantum factoring practical? Our work could potentially bring us one step closer to a practical implementation," says Vinod Vaikuntanathan, the Ford Foundation Professor of Engineering, a member of the Computer Science and Artificial Intelligence Laboratory (CSAIL), and senior author of a paper describing the algorithm.

The paper's lead author is Seyoon Ragavan, a graduate student in the MIT Department of Electrical Engineering and Computer Science. The research will be presented at the 2024 International Cryptology Conference.

Cracking cryptography

To securely transmit messages over the internet, service providers like email clients and messaging apps typically rely on RSA, an encryption scheme invented by MIT researchers Ron Rivest, Adi Shamir, and Leonard Adleman in the 1970s (hence the name "RSA"). The system is based on the idea that factoring a 2,048-bit integer (a number with 617 digits) is too hard for a computer to do in a reasonable amount of time.

That idea was flipped on its head in 1994 when Shor, then working at Bell Labs, introduced an algorithm which proved that a quantum computer could factor quickly enough to break RSA cryptography.

"That was a turning point. But in 1994, nobody knew how to build a large enough quantum computer. And we're still pretty far from there. Some people wonder if they will ever be built," says Vaikuntanathan.

It is estimated that a quantum computer would need about 20 million qubits to run Shor's algorithm. Right now, the largest quantum computers have around 1,100 qubits.

A quantum computer performs computations using quantum circuits, just like a classical computer uses classical circuits. Each quantum circuit is composed of a series of operations known as quantum gates. These quantum gates utilize qubits, which are the smallest building blocks of a quantum computer, to perform calculations.

But quantum gates introduce noise, so having fewer gates would improve a machine's performance. Researchers have been striving to enhance Shor's algorithm so it could be run on a smaller circuit with fewer quantum gates.

That is precisely what Regev did with the circuit he proposed a year ago.

"That was big news because it was the first real improvement to Shor's circuit from 1994," Vaikuntanathan says.

The quantum circuit Shor proposed has a size proportional to the square of the number being factored. That means if one were to factor a 2,048-bit integer, the circuit would need millions of gates.

Regev's circuit requires significantly fewer quantum gates, but it needs many more qubits to provide enough memory. This presents a new problem.

"In a sense, some types of qubits are like apples or oranges. If you keep them around, they decay over time. You want to minimize the number of qubits you need to keep around," explains Vaikuntanathan.

He heard Regev speak about his results at a workshop last August. At the end of his talk, Regev posed a question: Could someone improve his circuit so it needs fewer qubits? Vaikuntanathan and Ragavan took up that question.

Quantum ping-pong

To factor a very large number, a quantum circuit would need to run many times, performing operations that involve computing powers, like 2 to the power of 100.

But computing such large powers is costly and difficult to perform on a quantum computer, since quantum computers can only perform reversible operations. Squaring a number is not a reversible operation, so each time a number is squared, more quantum memory must be added to compute the next square.

The MIT researchers found a clever way to compute exponents using a series of Fibonacci numbers that requires simple multiplication, which is reversible, rather than squaring. Their method needs just two quantum memory units to compute any exponent.

"It is kind of like a ping-pong game, where we start with a number and then bounce back and forth, multiplying between two quantum memory registers," Vaikuntanathan adds.

They also tackled the challenge of error correction. The circuits proposed by Shor and Regev require every quantum operation to be correct for their algorithm to work, Vaikuntanathan says. But error-free quantum gates would be infeasible on a real machine.

They overcame this problem using a technique to filter out corrupt results and only process the right ones.

The end-result is a circuit that is significantly more memory-efficient. Plus, their error correction technique would make the algorithm more practical to deploy.

"The authors resolve the two most important bottlenecks in the earlier quantum factoring algorithm. Although still not immediately practical, their work brings quantum factoring algorithms closer to reality," adds Regev.

In the future, the researchers hope to make their algorithm even more efficient and, someday, use it to test factoring on a real quantum circuit.

"The elephant-in-the-room question after this work is: Does it actually bring us closer to breaking RSA cryptography? That is not clear just yet; these improvements currently only kick in when the integers are much larger than 2,048 bits. Can we push this algorithm and make it more feasible than Shor's even for 2,048-bit integers?" says Ragavan.

11.The Road to Post-Quantum Cryptography

https://cxotoday.com/specials/the-road-to-post-quantum-cryptography/

What does the future hold for quantum computing, and are we on the brink of a major breakthrough? Recent advancements by industry giants and startups suggest we're closer than ever to realizing the potential of this transformative technology.

In 2019, researchers at Google built a programmable quantum computer that achieved quantum supremacy. That is, it performed a task that no traditional computer could perform in a reasonable amount of time. In this case, quantum computing researchers performed a test computation in about 200 seconds that would have taken a supercomputer using today's best algorithm thousands of years to calculate.

However, the continued development of quantum computers faces several technical hurdles. Qubits, which are the basic building blocks of quantum computers, are extremely sensitive to outside interference. To really use quantum computers, researchers need better ways to correct the errors created by that interference.

"The field has seen significant progress recently, driven by improvements in qubit quality, error rates and scalability, alongside substantial investments from large tech companies and startups," said IEEE Senior Member Kevin Curran. "A key challenge remains in error correction, with advancements here being potentially transformative. Additionally, the development of new quantum algorithms could significantly enhance the utility of quantum computers."

Here, he discusses recent advances in quantum computing, what's holding the technology back and the leading edge of post-quantum cybersecurity.

Can you discuss any major developments in quantum computing that have increased the accessibility of quantum computers?

"In recent years, quantum computing has made significant strides across several key areas. The availability of quantum computing through cloud services by major tech companies has democratized access, enabling more widespread research and development. There has been substantial growth in hybrid quantum-classical algorithms, which combine classical and quantum computing strengths to tackle complex problems.

"Researchers have also expanded the portfolio of quantum algorithms with potential exponential speed-ups over classical methods, finding applications in diverse sectors such as pharmaceuticals, finance and material sciences. These developments signal a shift towards more practical and impactful quantum computing applications soon."

What is your view on the future of quantum computing and the likelihood of a near-term breakthrough?

"Predicting a near-term breakthrough in quantum computing is complex due to the interplay of technological advancements and theoretical innovations. While many experts suggest that practical, scalable quantum computers that consistently outperform classical systems may still be a few years away, there is optimism about achieving specific milestones soon. The next five to 10 years will likely be crucial for witnessing significant advancements in this area."

Y2Q stands for years-to-quantum, a shorthand for the point at which quantum computers can crack current encryption algorithms. What's your perspective on this milestone?

"It's crucial because quantum computers could potentially decrypt data previously thought to be secure, affecting everything from government communications to private internet transactions. Those most at risk include governments, financial institutions, technology companies, healthcare organizations and anyone relying on secure internet use."

What's the status of post-quantum encryption algorithms?

"Quantum-resistant cybersecurity algorithms, developed to secure communications against the potential threats of quantum computers, are rooted in mathematical problems believed to withstand classical and quantum attacks. The ongoing standardization efforts by the National Institute of Standards and Technology (NIST), which began in 2016, are critical in evaluating these algorithms for security and practicality, enhancing confidence in their robustness.

"Besides the efforts by NIST to standardize post-quantum cryptography, there are several other emerging standards and algorithms in the field of quantum computing. These include the Internet Engineering Task Force and the European Telecommunications Standards Institute, which also focus on quantum-resistant cryptographic standards."

How confident are you in these quantum-resistant algorithms?

"While these post-quantum cryptography systems are well-understood, they haven't been tested as extensively as traditional cryptographic methods. "As the cryptographic community continues to scrutinize and improve these algorithms, our confidence in them grows. However, this is a gradual process contingent on further research and adaptation to emerging threats. Therefore, while there is promising progress in the development of quantum-resistant algorithms, a cautious approach remains prudent as the field evolves."

12.Understanding NIST's post-quantum cryptography standards

by Jill McKeon

https://www.techtarget.com/healthtechsecurity/feature/Understanding-NISTs-post-quantum-cryptography-standards

NIST released its first set of post-quantum cryptography standards in August 2024, giving organizations a clear path forward in securing their systems with quantum-safe algorithms. The standards consist of three encryption algorithms engineered to withstand cyberattacks from a quantum computer.

Quantum computing technology has the potential to take complex variables into account and accomplish tasks that classic computers cannot, NIST states in its explainer on post-quantum cryptography. For example, quantum computers might be able to partake in drug design and create simulations of complex molecules.

But as experts race to build these powerful quantum computers, NIST has been working to address the potential security threats that could result from a quantum computer with the ability to break current encryption methods. The new standards are the result of an eight-year effort by NIST to tackle these issues under its post-quantum cryptography standardization project.

"Quantum computing technology could become a force for solving many of society's most intractable problems, and the new standards represent NIST's commitment to ensuring it will not simultaneously disrupt our security," said Laurie E. Locascio, NIST director and under secretary of commerce for standards and technology, in a press release.

"These finalized standards are the capstone of NIST's efforts to safeguard our confidential electronic information."

NIST recommended that organizations begin adopting these standards as soon as possible. For healthcare, like other industries, implementing these standards requires organizations to take a proactive approach now in preparation for the security challenges that will likely come with quantum computing in the near and distant future.

Why post-quantum cryptography standards are important

To Scott Crowder, vice president of quantum adoption and business development at IBM, the new standards are crucial for ensuring that data does not end up in the wrong hands in a post-quantum world. IBM cryptography researchers developed two of the three standards, and a scientist who has since joined IBM Research developed the third.

"What the U.S. government is spooked about is people being able to collect all the data that's on the internet today and then wait a number of years for the quantum computers to come, and then they can break all their cryptography and decrypt all the messages," Crowder explained to *TechTarget Editorial*.

"That is why they're being very proactive in certain sensitive industries to make this transition sooner rather than later. We can't do anything about stuff that got sent and captured five years ago, but we can do something about stuff that's sent and captured three months from now. That is one of the reasons why the U.S. government is pushing for people not to just ignore this until it's too late."

For that reason, researchers have spent the better part of the last decade identifying these new standards and fine-tuning encryption algorithms that are resistant to quantum attacks.

"This announcement is about NIST releasing the first standards or standard ways of doing asymmetric cryptography in a quantum-safe or post-quantum way in preparation for the days that quantum computers get bigger and badder, because we do not want our digital economy to fall down and then figure out how to fix it," Crowder said.

NIST's 3 new standards, explained

The three new post-quantum cryptography standards were designed for general encryption and digital signatures, which protect information exchanged across a public network and allow identity authentication, respectively.

The three algorithms NIST chose to standardize first, after dozens of algorithms were submitted by researchers worldwide, all use different complex math problems that will challenge both classical and quantum computers.

NIST explained the three finalized standards as follows:

- **Federal Information Processing Standard (FIPS) 203:** It is intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the CRYSTALS-Kyber algorithm, which has been renamed ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism.

- **FIPS 204:** It is intended as the primary standard for protecting digital signatures. The standard uses the CRYSTALS-Dilithium algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.

- **FIPS 205:** Also designed for digital signatures, the standard employs the Sphincs+ algorithm, which has been renamed SLH-DSA, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

FIPS 203 and FIPS 204 were both created on the foundation of lattice-based cryptography, which can be more efficient and more resistant to cracking. The third standard, FIPS 205, is a stateless hash-based digital signature scheme that will further challenge quantum computers in the future.

"The trick was having really brilliant mathematicians come up with different kinds of math that future quantum computers are not expected to be good at so that they're safe against both classical and quantum," Crowder noted.

"The hard part is making sure that the implementation doesn't create its own security holes that cause it to be less secure."

In addition to these three standards, NIST said it plans to release a draft of the FIPS 206 standard in late 2024, based on FALCON.

What's more, NIST is continuing to evaluate two sets of algorithms that could serve as backup standards in the future. Even though NIST continues to evaluate other standards, NIST mathematician Dustin Moody, who heads the post-quantum cryptography standardization project, urged organizations to move forward with these three standards.

"Go ahead and start using these three," Moody stated in a NIST press release. "We need to be prepared in case of an attack that defeats the algorithms in these three standards, and we will continue working on backup plans to keep our data safe. But for most applications, these new standards are the main event."

Implementing post-quantum cryptography standards in healthcare

Healthcare organizations currently rely on cryptography to keep sensitive patient information private. As quantum computing gains traction, healthcare will need to adjust its strategy for keeping that information protected.

Crowder stressed the fact that it will likely take some time to implement these standards. To begin, Crowder recommended that organizations assess the cryptography they are currently using, evaluate the new standards, and understand what the implications are so they can start building a strategy.

Crowder suggested that organizations create an inventory of the cryptography that they are using or have built themselves and identify what they can fix now versus what they can fix later. The level of complexity within this task will depend on hygiene and how much of the code that an organization runs on was written internally."The second piece, which is also challenging, is more about getting the industry aligned to understand how we all interoperate and make sure that all of us in these systems that are across the organization or across vendors -- you can think of the supply IT supply chain for healthcare -- are aligned," Crowder noted.

"How do we make sure we are all talking the same language in terms of what standards and implementation of standards we're using so we can share information back and forth?"

Healthcare organizations have IT in their environments, but they also outsource certain IT functions and work with a variety of third-party vendors to complete critical functions. The challenge will be to ensure that the underlying platforms that healthcare relies on are also protected by these new standards.

"There is a bunch of work to do, and I think the first step is to understand what this means for you and where you are going to get started," Crowder suggested.

While it might seem daunting, organizations can begin implementing these standards by establishing a strategy for an organization-wide quantum-safe transformation. This strategy will ultimately keep sensitive data safe as quantum computing capabilities expand.

13.With post-quantum cryptography standards published, what's next?

by Dan O'Shea
https://www.fierceelectronics.com/electronics/post-quantum-cryptography-standards-published-whats-next

A technology standards effort eight years in the making has culminated in an initial three standards that mark the first series of protections against a cybersecurity threat that still could be a decade from reaching full strength.

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) this month published its first three finalized post-quantum cryptography (PQC) standards that it believes will help protect the world against the threat of quantum computers capable of executing Shor's Algorithm, which potentially could be used break down RSA and other current encryption standards. These new PQC cybersecurity algorithms have been carefully chosen, intensely debated and analyzed, and evaluated and tested at length from among dozens of candidates during a process that began in 2016 when NIST is-

sued a call for PQC candidates. The formal publishing of the finalized standards means that government agencies, corporate enterprises, and research institutions can confidently deploy security products and services incorporating these algorithms. (More details on each of the new PQC standard algorithms can be found here.)

IBM was deeply involved in the development of two of the three finalized standards, and the creator of the third has since joined IBM Research. Gregor Seiler, cryptography researcher, IBM Research, told *Fierce Electronics*, "The publication of NIST's first post-quantum cryptography standards signals to enterprises, government agencies, and supply chain vendors that quantum-safe cryptography is ready for deployment and now is the time to start the journey to becoming quantum-safe. Now that these standards are available, our hope is that product developers, enterprises, and governments are motivated to begin integrating post-quantum cryptography."

The good news is that no quantum computer exists yet that is powerful enough to execute Shor's Algorithm, so time, for now, is on their side. The less-good news is that very broad adoption and implementation of security standards can take many years, even decades, which has been the case with RSA, and organizations do not have nearly that much time on their side. Another wrinkle: Some cybersecurity attacks that have occurred in recent years may have been conducted with the intent intent to steal encrypted data and and crack that encryption in the coming years on quantum computers, meaning the bad guys may be a step ahead of the good guys in those cases as they already have driven away with the safe and just need something to open it with.

"We don't know exactly when a cryptographically relevant quantum computer — a future quantum computer powerful enough to break today's cryptography — will be available, but current estimates show it could be as soon as the next decade," Seiler said. "The transition to post-quantum cryptography won't happen overnight, and it is critical that organizations begin the process now."

He added, "This threat should not be underestimated, but the good news is that we now have post-quantum cryptography standards that have proven resistant to both traditional and quantum computers."

IBM understands the protective measures to be taken as well as it understands the threat itself, as the company has been among the pioneers in developing quantum computers over the last decade. Some might wonder, "If quantum computers present such a threat, maybe we should not continue their development," but that is not an option, as these computers also could be invaluable to helping to solve many global industrial and social problems that previously have been viewed as too intractable to address, due among things to the inability of classical computers to compute all of the possible variables in play in a reasonable time.

"Regarding the advancement of quantum computers, there is incredible progress being made in how the technology could be applied in healthcare and life sciences; finance; materials development; logistics; and other fields with today's utility-scale systems," Seiler said. "And our roadmap through the end of the decade to achieve error-corrected quantum systems will be applied to the pressing challenges in these and other domains."

Quantum computing, like almost all of classical computing, also is beginning to converge with AI. While AI will be used in the coming years to make quantum computers easier to program and manage, and ultimately more useful, the intersection of these technologies also presents a heightened threat, according to Chris Hickman, chief security officer at Keyfactor, a cybersecurity software firm.

"While Q-day [shorthand for the date by which a quantum computer will be powerful enough to break current encryption] may seem years away, security leaders need to keep in mind that AI capabilities increase the need to transition to PQC algorithms," he said via email. "Attackers will leverage the speed of AI to get that much closer to breaking encryption and, in many cases, steal valuable and sensitive data

now to decrypt in the future, including personal information, trade secrets, and national security information, wreaking havoc on the long-term security of and trust in the entities that we rely on for our digital world to operate. The confluence of these two events means the world is now racing against an unknown timeline and opponent to secure [or break] encryption."

Ultimately, the implementation of PQC standard algorithms should be viewed as another layer of protection in a multi-layer security approach, and part of a broader effort to get organizations that leverage public key infrastructure (PKI)–the hardware, software, and policies that support encryption–to become more crypto-agile, or able to manage and switch between protection measures as necessary.

David Hook, vice president of software engineering & Crypto Workshop at Keyfactor, said, "Coupled with the application of crypto-agility, use of the new algorithms will be a necessary part of future-proofing public key infrastructure systems to ensure long-term resiliency. PKI represents the cornerstone of systems that rely on secure digital identities and the exchange of encrypted data and these algorithms represent a major advance for supporting both areas."

Where to begin

So, now that an initial set of PQC standards–likely the first of many–have been published, where should organizations looking to leverage these algorithms begin?

A large number of big and small companies, veterans and start-ups, many of whom have worked in cybersecurity for years, while others among them are newer quantum specialists, have been advising that conducting an assessment of all the cryptographic assets and cryptography technologies used across an entire enterprise is a huge part of the coming transition. But, depending on the awareness level an organization has about PQC, that is not necessarily the starting point.

In fact, adopting PQC is not as simple as flipping a switch or downloading a patch–though some existing security hardware and software can be quickly upgraded. Hickman told *Fierce Electronics*, "While some hardware and software will be upgradable, others will not have the prerequisites for handling post quantum cryptography. While efforts will continue to reduce key sizes and complexities, older hardware and constrained devices such as sensors, IoT devices, and older network hardware may struggle with PQC. Software will require use of updated cryptographic libraries and all software/firmware will eventually need to be resigned using post-quantum digital signature."

With that understood, organizations will need to put in some work to prepare for PQC.

"A migration to quantum-resistant cryptography (i.e., adopting the PQC algorithms) will be significant and, without proper planning, potentially disruptive to organizations," Hickman said. "While there have been some great publications from NIST and CISA [The U.S. Cybersecurity and Infrastructure Security Agency], as well as other government agencies in Canada, EU, etc., they all share some common advice to plan for the migrations."

In Hickman's words, the process of preparing for the PQC trabsisition includes the following:

- **Education –** This is a complex area as it relates to PKI in particular and, while this is not a specific step, it is critical as organizations look to learn about the PQC and the impact this will have on PKI, SSL/TLS, signing, etc. There are significant differences with respect to key sizes, operations times, and function that having a good foundation of knowledge will help in a successful transition.

- **Cryptographic inventory –** Simply put, you can't change what you don't know exists in your infrastructure and organization. Very few organizations have a full inventory of what cryptographic

assets exist in their organizations. Cryptographic assets go beyond just keys and certificates and also take into account cryptographic libraries, inventory of roots of trust, and any embedded cryptographic functions.

- **Data risks –** Not all data is equal, and some may hold greater risk to the organization than others. It is important to understand the data is being stolen today for decryption once a cryptographically-relevant computer (one that can break traditional algorithms like RSA) is available. Therefore, it is safe to assume that no data is currently safe. Evaluating the "shelf life" of the data and the organizational impact of it being decrypted will help to establish the priorities from adoption of PQC as it relates to systems and applications that need to migrate sooner than later.

- **Engage vendors –** The entire supply chain of an organization will need to be assessed for post-quantum readiness. This includes hardware, software suppliers, cloud service providers, operating systems, etc. Now is a good time to start the conversation with those vendors to ensure they have a roadmap and implementation timelines that line up to your business requirement. Organizations will only be as strong as the weakest link in its supply chain, so it is important to evaluate and identify potential changes in the supply chain that may need to happen.

- **Transition –** Once the above has been properly planned, evaluated, and tested, organizations can begin the transition to PQC.

14.India Nears Its Quantum Moment — Completion Of First Quantum Computer Expected Soon

by Matt Swayne
https://thequantuminsider.com/2024/08/21/india-nears-its-quantum-moment-completion-of-first-quantum-computer-expected-soon/

India is nearing completion of its first quantum computer, a milestone project led by the Tata Institute of Fundamental Research (TIFR) in Mumbai. The small-scale computer is being developed by TIFR's Quantum Measurement and Control (QuMaC) lab, established 12 years ago to tackle fundamental challenges in building quantum systems, according to India Today.

Dr. R. Vijayaraghavan, head of QuMaC, described the project as a critical initial move for the country into quantum technology. "This will allow us to get into this game," he told India Today.

The project is a collaboration between TIFR, the Defence Research and Development Organisation (DRDO), and Tata Consultancy Services (TCS). Together, they are designing essential components such as the quantum processing unit, electronics, and software, each presenting its own complexities, the news service reports.

While not detailed explicitly in the article, artwork that accompanies the article shows equipment that would suggest the machine is a superconducting quantum computer. This device would be more of a model to provide a path for further advances, according to Dr. Vijayaraghavan. He added that while the equations this small-scale quantum computer can solve can be replicated by a regular laptop, the project lays the groundwork for more advanced systems.

"If we have to build a 100-qubit system, we have to start somewhere. So, this gives us all the necessary expertise in understanding the different parts of a quantum computer and where the challenges are," he explained in India Today. He compared the effort to IBM's launch of its first 5-qubit quantum computer on the cloud eight years ago, emphasizing that "for us, it's the first step."

As part of the National Quantum Mission, Dr. Vijayaraghavan leads a team of eight scientists from five institutes aiming to build a 24-qubit computer in three years and a 100-qubit computer in five years, reported India Today. Other specialist teams are working on different proposals, exploring various technological approaches using photons, neutral atoms, or trapped ions as qubits.

Despite the progress, significant scientific challenges remain. Qubits are inherently unstable and susceptible to disturbances, leading to 'decoherence'. Researchers worldwide are striving to overcome this through error-corrected qubits. "You have to show that by using such a system, you are actually solving some problem which is of relevance to industry or science or society and show that it is better, faster and cheaper," Dr. Vijayaraghavan told India Today. "That of course will be the first holy grail of useful quantum computers. We are not there yet."

In Bengaluru, startup QpiAI is also venturing into quantum computing. Led by CEO and chairman Dr. Nagendra Nagaraja, the company is constructing a 25-qubit quantum computer, with plans to unveil it by the end of the year, according to the news service. With $6 million in funding, QpiAI intends to offer the platform to customers via cloud services and supply systems to top institutes and research groups across India.

"Our vision is to integrate AI and quantum computing in enterprises," Dr. Nagaraja told India Today, highlighting the potential for Indian companies to compete globally. "The more companies you have in advanced technology, the wealthier a nation. It's as simple as that."

The National Quantum Mission's allocation of Rs 6,000 crore — about $720 million US — underscores the government's commitment to this emerging field. While the investment is substantial relative to historical R&D funding in India, the vastness of quantum technology necessitates focused and strategic use of these resources, according to India Today. Early economic impacts are expected in industries such as chemicals, life sciences, financ, and mobility.

Dr. Nagaraja pointed out several areas where quantum computers and artificial intelligences could drive new levels of innovation, including areas of global concern, such as sustainable energy and cost-effective manufacturing.

"If we have 300 error-corrected qubits, then I think material science is all disrupted," he said.

15.Challenges of deploying PQC globally

by Cliff Saran

https://www.computerweekly.com/news/366605462/Challenges-of-deploying-PQC-globally

The US National Institute of Standards and Technology (NIST) has announced three standards for post-quantum cryptography (PQC). But for PQC to work, all devices will need to have the technology installed. This is a massive project because some devices are difficult to access, and some may not be powerful enough to run the new algorithms. There are also questions over whether the techniques used for PQC are strong enough, as the cryptography standards use module lattice-based algorithms that some quantum researchers believe can be hacked.

In a research note looking at the broad economic impact of the PQC standards, ratings agency Moody's noted that challenges in error correction, scalability, talent shortages and limited computing power currently mitigate the risk of quantum computing cracking strong encryption. However, many experts recommend the swift adoption of quantum-resistant algorithms, since cyber criminals could harvest data now and wait for the arrival of powerful, reliable quantum computing technology.

Karl Holmqvist, founder and CEO of Lastwall, a company specialising in quantum resilience, said: "Thirty years ago, in 1994, Peter Shor demonstrated that we would need approximately 4,100 qubits to factor 2048-bit RSA, which is the most broadly deployed asymmetric encryption algorithm. At that time, we had no quantum computers available, and people questioned if we would ever develop a functional quantum computer."

The Moody's report stated that by using Shor's algorithm, a quantum algorithm specifically designed for finding the prime factors of an integer, quantum computers would be able to factor integers exponentially faster, essentially breaking asymmetric encryption (such as the widely used RSA-2048 cryptosystem) altogether.

Experts think quantum computers will be able to break asymmetric encryption in five to 30 years. The Moody's report quoted a 2022 poll of 37 experts for the Global Risk Institute's *Quantum threat timeline report 2022*, which reported that over half (54%) were optimistic that within 15 years quantum computers would be able to crack RSA-2048 encryption in 24 hours.

Holmqvist said that five years ago, KTH and Google researchers demonstrated that a 20-million-qubit system would crack 2048-bit RSA in less than eight hours. However, he pointed out that over 3,500 qubits are needed to make each stable logical qubit, since qubits are extremely error-prone. Nevertheless, quantum technology is advancing. "Time is not on our side to change to quantum-resistant ciphers. We need to address this now – it's time to get to work and eliminate outdated cryptography," said Holmqvist.

As big as Y2K

According to Moody's, the ability to break asymmetric encryption could have profound repercussions on e-commerce. Pointing to the US International Trade Administration projections, Moody's reported that global e-commerce is set to grow to $41.7tn a year by 2027.

"If there is a loss of trust in online transactions, these flows would be at risk. Air traffic systems and GPS signals could also be manipulated, risking lives. The ability to break this encryption could also imperil companies' intellectual property as well as governments' classified documents," the Moody's report warned.

Moody's also noted that the transition to PQC is likely to take a long time and will also be extremely expensive. It estimated that implementing new cryptographic standards across devices could take 10 to 15 years due to operational challenges. While the cost of the transition is hard to estimate, it said that parallels can be drawn with the expensive, large-scale efforts required to address the Y2K bug.

For instance, as Moody's pointed out, some devices are in hard-to-reach places, such as satellites in orbit, and some types of hardware, such as in cars and cash machines, are difficult to update. Its report referenced data from US officials that shows implementing a new cryptographic standard in devices widely could take 10 to 15 years.

Beyond the challenges of a wide-scale roll-out of PQC, implementing the new encryption standards may prove very difficult, as Roberta Faux, field chief technology officer at Arqit and former NSA cryptograph-

er, explained.

“We are still in the early stages of a fast-moving industry, and unfortunately even the secure implementation of these standards will be a difficult process,” she said. “These aren’t ‘drop-in’ solutions. As we migrate systems, we will find all kinds of interoperability issues, alongside the plethora of vulnerabilities and downtime that come from making systems more complex. It’s a long-term project with a lot of uncertainty.”

However, Moody’s noted that the rapid deployment of PQC by some key technology and internet infrastructure companies would speed up protections for swathes of users.

Global adoption

Questions are also being raised over whether the UK and Europe should adopt the NIST standards. Faux said the German and French governmental cyber security agencies are shying away from endorsing the NIST post-quantum key exchange.

Ekaterina Almasque, general partner at early-stage tech venture capital firm OpenOcean, said: “Europe must take the lead in post-quantum cryptography standards, not just ride on the US’s coattails. That requires strategic thinking.”

Almasque said the US government has already communicated to companies working on sensitive projects that they may soon be required to use quantum encryption algorithms. “If Europe and the UK want to direct their own quantum funding efficiently and build public confidence in PQC, they need a clear and well-communicated strategy that reaches startups, the public sector and other key stakeholders,” she added.

“While Europe and the EU’s diversity is a strength, it could easily become a vulnerability if we don’t introduce a cohesive quantum strategy that ensures all member states are aligned in their quantum defences.”

There appears to be wide industry consensus around the new NIST PQC standards. However, as Arqit’s Faux points out, some quantum cryptography experts like Michele Mosca have raised concerns that the lattice algorithms on which NIST has based its PQC encryption standards may be broken within a decade.

16.Google Outlines Implementation of NIST’s Post-Quantum Cryptography Standard

by Royal Hansen and Phil Venables
https://www.hpcwire.com/off-the-wire/google-outlines-implementation-of-nists-post-quantum-cryptography-standard/

In this recent blog post, Google’s Royal Hansen and Phil Venables provide an in-depth look at the newly finalized post-quantum cryptography standards released by NIST. They explore what these standards mean for the future of encryption, how Google is already implementing them, and offer guidance for or-

ganizations preparing for the transition to a quantum-resistant security landscape.

The National Institute of Standards and Technology (NIST) just released three finalized standards for post-quantum cryptography (PQC) covering public key encapsulation and two forms of digital signatures. In progress since 2016, this achievement represents a major milestone towards standards development that will keep information on the Internet secure and confidential for many years to come.

Here's a brief overview of what PQC is, how Google is using PQC, and how other organizations can adopt these new standards. You can also read more about PQC and Google's role in the standardization process in this 2022 post from Cloud CISO Phil Venables.

What Is PQC?

Encryption is central to keeping information confidential and secure on the Internet. Today, most Internet sessions in modern browsers are encrypted to prevent anyone from eavesdropping or altering the data in transit. Digital signatures are also crucial to online trust, from code signing proving that programs haven't been tampered with, to signals that can be relied on for confirming online identity.

Modern encryption technologies are secure because the computing power required to "crack the code" is very large; larger than any computer in existence today or the foreseeable future. Unfortunately, that's an advantage that won't last forever. Practical large-scale quantum computers are still years away, but computer scientists have known for decades that a cryptographically relevant quantum computer (CRQC) could break existing forms of asymmetric key cryptography.

PQC is the effort to defend against that risk, by defining standards and collaboratively implementing new algorithms that will resist attacks by both classical and quantum computers.

You don't need a quantum computer to use post-quantum cryptography, or to prepare. All of the standards released by NIST today run on the classical computers we currently use.

How Is Encryption at Risk?

While a CRQC doesn't exist yet, devices and data from today will still be relevant in future. Some risks are already here:

- **Stored Data** Through an attack known as *Store Now, Decrypt Later*, encrypted data captured and saved by attackers is stored for later decryption, with the help of as-yet unbuilt quantum computers.

- **Hardware Products** Defenders must ensure that future attackers cannot forge a digital signature and implant compromised firmware, or software updates, on pre-quantum devices that are still in use.

For more information on CRQC-related risks, see our PQC Threat Model post.

How Can Organizations Prepare for PQC Migrations?

Migrating to new cryptographic algorithms is often a slow process, even when weaknesses affect widely-used crypto systems, because of organizational and logistical challenges in fully completing the transition to new technologies. For example, NIST deprecated SHA-1 hashing algorithms in 2011 and recommends complete phase-out by 2030.

That's why it's crucial to take steps now to improve organizational preparedness, independent of PQC,

with the goal of making your transition to PQC easier.

These crypto agility best practices can be enacted anytime:

- **Cryptographic inventory** Understanding where and how organizations are using cryptography includes knowing what cryptographic algorithms are in use, and critically, managing key material safely and securely

- **Key rotation** Any new cryptographic system will require the ability to generate new keys and move them to production without causing outages. Just like testing recovery from backups, regularly testing key rotation should be part of any good resilience plan

- **Abstraction layers** You can use a tool like Tink, Google's multi-language, cross-platform open source library, designed to make it easy for non-specialists to use cryptography safely, and to switch between cryptographic algorithms without extensive code refactoring

- **End-to-end testing** PQC algorithms have different properties. Notably, public keys, ciphertexts, and signatures are significantly larger. Ensure that all layers of the stack function as expected

Our 2022 paper "Transitioning organizations to post-quantum cryptography" provides additional recommendations to help organizations prepare and this recent post from the Google Security Blog has more detail on cryptographic agility and key rotation.

Google's PQC Commitments

Google takes these risks seriously, and is taking steps on multiple fronts. Google began testing PQC in Chrome in 2016 and has been using PQC to protect internal communications since 2022. In May 2024, Chrome enabled ML-KEM by default for TLS 1.3 and QUIC on desktop. ML-KEM is also enabled on Google servers. Connections between Chrome Desktop and Google's products, such as Cloud Console or Gmail, are already experimentally protected with post-quantum key exchange.

Google engineers have contributed to the standards released by NIST, as well as standards created by ISO, and have submitted Internet Drafts to the IETF for Trust Expressions, Merkle Tree Certificates, and managing state for hash-based signatures. Tink, Google's open source library that provides secure and easy-to-use cryptographic APIs, already provides experimental PQC algorithms in C++, and our engineers are working with partners to produce formally verified PQC implementations that can be used at Google, and beyond.

As we make progress on our own PQC transition, Google will continue to provide PQC updates on Google services, with updates to come from Android, Chrome, Cloud, and others.

17.NIST Has Finalized the First Three PQC Algorithms; 45 More Are Still in the Pipeline

by GQI

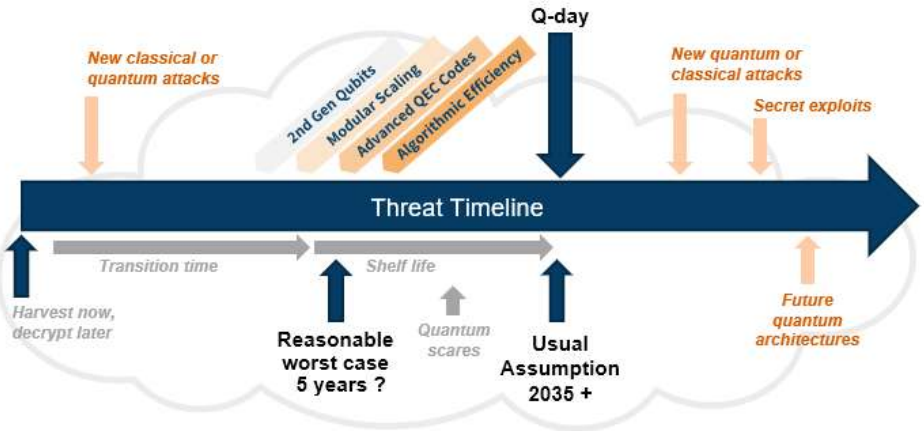
https://quantumcomputingreport.com/nist-has-finalized-the-first-three-pqc-algorithms-45-more-are-still-in-the-pipeline/

After eight years of intensive review and analysis, the U.S. National Institute of Standards and Technology (NIST) has released the final, approved specifications for the first three Post Quantum Cryptography (PQC) algorithms. The effort start in 2016 with 82 algorithms initially submitted with 69 algorithms accepted for further review. And after three rounds of analysis, NIST has selected the first three algorithms for final approval. The three algorithms include the following:

Specification Number	Name	Based Upon	Usage Type
FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*	ML-KEM	Crystals-Kyber	Key Encapsulation
FIPS 204, *Module-Lattice-Based Digital Signature Standard*	ML-DSA	Crystals-Dilithium	Digital Signature
FIPS 205, *Stateless Hash-Based Digital Signature Standard*	SLH-DSA	SPHINCS+	Digital Signature

For enterprise Chief Information Officers (CIO) and Chief Security Officers (CSO) this is a signal for them to start implementing PQC in their IT infrastructure to protect their organizations against cybersecurity attacks from future large scale quantum computers that run algorithms which break existing encryption codes. NIST is encouraging computer system administrators to begin transitioning to these new standards as soon as possible. The U.S. government has put in motion plans to upgrade all the government's IT systems to the new standards. A new report titled Report on Post Quantum Cryptography provides and outline of the strategy and timeline for the government to upgrade its internal systems to these new standards and estimates they will spend about $7.1 billion on it between 2025 and 2035.

Global Quantum Intelligence (GQI) is also recommending that IT departments implement these new algorithms as soon as possible. In our Quantum Safe Outlook report, we point out that users consider a **Worst Case** mindset, because of the possible that an algorithm that attacks existing asymmetric encryption codes is found earlier than anticipated.



A number of commercial companies have also issued blogs and press releases in support of the algo-

rithms and a recommendation to start now. These include a press release and blog which point out that IBM researchers had a hand in developing these three algorithms. Other announcements have come out today from SandboxAQ, Terra Quantum, Thales, PQShield, Quantum Xchange, and many others also in support of this recommendation.

But Wait! There's More!

It is important to understand that there are still many more years of work left in this program. One of the concerns about the software based PQC algorithms is that no one has been able to create a theoretical proof that these new algorithms are unbreakable. What can be proven is that some algorithms can be broken by showing people how it can be done. This did occur with several of the original 69 algorithms that NIST started out with in 2016. The ones that have survived and are being standardized survived years of attempts from researchers trying to break them without seeing success. But that does not say that someday in the future, some clever PhD student will find a way to break one of these algorithms in a way that no one had done before.

Because of this potential jeopardy, NIST is pursuing a strategy of developing and finalizing several different asymmetrical encryption algorithms using a variety of different mathematical approaches such that if one is eventually broken users can switch to one of the other ones. They are also recommending that IT departments utilize a strategy of quantum agility in the deployment. This implement the upgrades in a modular way, such that if one needs to replace one algorithm with another it can be easily done.

So this is where the 45 other candidates come in. As shown in the table above, of the three algorithms that have been finalized, one is intended for usage for key encapsulation and the other two are intended for use with digital signatures. That is not enough that they are continue to work on finalizing and approving more algorithms.

The next algorithm expected to be standardized is called FALCON. It uses a structured lattice class of algorithms similar to ML-DSA. It was selected along with the first three of the project but hasn't yet gone through the full process of developing a draft standard, receiving comments, making corrections, and receiving the final Secretary of Commerce's approval. The draft standard for FALCON is expected to be available in late 2024 with final approval in 2025.

Next, there were four algorithms analyzed during Round 3 with the others where NIST felt that additional analysis was needed. So these algorithms which are named BIKE, HQC, SIKE, and Classic McEliece are currently being analyzed in a Round 4 for additional algorithms to use in key encapsulation. BIKE, HQC, SIKE and Classic McEliece are based upon a code-based mathematical approach while SIKE is based on an Isogeny mathematical approach. There were chosen by NIST for Round 4 because the are all based upon a different approach than the ML-KEM already chosen for key encapsulation and provide some diversity and protection against being broken. An issue was found with SIKE, so we do not expect it to be standardized. But we do expect that NIST will approve one of the other three code-based algorithms.

Finally, in 2022 NIST was concerned that they also need additional diversity in algorithms for the digital signatures. SLH-DSA and Falcon were both based upon a Lattice approach and SPHINCS+ is based upon a Hash based approach, they requested additional submissions for new digital signature algorithms to be evaluated that don't use a Lattice approach. In July 2023, they received 40 new candidate algorithms and they are current in a Round 1 analysis of these. These 40 candidates include 6 Code-based, Isogeny-based, 7 Lattice based, 7 MPC-In-The-Head, 10 Multivariate-based, 4 Symmetric-based, and 5 others types of approaches. A list of these 40 additional signature candidates has been posted on the NIST website here.

For more about the announcement of the standardization of these first three algorithms, you can view an

announcement posted on the NIST website here and also another announced that will be posted in the U.S. Federal Register here. For an overview of the overall project that includes information on all the rounds and all the algorithm candidates, you can visit the NIST PQC project webpage here.

18.NIST Releases First 3 Finalized Post-Quantum Encryption Standards

by Chad Boutin
https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) has finalized its principal set of encryption algorithms designed to withstand cyberattacks from a quantum computer.

Researchers around the world are racing to build quantum computers that would operate in radically different ways from ordinary computers and could break the current encryption that provides security and privacy for just about everything we do online. The algorithms announced today are specified in the first completed standards from NIST's post-quantum cryptography (PQC) standardization project, and are ready for immediate use.

The three new standards are built for the future. Quantum computing technology is developing rapidly, and some experts predict that a device with the capability to break current encryption methods could appear within a decade, threatening the security and privacy of individuals, organizations and entire nations.

"The advancement of quantum computing plays an essential role in reaffirming America's status as a global technological powerhouse and driving the future of our economic security," said Deputy Secretary of Commerce Don Graves. "Commerce bureaus are doing their part to ensure U.S. competitiveness in quantum, including the National Institute of Standards and Technology, which is at the forefront of this whole-of-government effort. NIST is providing invaluable expertise to develop innovative solutions to our quantum challenges, including security measures like post-quantum cryptography that organizations can start to implement to secure our post-quantum future. As this decade-long endeavor continues, we look forward to continuing Commerce's legacy of leadership in this vital space."

The standards — containing the encryption algorithms' computer code, instructions for how to implement them, and their intended uses — are the result of an eight-year effort managed by NIST, which has a long history of developing encryption. The agency has rallied the world's cryptography experts to conceive, submit and then evaluate cryptographic algorithms that could resist the assault of quantum computers. The nascent technology could revolutionize fields from weather forecasting to fundamental physics to drug design, but it carries threats as well.

"Quantum computing technology could become a force for solving many of society's most intractable problems, and the new standards represent NIST's commitment to ensuring it will not simultaneously disrupt our security," said Under Secretary of Commerce for Standards and Technology and NIST Director Laurie E. Locascio. "These finalized standards are the capstone of NIST's efforts to safeguard our confidential electronic information."

Encryption carries a heavy load in modern digitized society. It protects countless electronic secrets, such as the contents of email messages, medical records and photo libraries, as well as information vital to

national security. Encrypted data can be sent across public computer networks because it is unreadable to all but its sender and intended recipient.

Encryption tools rely on complex math problems that conventional computers find difficult or impossible to solve. A sufficiently capable quantum computer, though, would be able to sift through a vast number of potential solutions to these problems very quickly, thereby defeating current encryption. The algorithms NIST has standardized are based on different math problems that would stymie both conventional and quantum computers.

“These finalized standards include instructions for incorporating them into products and encryption systems,” said NIST mathematician Dustin Moody, who heads the PQC standardization project. “We encourage system administrators to start integrating them into their systems immediately, because full integration will take time.”

Moody said that these standards are the primary tools for general encryption and protecting digital signatures.

NIST also continues to evaluate two other sets of algorithms that could one day serve as backup standards.

One of these sets consists of three algorithms designed for general encryption but based on a different type of math problem than the general-purpose algorithm in the finalized standards. NIST plans to announce its selection of one or two of these algorithms by the end of 2024.

The second set includes a larger group of algorithms designed for digital signatures. In order to accommodate any ideas that cryptographers may have had since the initial 2016 call for submissions, NIST asked the public for additional algorithms in 2022 and has begun a process of evaluating them. In the near future, NIST expects to announce about 15 algorithms from this group that will proceed to the next round of testing, evaluation and analysis.

While analysis of these two additional sets of algorithms will continue, Moody said that any subsequent PQC standards will function as backups to the three that NIST announced today.

“There is no need to wait for future standards,” he said. “Go ahead and start using these three. We need to be prepared in case of an attack that defeats the algorithms in these three standards, and we will continue working on backup plans to keep our data safe. But for most applications, these new standards are the main event.”

More Details on the New Standards

Encryption uses math to protect sensitive electronic information, including secure websites and emails. Widely used public-key encryption systems, which rely on math problems that computers find intractable, ensure that these websites and messages are inaccessible to unwelcome third parties. Before making the selections, NIST considered not only the security of the algorithms’ underlying math, but also the best applications for them.

The new standards are designed for two essential tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication. NIST announced its selection of four algorithms — CRYSTALS-Kyber, CRYSTALS-Dilithium, Sphincs+ and FALCON — slated for standardization in 2022 and released draft versions of three of these standards in 2023. The fourth draft standard based on FALCON is planned for late 2024.

While there have been no substantive changes made to the standards since the draft versions, NIST has changed the algorithms' names to specify the versions that appear in the three finalized standards, which are:

- **Federal Information Processing Standard (FIPS) 203**, intended as the primary standard for general encryption. Among its advantages are comparatively small encryption keys that two parties can exchange easily, as well as its speed of operation. The standard is based on the **CRYSTALS-Kyber** algorithm, which has been renamed ML-KEM, short for Module-Lattice-Based Key-Encapsulation Mechanism.

- **FIPS 204**, intended as the primary standard for protecting digital signatures. The standard uses the **CRYSTALS-Dilithium** algorithm, which has been renamed ML-DSA, short for Module-Lattice-Based Digital Signature Algorithm.

- **FIPS 205**, also designed for digital signatures. The standard employs the Sphincs+ algorithm, which has been renamed **SLH-DSA**, short for Stateless Hash-Based Digital Signature Algorithm. The standard is based on a different math approach than ML-DSA, and it is intended as a backup method in case ML-DSA proves vulnerable.

Similarly, when the draft FIPS 206 standard built around FALCON is released, the algorithm will be dubbed **FN-DSA**, short for FFT (fast-Fourier transform) over NTRU-Lattice-Based Digital Signature Algorithm.

19.Worried about the Windows BitLocker recovery bug? 6 things you need to know

by Ed Bott
https://www.zdnet.com/article/worried-about-the-windows-bitlocker-recovery-bug-6-things-you-need-to-know/

Five years ago, after a particularly embarrassing run of flawed Windows updates, Microsoft vowed to do better. Part of its cleanup program included the introduction of a "release health dashboard" that documents the status of known issues with every update.

That transparency is a good thing, to be sure, but sometimes those disclosures raise more questions than they answer. A case in point is the July 2024 security update, which the release health dashboard flagged as having a known issue affecting PCs running Windows 10 and Windows 11 and multiple versions of Windows Server. (See "Device might boot into BitLocker recovery with the July 2024 security update.")

On affected PCs and servers, Windows refuses to boot to the normal login screen.

As the Microsoft report dryly notes: "This screen does not commonly appear after a Windows update." The advisory does not provide a cause for the issue, but it offers one clue: "You are more likely to face this issue if you have the Device Encryption option enabled in Settings under Privacy & Security -> Device encryption."

After entering the recovery key, Windows starts up normally. If you can't find the recovery key, your data is lost for good.

That sounds bad, but the story is not nearly as alarming as media coverage has made it sound. I've been digging into this issue for the past week. Here's what I've found.

How widespread is this bug?

In typically frustrating fashion, Microsoft provided no details about how common this issue is or what triggers it. Obviously, it doesn't affect every machine that received the July 2024 security update. (If that were the case, the update would have been pulled immediately and it would have been front-page news.) It hasn't occurred on any machine I've tested, and I haven't heard from any readers affected by it. When I searched on Microsoft's community forums, I didn't find any reports related to this bug.

On Reddit, I did find several network administrators reporting that this issue affected multiple machines in their organization. (See this thread and this one for examples.) It appears all the devices were HP or Lenovo laptops that were managed on corporate networks and received firmware updates as part of the July 2024 Patch Tuesday update release.

When I asked Microsoft for additional details on the scope of the issue, a company spokesperson said: "Microsoft has nothing more to share beyond what is available in the following resources," providing links to an overview of BitLocker technology (with the Device Encryption section highlighted) and a support article titled "BitLocker drive encryption in Windows 11 for OEMs".

Why is this happening?

BitLocker is an extremely effective security option that encrypts the contents of an entire drive so that no one can access its contents without your permission. BitLocker works in conjunction with a Trusted Platform Module (TPM) and the Secure Boot feature to securely save a fingerprint of your boot configuration.

When you see the recovery prompt, that usually means that something about the boot process doesn't look right to BitLocker. So, instead of proceeding to a normal login screen, it prompts you for the recovery key. This can happen for all sorts of reasons that might or might not be related to an outside attacker.

In a separate section of the support article the Microsoft spokesperson pointed me to, there's a section titled "BitLocker recovery scenarios" that lists no fewer than 15 "examples of common events that cause a device to enter BitLocker recovery mode when starting Windows." The list includes some actions that are typical of what might happen when an unauthorized person is trying to access data on the device, such as making changes to the boot manager or the NTFS partitions on the disk, disabling the TPM, or moving the BitLocker-protected drive into a new computer.

But you can also trigger BitLocker recovery by upgrading critical early startup components, such as a BIOS or UEFI firmware upgrade, which is what I suspect happened here. Firmware upgrades are supposed to suspend BitLocker encryption while they're installed, but it appears that this isn't happening on the laptops in question.

What's the difference between BitLocker and Device Encryption?

Device Encryption is a feature that's standard on all modern PCs designed for Windows 11. It works with all Windows editions (including Home edition), encrypting the contents of the system drive. It's on by default but is only activated when you sign in with a free Microsoft account or an Entra ID account. In those cases, the recovery key is automatically saved in the account dashboard for your account.

BitLocker Drive Encryption is a feature that's available for business customers, only on Pro, Enterprise, and Education editions of Windows. It allows you to encrypt the system volume as well as secondary

drives and removable media, such as USB flash drives. This version of BitLocker includes a complete set of management tools.

Is your system drive encrypted?

The Device Encryption feature is controlled with a simple toggle switch in Windows Settings. On Windows 11, you can find this switch by going to Settings > Privacy & security > Device Encryption.

If this switch isn't available, then your system, for one reason or another, doesn't support encryption. One common reason is that the TPM is unavailable; you can find the details by opening the System Information utility (Msinfo32.exe) using an administrator's credentials. Look for a line labeled Device Encryption Support, at the bottom of the System Summary page.

There, you can search for your device name and confirm that the encryption key is accessible. The BitLocker recovery screen contains a Key ID; compare the group of eight characters at the beginning of that key with the Key ID column on the web page to confirm that you've found the right one. You can copy that recovery key to a text file, save the text file in a safe place in the cloud or on a USB flash drive, and even print the recovery key out and store it in a secure location where you can find it if needed.

If you'd rather use PowerShell to find your encryption key, open PowerShell as an administrator and use the following command:

(Get-BitLockerVolume -MountPoint C).KeyProtector

That process should give you all the information you need.

Should you turn encryption off?

If you're worried about the possibility that you'll be locked out of your PC by a BitLocker failure, you can turn device encryption off by going to its page in Settings and sliding the Device Encryption page to the Off position.

Have you saved a backup copy of your recovery key?

As mentioned earlier, Windows automatically saves a copy of your recovery key to your Microsoft account. If you're ever prompted to enter that key, you can find it by opening a browser window (on a PC, Mac, or mobile device) and going to microsoft.com/recoverykey.

Sign in with the account you used for the device where you're seeing the recovery prompt.

However, that's an extreme solution to a problem that's unlikely to affect you. If you've got a backup copy of your recovery key, you're in no risk of losing data, and you're fully protected from having your digital life turned upside down by a thief who steals your laptop and accesses your data files.

20.Russia blocks Signal messaging app as authorities tighten control over information

https://apnews.com/article/russia-crackdown-signal-messenger-blocked-2ad-c9c67fc749727c41375f5b5ffb2a3

Russia's state communications watchdog said Friday it has blocked access to the Signal messaging app, the latest move in the authorities' efforts to tighten controls over information amid the fighting in Ukraine.

The agency, Roskomnadzor, said it made the decision because of Signal's "violation of the requirements of Russian legislation which must be observed to prevent the messenger's use for terrorist and extremist purposes."

Signal uses end-to-end encryption, making it difficult for the Russian government to intercept communications.

Russian authorities expanded their crackdown on dissent and free media after Russian President Vladimir Putin sent troops into Ukraine in February 2022. They have blocked multiple independent Russian-language media outlets critical of the Kremlin, and cut access to Twitter, which later became X, as well as Meta's Facebook and Instagram.

In the latest blow to the freedom of information, YouTube faced mass outages on Thursday following repeated slowdowns in recent weeks.

Russian authorities have blamed the slowdowns on Google's failure to upgrade its equipment in Russia, but many experts have challenged the claim, arguing that the likely reason for the slowdowns and the latest outage was the Kremlin's desire to shut public access to a major platform that carries opposition views.

21.Secure-IC signs International Collaboration with Taiwan Quantum Safe Association and PQC-CIA

https://www.design-reuse.com/news/56625/secure-ic-with-taiwan-quantum-safe-association-pqc-cia.html

The collaboration focuses on promoting Post-Quantum cybersecurity and the development of semiconductor industry intellectual property (IP) chips. Today, Taiwan Quantum Security Industry Association (TQSA) announced collaborations with global provider of end-to-end cybersecurity solutions for embedded systems, Secure-IC, and the Post- Quantum Cybersecurity Industry Alliance (PQC-CIA). The three entities have signed a memorandum of understanding (MOU) focusing on promoting the development of semiconductor industry intellectual property (IP) chips. Together, they will organize workshops on PQC Post-Quantum security for high-tech semiconductor industries, assist in the implementation of compliant chip testing collaborations, and accelerate entry into international markets.

Hassan Triqui, Secure-IC's CEO and Co-Founder said, "Our partnership with TQSA and PQC-CIA represents a unified global effort to secure the future of digital security. Leveraging Secure-IC's extensive expertise, grounded in many years of dedicated research, innovative PQC algorithm creation, and ad-

vanced PQC-based product development, we aim to deliver state-of-the-art PQC solutions. This collaboration will robustly fortify the semiconductor industry against the looming quantum threats."

Vice Chairman Zhang Peiren of TQSA stated, "Promoting widespread encryption technology adoption and establishing an industry supply chain have been the core missions of our association since its inception. Today's MOU signing with Secure-IC and PQC-CIA marks a significant step in turning our vision into action. Our collaboration starts in the semiconductor industry, with a focus on aiding high-tech semiconductor industries through hands-on PQC technical knowledge transfer, secure chip design, and international certification consultancy services for market entry."

With the rapid advancement of quantum computing technology, experts predict that within 15 years, quantum computers will possess sufficient computational power to potentially decrypt current encryption mechanisms in minutes. This poses significant challenges to sensitive data protection, network communications security, online financial transactions, and more. Since 2016, in response to the impending obsolescence of current encryption mechanisms in the era of quantum computing, the National Institute of Standards and Technology (NIST) of the United States has initiated the PQC Cryptography Standardization Competition. Later this year, four PQC postquantum cryptography algorithms will be standardized to mitigate the risks posed by quantum computing.

Vice Chairman Zhang further emphasized, "Given the limited time until the quantum era arrives, rigorous verification of encryption mechanisms and widespread migration operations are paramount to ensuring the continued robust operation of our digital society and industries. Practical implementation should prioritize sectors based on their importance and urgency. Domestically, various application scenario validations and PQC migration operations have been initiated by public sectors. The semiconductor industry, a vital core industry of our nation, requires urgent establishment of security measures. Therefore, today's declaration of collaboration through the MOU signing between TQSA, Secure-IC, and the Post-Quantum Cybersecurity Industry Alliance underscores our commitment to expanding industry resilience."

22.Deep dive into quantum-resistant cryptography for email security

by Isla Sibanda
https://www.computerweekly.com/feature/Deep-dive-into-quantum-resistant-cryptography-for-email-security

Imagine waking up one day to find that all your confidential emails are suddenly an open book for anyone with a powerful enough computer. Sounds like a nightmare, right? Well, with the rapid advancement of quantum computing, despite the challenges involved, this scenario isn't as far-fetched as you might think.

Once fully realised, quantum computers have the potential to crack many of the encryption methods we currently rely on to keep our digital communications safe. And let's face it: email is still the backbone of our online interactions, both personal and professional.

What's the solution? How do we maintain the confidentiality and integrity of email communications in a post-quantum world? The answer is quantum-resistant cryptography.

At its heart, quantum computing applies the principles of quantum mechanics to process information. Instead of using bits (0s and 1s), quantum computers use units known as quantum bits or qubits.

One unique aspect of qubits is that they can exist in multiple states at the same time, thanks to a phenomenon called quantum superposition. It's like being able to flip a coin and have it land on both heads and tails at the same time – but that's not all. Qubits can also be entangled, meaning the state of one qubit can instantly affect the state of another, no matter the distance between them.

So, how do quantum computers differ from classical computers? While classical computers are great for straightforward, sequential calculations, quantum computers excel at solving complex problems with multiple variables. They can explore countless possibilities simultaneously, making them ideal for tasks such as breaking encryption, modelling molecular structures or optimising complex systems.

The potential capabilities of fully realised quantum computers are staggering. They could revolutionise drug discovery, optimise financial models, enhance artificial intelligence, and, yes, crack many of our current encryption methods.

Impact of quantum computing on current encryption methods

Most email encryption today relies on public-key cryptography, with Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC) being the most popular. These systems work on the principle that some mathematical problems are very hard for classical computers to solve.

For instance, RSA's security is based on the difficulty of factoring large numbers. It's like trying to figure out which two numbers were multiplied together to get a really big number – easy to do in one direction, but a nightmare to reverse.

Quantum computers, with their ability to perform many calculations simultaneously, are poised to turn these "tough problems" into a walk in the park, rendering current encryption methods vulnerable.

A prime example of this vulnerability is Shor's algorithm, which can factor large integers exponentially faster than the best-known algorithms running on classical computers. A sufficiently powerful quantum computer running Shor's algorithm could break these encryption methods in minutes, compared with the billions of years it would take classical computers.

This capability poses a direct threat to RSA, which relies on the difficulty of factoring large numbers as its security foundation. Similarly, ECC and other encryption methods that depend on the hardness of the discrete logarithm problem are also at risk.

The implications for email security are immense, which is why the cyber security community is already hard at work developing quantum-resistant cryptography.

Understanding quantum-resistant cryptography

Quantum-resistant cryptography, also known as post-quantum cryptography, is all about developing encryption methods that can stand up to both classical and quantum computers. It relies on mathematical problems that are tough to crack for both classical and quantum machines.

Why not just use quantum encryption to fight quantum decryption? Unfortunately, while quantum key distribution is possible, it requires specialised hardware that's not practical for widespread use, especially in something as ubiquitous as email. Instead, it's easier to focus on creating classical algorithms that can resist quantum attacks.

Quantum-resistant algorithms for email security

Several promising algorithms have emerged in the fight against quantum threats to email security. These include:

- **Lattice-based cryptography:** These algorithms rely on the hardness of problems related to lattice structures in high-dimensional spaces. An example of a lattice-based algorithm is Crystals-Kyber. It's fast, has reasonably small key sizes, and is versatile enough for various applications, including email encryption.

- **Hash-based cryptography:** This approach utilises cryptographic hash functions to construct secure digital signatures. They're not the most efficient, with large signature sizes, but they're trusted due to their simplicity and the extensive study of hash functions. For email, they're more suitable for signing than encryption.

- **Code-based cryptography:** This approach uses error-correcting codes, which are typically used to ensure accurate data transmission. In cryptography, they're flipped on their head to create hard-to-solve problems. The McEliece system is a classic example. However, these algorithms tend to have large key sizes, which can be a drawback for email systems where efficiency is key.

- **Multivariate polynomial cryptography:** These algorithms use systems of multivariate polynomials to create complex mathematical puzzles. They're known for fast signature verification, which could be great for quickly checking the authenticity of emails. However, they often have large key or signature sizes.

For email security, we're likely to see a mix of these approaches. Lattice-based algorithms such as IBM's z16 might handle the asymmetric part (like key exchange), while beefed-up symmetric algorithms secure the actual message content. Hash-based signatures could verify the sender's identity.

Integration challenges

While technically possible, integrating quantum-resistant cryptography into existing email systems comes with its fair share of headaches.

Most email systems are built around current encryption standards such as RSA and ECC. Swapping these out for quantum-resistant algorithms requires significant changes to the underlying infrastructure, potentially breaking interoperability with older systems.

Some post-quantum algorithms come with larger key sizes and slower processing times. In a world where we expect our emails to zip across the globe in seconds, this could lead to noticeable delays. Last, with these potentially larger keys and new algorithms, we need robust systems to generate, distribute and store these keys securely.

In addition, properly testing quantum-resistant cryptographic methods and their effectiveness might be time-consuming, but it's still more reliable and efficient compared with classic data redaction techniques, as even script kiddies can bypass it nowadays if they get their hands on sensitive emails.

Strategies for transitioning to quantum-resistant cryptography

Start by assessing your organisation's readiness. Take stock of your current encryption methods, identify vulnerable systems and determine the potential impact of a quantum breach. Additionally, determine the resources required for a seamless transition.

As part of assessing your organisation's readiness, you should evaluate your digital asset management system, especially if your organisation deals with large volumes of multimedia email attachments. This ensures all digital assets are properly catalogued, and provides clarity on the types of data being shared via email, how frequently and by whom.

To use an example, highly sensitive documents might require immediate implementation of the strongest quantum-resistant encryption, while less critical communications could be transitioned more gradually.

Start with the most critical systems and work your way through your infrastructure. For instance, begin with email signatures, then move to key exchange protocols, and finally to full message encryption. This phased approach minimises disruptions, and allows for adjustments based on real-world feedback and performance metrics.

Finally, don't forget the human element in email security. Employee training and awareness are crucial. Your team needs to understand the why and how of these new security measures. Awareness programmes and hands-on training ensure that staff are equipped to handle the transition effectively, maintain security practices and minimise potential risks.

Broader implications of quantum-resistant cryptography

The shift to quantum-resistant cryptography will have far-reaching consequences – not just in email security, but in many other domains.

In terms of global cyber security, quantum-resistant cryptography is set to redefine global cyber security power dynamics. Countries and organisations that get ahead in developing and implementing quantum-resistant methods could gain a significant edge, potentially altering the balance of cyber power and influencing geopolitical relations.

Quantum-resistant cryptography will also be crucial for protecting national security interests. Government agencies and military operations rely heavily on secure communications, so transitioning to post-quantum cryptographic standards is vital to safeguarding sensitive information from future quantum-based cyber threats.

When it comes to data privacy, quantum-resistant cryptography will become the new gold standard. In a world where quantum computers could potentially crack current encryption methods, quantum-resistant algorithms will perhaps be the only way to maintain the privacy and confidentiality of personal and corporate data, and uphold trust in digital communications.

Wrapping up

The quantum age will undoubtedly revolutionise computing, but it also threatens to upend the very foundations of our current cyber security infrastructure.

The good news? We're not defenceless. Quantum-resistant cryptography offers a gateway to a new era of digital security, where our emails – and all our digital communications – can remain private and secure, no matter what computational advances the future holds.

23.PQShield CEO predicts major post-quantum shift as Apple and Google lead the charge

by Nancy Liu
https://www.sdxcentral.com/articles/interview/pqshield-ceo-predicts-major-post-quantum-shift-as-apple-and-google-lead-the-charge/2024/08/

Several tech giants, including Apple and Google, have embarked on their post-quantum cryptography (PQC) transition journey. PQShield CEO Al El Kaafarani noted that 20% of the dominant players in each industry are expected to begin the PQC migration process this year.

The National Institute of Standards and Technology (NIST) is expected to release its long-awaited PQC standards in the next few weeks. “This switches the whole scenery from readiness and preparing for post-quantum cryptography to compliance,” Kaafarani told SDxCentral.

Kaafarani emphasized the importance of the NIST PQC standard release, noting that many organizations are ready to move to the next phase but are held back by the lack of formal standards. “Some of the partners that we’ve worked with are super ready now to move to the next phase, where they can actually start selling products with post-quantum cryptography in it. But they can’t do this because that’s not compliant with any standards,” Kaafarani said.

Tech giants taking the lead

Significant strides have been made by leading tech companies in PQC implementations.

Apple earlier this year introduced iMessage with PQ3, which is its first post-quantum cryptographic messaging protocol to reach what the vendor calls “level-3 security.” Google followed suit with its Chrome 124 update that enabled a new quantum-resistant X25519Kyber768 encapsulation mechanism by default for TLS 1.3 and QUIC protocol connections on all desktop platforms to protect Chrome TLS traffic against quantum cryptographic analysis.

Zoom Video Communications announced the global availability of post-quantum end-to-end encryption for Zoom Workplace; Meta initiated a multi-year plan to migrate toward PQC spanning from its internal infrastructure to user-facing apps; and AMD partnered with PQShield to deliver a demonstration of quantum-resistant algorithms deployed on AMD’s high-performance Versal products.

These moves signal the seriousness with which large corporations are approaching the transition to post-quantum cryptography, Kaafarani said.

“But also it shows that sectors are ready, and the guidelines are not things that will stop them if they are drafted and transformed into final guidance, because guidance will always change, but they change at a very high level, they don’t change the details of how things should be implemented and where and why,” Kaafarani added.

The supply chain needs to sync on PQC

A large number of companies involved in different layers of the cybersecurity supply chain have begun the PQC transition process, or at least the discussion. Other organizations "need to have a complete picture of what are the things that they need to do themselves, which is usually less than 20%, and what are the things that their suppliers have to do and understand from their supplier their timelines," Kaafarani said.

Banks, for example, rely on hardware security modules (HSMs) and network security from suppliers, and need to know if and when these will be post-quantum secured. Network security vendors need to talk to their semiconductop-of-rack (TOR) suppliers who work with PQC companies for the fundamental post-quantum capabilities.

Everyone in the supply chain needs to be in sync, Kaafarani stressed.

"If someone is using post quantum and others in the sector are not using post quantum, it's going to create some compatibility problems. And therefore you can't isolate yourself from the rest of the crowd by not being able to speak the post-quantum cryptography language," Kaafarani said. "There's this risk also of falling behind and not being able to continue to work with other providers and other protocols around the world."

All major web browsers are expected to migrate to PQC in 2024

Kaafarani expects all the major web browsers to support and enable PQC in the second half of this year, noting "if 90% of web browsers are using post-quantum cryptography … then the cloud side or the server side can also switch and use it."

Kaafarani also predicts that 20% of the dominant players in each sector will start the PQC migration process this year. "You will see that the 20% of the companies that cover 80% of use cases and protocols and solutions and control the market will be the first to move. And then you will see that the rest of the cards will start following suit," he said.

24.U.S. quantum cryptography standards set for release next week

by David DiMolfetta and Alexandra Kelley
https://www.nextgov.com/emerging-tech/2024/08/us-quantum-cryptography-standards-set-release-next-week/398713/

Scientific guidance meant to ensure the U.S. is ready to shore up cyber defenses against a potential quantum computers' ability to break through modern encryption methods are set for release the week of Aug. 12, according to people familiar with the matter.

The development of the finalized post-quantum cryptography (PQC) standards are led by the National Institute of Standards and Technology, the Commerce Department's scientific standards bureau. NIST has finalized the guidance and is readying its release in the coming days, said the people, who spoke on condition of anonymity because they were not authorized to publicly discuss the release timeline.

Today's cryptographic systems rely on complex mathematical algorithms that are difficult for traditional

computers to unravel. Future quantum computers could potentially solve these problems much faster, processing information based on the laws of quantum mechanics where a vast number of possibilities can be solved simultaneously. In cybersecurity terms, it means malicious hackers in the coming years may be augmented with new abilities to unravel encrypted information previously deemed secure.

Federal officials are trying to prevent future quantum computing-powered cyber incidents like "record now, decrypt later" attacks, where an adversary will hoover up encrypted datasets, store them, and — with the eventual existence of a quantum device — decrypt that data to use for theft or exploitation.

Ahead of the algorithms' release, NIST spent months seeking feedback on draft standards for post-quantum algorithms approved by the agency as it looks to help organizations migrate their networks toward a state of quantum-resilient code.

NIST made an initial selection of four algorithms deemed suitable for post-quantum cryptographic migration in July 2022. The algorithms — CRYSTALS-Kyber, CRYSTALS-Dilithium, SPHINCS+, and FALCON — are specialized for different applications based on draft Federal Information Processing Standards, or FIPS, which are government-stamped blueprints deemed for optimal computer interoperability and security.

CRYSTALS-Kyber, for example, is designed for general secure website encryption, while the others focus on securing digital signature software.

Experts have previously told *Nextgov/FCW* that implementing quantum readiness cryptography into digital systems is just "the starting gun" for a larger mass migration to secure digital networks in an uncertain quantum future.

"You can think of the NIST standardization as basically the starting gun," Scott Crowder, vice president for IBM Quantum Adoption and Business Development said in a previous interview. "But there's a lot of work to be done on taking those standards, making sure that all the open source implementations, all the proprietary implementations get done, and then rippling through and doing all the hard work in terms of doing the transformation upgrade."

Practical quantum computing tools are about 3 to 5 years out from workforce use and will likely be accessed through cloud based environments, a top National Security Agency official predicted in April.

25.512-bit RSA key in home energy system gives control of "virtual power plant"

by Dan Goodin
https://arstechnica.com/security/2024/08/home-energy-system-gives-researcher-control-of-virtual-power-plant/

When Ryan Castellucci recently acquired solar panels and a battery storage system for their home just outside of London, they were drawn to the ability to use an open source dashboard to monitor and control the flow of electricity being generated. Instead, they gained much, much more—some 200 megawatts of programmable capacity to charge or discharge to the grid at will. That's enough energy to power roughly 40,000 homes.

Castellucci, whose pronouns are they/them, acquired this remarkable control after gaining access to the

administrative account for GivEnergy, the UK-based energy management provider who supplied the systems. In addition to the control over an estimated 60,000 installed systems, the admin account—which amounts to root control of the company's cloud-connected products—also made it possible for them to enumerate names, email addresses, usernames, phone numbers, and addresses of all other GivEnergy customers (something the researcher didn't actually do).

“My plan is to set up Home Assistant and integrate it with that, but in the meantime, I decided to let it talk to the cloud,” Castellucci wrote Thursday, referring to the recently installed gear. “I set up some scheduled charging, then started experimenting with the API. The next evening, I had control over a virtual power plant comprised of tens of thousands of grid connected batteries.”

Still broken after all these years

The cause of the authentication bypass Castellucci discovered was a programming interface that was protected by an RSA cryptographic key of just 512 bits. The key signs authentication tokens and is the rough equivalent of a master-key. The bit sizes allowed Castellucci to factor the private key underpinning the entire API. The factoring required $70 in cloud computing costs and less than 24 hours. GivEnergy introduced a fix within 24 hours of Castellucci privately disclosing the weakness.

The first publicly known instance of 512-bit RSA being factored came in 1999 by an international team of more than a dozen researchers. The feat took a supercomputer and hundreds of other computers seven months to carry out. By 2009 hobbyists spent about three weeks to factor 13 512-bit keys protecting firmware in Texas Instruments calculators from being copied. In 2015, researchers demonstrated factoring as a service, a method that used Amazon cloud computing, cost $75, and took about four hours. As processing power has increased, the resources required to factor keys has become ever less.

It’s tempting to fault GivEnergy engineers for pinning the security of its infrastructure on a key that’s trivial to break. Castellucci, however, said the responsibility is better assigned to the makers of code libraries developers rely on to implement complex cryptographic processes.

“Expecting developers to know that 512 bit RSA is insecure clearly doesn’t work,” the security researcher wrote. “They’re not cryptographers. This is not their job. The failure wasn’t that someone used 512 bit RSA. It was that a library they were relying on *let them*.”

Castellucci noted that OpenSSL, the most widely used cryptographic code library, still offers the option of using 512-bit keys. So does the Go crypto library. Coincidentally, the Python cryptography library removed the option only a few weeks ago (the commit for the change was made in January).

In an email, a GivEnergy representative reinforced Castellucci’s assessment, writing:

> “*In this case, the problematic encryption approach was picked up via a 3rd party library many years ago, when we were a tiny startup company with only 2, fairly junior software developers & limited experience. Their assumption at the time was that because this encryption was available within the library, it was safe to use. This approach was passed through the intervening years and this part of the codebase was not changed significantly since implementation (so hadn't passed through the review of the more experienced team we now have in place*).”

A key factor

RSA encryption relies on extremely large numbers that are the product of two prime numbers. The large number, known as a modulus, is typically denoted as 'n' while the primes are denoted as 'p' and 'q.' While it’s easy to multiply the two prime numbers, it's nearly impossible for someone with only the modulus of a key of sufficient length to identify its two underlying prime numbers, a process known as factorizing. The difficulty of solving this problem allows for the creation of two keys. One is a public key any-

one can have and the other is a private key that must be kept absolutely secret. Factorizing a key pair completely breaks their security because it reveals the private portion.

The difficulty of solving this problem is directly proportional to the number of possible primes that must be tested. The more possibilities the harder it is to find the right pair. This entropy, in turn, is proportional to the bit length of the modulus. In 2019, a team of researchers factored a 795-bit RSA key, making it the biggest key size to be broken at the time. A year later, researchers factorized an 829-bit RSA key. To date, there are no confirmed cases of 1024-bit RSA being factorized, but that doesn't mean it can't be done.

“The only barrier for [factorizing 1024-bit RSA] in public is some engineering effort and funding, and finding a large organization willing to put up enough computing power,” Nadia Heninger, a University of California at San Diego professor specializing in cryptography, wrote in an email. “It could have been done years ago if people wanted to—there's no technical barrier, and multiple large companies certainly have the computing resources.”

Anticipating the inevitable fall of 1024-bit RSA, the US National Institute of Standards and Technology stopped allowing its use in 2013 and will stop allowing the use of 2048-bit RSA in 2031. Microsoft earlier this year announced the deprecation of 1024-bit RSA in Windows.

Castillucci’s task was made more difficult because they didn’t have access to the public key securing the admin account. Instead they had only a JWT—short for a JSON Web Token—that was signed by the key. Castellucci explained how they overcame the limitation:

> *RSA needs three values to work, the modulus n, the private exponent d, and the public exponent e. An RSA signature is computed as $s \equiv m^d \mod n$. It’s validated by checking that $s^e \mod n = m$. With the prime factors of n, it’s trivial to calculate d, and for a 512 bit key finding the prime factors is doable, but I didn’t have n or e. By convention, e is nearly always 65537, but I had no idea what n was. I do, however, know algebra.*
>
> *Subtracting n from both sides of the signature verification equation gives $s^e \mod n - m = 0$. Since modular subtraction is associative, that also means that $(s^e - m) \mod n = 0$. The modulo operation finds the remainder, so $s^e - m$ is an integer multiple of n. This is not useful on its own, but it means that with another message and signature, I’d have two different integer multiples of n. Running those through a GCD algorithm would give me $n \times x$ where x is a small integer, easily factored out by trial division.*

This Isn’t Textbook RSA

> *The math above only covers “Textbook RSA” operating on raw numbers, which has a number of problems in practice. It can only operate on numbers smaller than the key’s modulus. The numbers also can’t be too small, otherwise various attacks are possible. To address this, the message is hashed and padded using PKCS #1 v1.5 encoding before being signed. Not wanting to deal with the encoding, I went looking for a pre-existing tool. After a few false starts, I found JWT-Key-Recovery, which quickly provided the modulus.*

Cracking the Key

> *The modulus is generated by picking large prime numbers, usually denoted p and q, and multiplying them together. If you want more detail, please see my previous post, Artisanal RSA. The most efficient known algorithm for factoring the modulus back into primes is called general number field*

> *sieve (GNFS). This wasn't my first time cracking an RSA key, but it'd been a while, so I found some instructions. I started cado-nfs on my workstation and let it run overnight. By the time I got done with work the next day, I was feeling impatient and rented a few hundred CPU cores to make it go faster. A few hours and a $70 compute bill later, I had the two prime numbers I needed.*

Once in possession of the two primes, the researcher used a custom tool to generate the private key and then signed the JWT provided with a demo account they were using. With a few additional steps, Castellucci had transformed the token to give the same access admins inside GivEnergy had.

Based on the sequential numbering of each account, Castellucci estimated that the account had control of about 60,000 installed systems. Assuming each system can charge or discharge 3 to 4 kW per inverter, that equates to roughly 200 MW of electricity.

Castellucci praised GivEnergy for taking their report seriously and fixing it less than a day after receiving it. The researcher confirmed that factorizing the API key was no longer possible. GivEnergy disclosed its previous use of the weak key here. An analysis of system logs indicated the weakness had never been exploited maliciously, the company said.
In an interview, Castellucci returned to the problem of outdated code libraries that still haven't removed support for weak keys and noted the potentially catastrophic harm that can result years later.

"The GivEnergy issue I found was someone stepping on an old land mine," they said. "These ones just take a couple years before they actually blow your leg off."

26.Quantum Cryptography Has Everyone Scrambling

by Margo Anderson
https://spectrum.ieee.org/quantum-key-distribution

While the technology world awaits NIST's latest "post-quantum" cryptography standards this summer, a parallel effort is underway to also develop cryptosystems that are grounded in quantum technology—what are called quantum-key distribution or QKD systems.

As a result, India, China, and a range of technology organizations in the European Union and United States are researching and developing QKD and weighing standards for the nascent cryptography alternative. And the biggest question of all is how or if QKD fits into a robust, reliable, and fully future-proof cryptography system that will ultimately become the global standard for secure digital communications into the 2030s. As in any emerging technology standard, different players are staking claims on different technologies and implementations of those technologies. And many of the big players are pursuing such divergent options because no technology is a clear winner at the moment.

According to Ciel Qi, a research analyst at the New York-based Rhodium Group, there's one clear leader in QKD research and development—at least for now. "While China likely holds an advantage in QKD-based cryptography due to its early investment and development, others are catching up," says Qi.

Two different kinds of "quantum secure" tech

At the center of these varied cryptography efforts is the distinction between QKD and post-quantum cryptography (PQC) systems. QKD is based on quantum physics, which holds that entangled qubits can

store their shared information so securely that any effort to uncover it is unavoidably detectable. Sending pairs of entangled-photon qubits to both ends of a network provides the basis for physically secure cryptographic keys that can lock down data packets sent across that network.

Typically, quantum cryptography systems are built around photon sources that chirp out entangled photon pairs—where photon A heading down one length of fiber has a polarization that's perpendicular to the polarization of photon B heading in the other direction. The recipients of these two photons perform separate measurements that enable both recipients to know that they and only they have the shared information transmitted by these photon pairs. (Otherwise, if a third party had intervened and measured one or both photons first, the delicate photon states would have been irreparably altered before reaching the recipients.)

This shared bit the two people on opposite ends of the line have in common then becomes a 0 or 1 in a budding secret key that the two recipients build up by sharing more and more entangled photons. Build up enough shared secret 0s and 1s between sender and receiver, and that secret key can be used for a type of strong cryptography, called a one-time pad, that guarantees a message's safe transmission and faithful receipt by only the intended recipient.

By contrast, post-quantum cryptography (PQC) is based not around quantum physics but pure math, in which next-generation cryptographic algorithms are designed to run on conventional computers. And it's the algorithms' vast complexity that makes PQC security systems practically uncrackable, even by a quantum computer. So NIST—the U.S. National Institute of Standards and Technology—is developing gold-standard PQC systems that will undergird tomorrow's post-quantum networks and communications.

The big problem with the latter approach, says Doug Finke, chief content officer of the New York-based Global Quantum Intelligence, is PQC is only *believed* (on very, very good but not infallible evidence) to be uncrackable by a fully-grown quantum computer. PQC, in other words, cannot necessarily offer the ironclad "quantum security" that's promised.

"People can't predict theoretically that these PQC algorithms won't be broken one day," Finke says. "On the other hand, QKD—there are theoretical arguments based on quantum physics that you can't break a QKD network."

That said, real-world QKD implementations might still be hackable via side-channel, device-based, and other clever attacks. Plus, QKD also requires direct access to a quantum-grade fiber optics network and sensitive quantum communications tech, neither of which is exactly commonplace today. "For day-to-day stuff, for me to send my credit card information to Amazon on my cellphone," Finke says, "I'm not going to use QKD."

China's early QKD lead dwindling

According to Qi, China may have originally picked QKD as a focal point of their quantum technology development in part because the U.S. was *not* directing its efforts that way. "[The] strategic focus on QKD may be driven by China's desire to secure a unique technological advantage, particularly as the U.S. leads in PQC efforts globally," she says.

In particular, she points to ramped up efforts to use satellite uplinks and downlinks as the basis for free-space Chinese QKD systems. Citing as a source China's "father of quantum," Pan Jianwei, Qi says, "To achieve global quantum network coverage, China is currently developing a medium-high orbit quantum satellite, which is expected to be launched around 2026."

That said, the limiting factor in all QKD systems to date is their ultimate reliance on a single photon to

represent each qubit. Not even the most exquisitely-refined lasers and fiber optic lines can't escape the vulnerability of individual photons.

QKD repeaters, which would blindly replicate a single photon's quantum state but not leak any distinguishing information about the individual photons passing through—meaning the repeater would not be hackable by eavesdroppers—do not exist today. But, Finke says, such tech is achievable, though at least 5 to 10 years away. "It definitely is early days," he says.

"In China they do have a 2,000-kilometer network," Finke says. "But it uses this thing called trusted nodes. I think they have over 30 in the Beijing to Shanghai network. So maybe every 100 km, they have this unit which basically measures the signal... and then regenerates it. But the trusted node you have to locate on an army base or someplace like that. If someone breaks in there, they can hack into the communications."

Meanwhile, India has been playing catch-up, according to Satyam Priyadarshy, a senior advisor to Global Quantum Intelligence. Priyadarshy says India's National Quantum Mission includes plans for QKD communications research—aiming ultimately for QKD networks connecting cities over 2,000-km distances, as well as across similarly long-ranging satellite communications networks.

Priyadarshy points both to government QKD research efforts—including at the Indian Space Research Organization—and private enterprise-based R&D, including by the Bengaluru-based cybersecurity firm QuNu Labs. Priyadarshy says that QuNu, for example, has been working on a hub-and-spoke framework named ChaQra for QKD. (*Spectrum* also sent requests for comment to officials at India's Department of Telecommunications, which were unanswered as of press time.)

In the U.S. and European Union, similar early-stage efforts are also afoot. Contacted by *IEEE Spectrum*, officials from the European Telecommunications Standards Institute (ETSI); the International Standards Organization (ISO); the International Electrotechnical Commission (IEC); and the IEEE Communications Society confirmed initiatives and working groups that are now working to both promote QKD technologies and emergent standards now taking shape.

"While ETSI is fortunate to have experts in a broad range of relevant topics, there is a lot to do," says Martin Ward, senior research scientist based at Toshiba's Cambridge Research Laboratory in England, and chair of a QKD industry standards group at ETSI.

Multiple sources contacted for this article envisioned a probable future in which PQC will likely be the default standard for most secure communications in a world of pervasive quantum computing. Yet, PQC also cannot avoid its potential Achilles' heel against increasingly powerful quantum algorithms and machines either. This is where, the sources suggest, QKD could offer the prospect of hybrid secure communications that PQC alone could never provide.

"QKD provides [theoretical] information security, while PQC enables scalab[ility]," Priyadarshy says. "A hybrid of QKD and PQC is the most likely solution for a quantum safe network." But he added that efforts at investigating hybrid QKD-PQC technologies and standards today are "very limited."

Then, says Finke, QKD could still have the final say, even in a world where PQC remains preeminent. Developing QKD technology just happens, he points out, to also provide the basis for a future quantum Internet.

"It's very important to understand that QKD is actually just one use case for a full quantum network," Finke says.

"There's a lot of applications, like distributed quantum computing and quantum data centers and quantum sensor networks," Finke adds. "So even the research that people are doing now in QKD is still very,

very helpful because a lot of that same technology can be leveraged for some of these other use cases."

27.Preparing for the Future of Post-Quantum Cryptography

by David O'Berry
https://www.darkreading.com/vulnerabilities-threats/future-of-post-quantum-cryptography

Quantum computing has been projected to enable market-defining and life-changing capabilities since its inception more than three decades ago. From financial portfolio optimization and improved electric vehicle (EV) battery production to enhanced drug discovery and advanced semiconductor manufacturing, quantum computers can perform complex calculations at faster speeds than both traditional and super computers.

Thanks to the recent artificial intelligence (AI) boom, quantum computing is predicted to become even more significant in the coming years. Quantum computers will facilitate advancements in AI algorithms — better known as quantum AI or QAI. These quantum-enabled AI models will be faster as well as more accurate and efficient, due to quantum computers' parallel processing abilities that can simultaneously solve complex problems and prepare large datasets. This also means that quantum computing can deliver more energy-efficient AI algorithms, as well as hybrid architecture, neural network-enabled data modeling, and improved AI and data security.

Despite the positivity surrounding quantum computing, there is also a dark side to this burgeoning technology. Cybersecurity criminals are increasingly using quantum computing techniques to attack enterprises and break encryptions. It is believed that in the next five to 10 years, quantum computers will be able to break the majority of today's cryptographic algorithms.

This reality leaves corporate leaders and cybersecurity experts with one choice — prepare for the future of post-quantum cryptography (PQC) before it's too late.

Current State of Post-Quantum Cryptography

Encryption has been a highly divisive cybersecurity tool in the United States for several decades. In fact, if it was not for the work of experts like Phil Zimmerman catalyzing public-private discussion during the Crypto Wars, we could be living in a more vulnerable world, where encryption was still widely outlawed.

Fortunately, after years of debate and a growing onslaught of concerning cyberattacks, cryptography is now a broadly accepted security technique, backed by the US government. Encryption is used to protect everything from emails to cryptocurrencies to private wireless networks. However, of all the cryptographic applications, post-quantum cryptography in particular is now the gold standard.

In 2022, Congress passed the Quantum Computing Cybersecurity Preparedness Act to ensure all federal entities will have quantum-resilient plans and technology in the coming years. The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and National Institute of Standards and Technology (NIST) also collectively developed the "Quantum Readiness: Migration to Post-Quantum Cryptography" information sheet last year, to advise US defense agencies and private enterprises alike on the new reality of cybersecurity in our post-quantum world.

This surge in PQC legislation is largely due to the fact that most of our existing encryption is weak and cannot withstand a quantum-enabled attack. And while there is some work being done to advance quantum-proof algorithms, it is not nearly enough. Organizations across industries will be subjected to quantum-led attacks, including government agencies, financial and insurance enterprises, government suppliers — such as aerospace and defense companies — and corporations managing critical infrastructure like telcos and utilities. In other words, PQC is a matter of national security and personal privacy.

Bolstering Unbreakable Security

Cyber leaders have always been tasked with preparing for the unpredictable, but now perhaps for the first time, they must prepare for the unknown. Cyber teams have limited knowledge of both quantum-enabled attacks and quantum-resistant encryption. So how can leaders across sectors bolster their defenses in the unfolding era of PQC?

To start, preparations should begin with risk assessments and inventories to help organizations understand where they have cryptographic gaps. Cyber teams should ask themselves where and how they are using encryption. Moreover, they should identify the various kinds of encryption algorithms and their current use cases across the enterprise. This will, in turn, help companies achieve crypto agility across systems.

Leaders must also enable a cultural and technological reset. Most cybersecurity professionals will need to be trained to identify, mitigate, respond to, and even predict and prevent quantum-driven threats. These upskilling and reskilling initiatives will typically require third-party support from cyber vendors with deep expertise in quantum technologies.

In order to ultimately protect data and secure AI models using post-quantum cryptographic protocols, algorithms, and systems, organizations will also have to revamp their key management strategy, public key infrastructure deployments, and certificate life cycle management practices.

The AI boom and increasing popularity of quantum computing necessitates quantum-resilient security. The US government has seen the writing on the wall — and now, enterprises must meet the unknown head-on as well.

28.Harvest Now, Decrypt Later (HNDL): A Look at This Current & Future Threat

by Casey Crane
https://www.thesslstore.com/blog/harvest-now-decrypt-later-hndl/

HNDL retrospective decryption attacks are a major concern for more than half of the professionals surveyed by Deloitte. We'll explore what these quantum-related future threats are and how you can future-proof your enterprise against them

Bad guys, right now, might be loading up your most sensitive data like it's clearance day at their favorite warehouse store.

Your data is encrypted? They don't care. Threat actors are putting your data "on ice," storing it until

quantum computing capabilities come along that can break modern encryption schemes. (And Q-Day might be here sooner than you think!)

This activity is known as a "harvest now, decrypt later" attack. We'll explore what HNDL attacks are and how you can harden your cyber defenses and data against these threats now and in the future.

Let's hash it out.

What Is a Harvest Now, Decrypt Later (HDNL) Attack?

Harvest now, decrypt later is a surreptitious two-part cyber attack in which threat actors collect sensitive information now for use at a later date. It's about collecting a wealth of encrypted data now that can be capitalized upon "tomorrow" (i.e., whenever these silicone-based systems become available outside a laboratory setting). For this reason, this method is also called "store now, decrypt later" and "catch now, break later" attacks.

Bad guys are biding their time until quantum computers are readily available, simply collecting and storing the information in the meantime. After all, why should they invest all of the time, effort, and resources required to break cryptographic algorithms that future quantum computers will be able to break within a matter of minutes, hours, or days?

Why Quantum Computing Is the Key to HNDL Attacks

Quantum computers harness the power of the quantum mechanics superposition principle (i.e., the ability for elements to exist in multiple states simultaneously). This computational power is central to concerns about harvest now, decrypt later attacks. This is why quantum-safe (or, more accurately, quantum-*resistant*) cryptosystems must withstand the processing power of quantum computers. As such, data must be cryptographically secured using quantum-resistant algorithms (i.e., post-quantum cryptography).

Cryptographically relevant quantum computers are expected to break the factorization problem that's at the heart of modern public key encryption schemes. Basically, any data secured by modern public key encryption schemes alone would be at risk of compromise once the quantum tools are available. It doesn't matter whether you're a small business or one of the world's biggest enterprises; we'll all require the same post-quantum encryption and key exchange algorithms that are specifically designed to combat quantum computer-based attacks.

Shor's Algorithm is poised to break the public key cryptography schemes we rely on today that are based on the discrete logarithm (ECDH) and prime factorization (RSA) integers. Wondering how it all works? Rather than me trying to explain it, you can hear it straight from the horse's mouth and get the low-down from mathematician Peter Shor himself.

Hybrid Algorithms Help You Bridge the Gap in the Meantime

The crypto-agile approach of using hybrid algorithms aims to nip in the bud the security issues posed by Shor's Algorithm. This is why the Internet Engineering Task Force (IETF) recommends using hybrid public key encryption (HPKE) algorithms to fend off modern attacks and protect data against future cryptographic attacks (like HNDL).

An example of an HPKE algorithm is **X25519Kyber768Draft00**. This hybrid algorithm — the combination of the traditional elliptic curve cryptography [ECC] key exchange algorithm X25519 and the Kyber-768 Module Lattice Key Encapsulation Mechanism [ML-KEM] — is used by Google Chrome and Cloudflare as of 2023). Zoom announced in May 2024 that it deployed Kyber-768 to enable

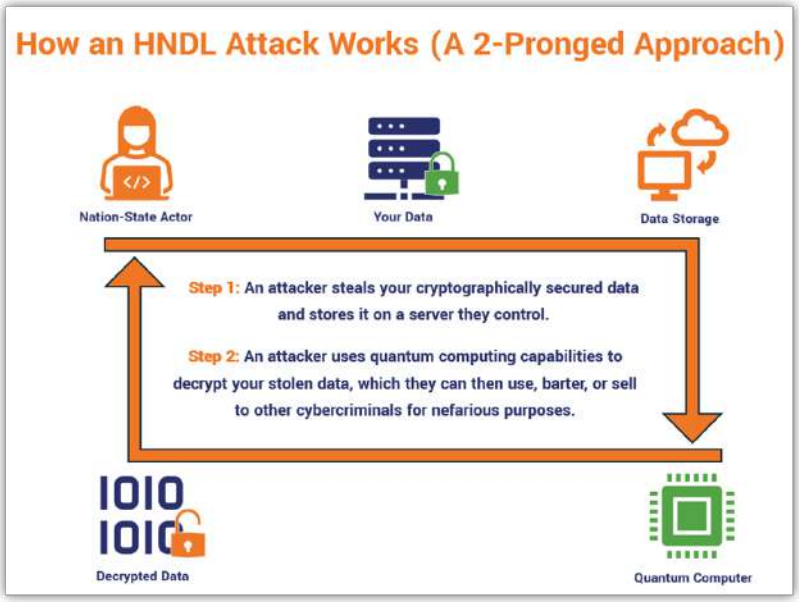
end-to-end encryption (E2EE) for its Zoom Meetings with plans to employ it for Zoom Phone and Rooms products next.

Lattice-based algorithms are mathematically difficult problems to solve as doing so requires figuring out the shortest and closest vectors. (Lattices are typically multi-dimensional charts. The more dimensions that are taken into account when calculating the lattice points [bases], the more challenging the lattice is to solve.) Putting it simply, these algebraic problems are nightmares for mathematically challenged individuals but great for PQC digital security.

Here's a quick primer on how lattice-based cryptography works.

How a Harvest Now, Decrypt Later Attack Works

Unlike many other modern cyber attacks that give attackers instant gratification, harvet now, derypt later attacks require patient attackers who are willing to wait for more reliable quantum capabilities. HNDL attackers can set up eavesdropping tools to collect a plethora of encrypted data that they can then sit on for the next 3-10 years.



Of course, there's no rush or time limit to decrypt certain types of information. For example, an HNDL attack is ideally suited for evergreen data such as social security numbers, bank account information, government secrets, and other sensitive data that aren't prone to change much (if at all) and/or have perpetual value.

For example, secret plans for a nuclear weapon or your company's most secret intellectual property aren't likely to lose their value within the next few years.

This differs from, say, credit cards, which change more frequently due to the owners' name changes, card expiration dates, and reported fraud issues. This isn't evergreen data and cybercriminals know it can lose its intrinsic value if it's not used quickly.

Attackers Are Getting Smarter About What They Choose to Save

Let's face it: there's a ridiculous amount of data in the world, and the overwhelming amount of data

businesses generate and store is growing at an inordinate rate. And attackers want to get their hands on your most valuable secret data.

Effective HNDL attacks aren't about harvesting every scrap of data attackers can get their hands on. It behooves attackers to make more educated guesses about which data payloads to steal to achieve the highest value, as data storage costs can certainly add up over time, particularly when someone is storing massive quantities for years.)

So, how do HNDL threat actors figure out which encrypted data to store or dump? On the surface, you can't. All encrypted data just looks like a bunch of gibberish without the necessary decryption key. But there are contextual clues that cybercriminals can analyze to figure out which data might hold the most value:

- Transmission source and destination IP addresses (i.e., to whom or where it is being sent or received from)
- Transaction frequencies
- Application connection behaviors and patterns
- Data transmission sizes

Who's Thought to Be Responsible for HNDL Attacks?

Technically, anyone can be an harvest now, decrypt later attacker. If you have a way to get your hands on organizations' encrypted sensitive data payloads, then you have the potential to carry out "store now, decrypt later" attacks in the future with the help of quantum computing technologies.

However, when people within the industry discuss these types of attacks, they typically refer to the threats posed by nation-state threat actors and other large groups of bad actors. Basically, the biggest threats are the groups of individuals or government-sponsored entities that have more resources and data storage at their disposal rather than necessarily the individual attackers (though they still pose threats as well).

Knowing all of this, what steps can you take to help protect your data now against these retrospective decryption attacks in the future?

How to Protect Your Organization Against HNDL Attacks

1. **Start Planning Your PQC Strategy Now (If You Haven't Already Done So)**

   Back in November 2023, we shared our top takeaways from the second annual PKI Consortium's Post-Quantum Cryptography Conference. One of the key insights shared by many of the experts is that it's a mistake for organizations to wait to start figuring out a game plan.

   Adopting PQC isn't simply a matter of swapping out classical PKI digital certificates for shiny new PQC certs; there's a lot more to it that's required. It also boils down to implementing a wealth of new policies, processes, procedures, and technologies.

   For example, here are a few of the ways you can start preparing your organization for an inevitable Quantum future:

   - Inventory your cryptographic assets so you know what you need to secure.
   - Closely manage your PKI lifecycle to address any vulnerabilities that pop up quickly.
   - Integrate quantum-based threats and considerations into your ongoing risk analyses.

NIST and Other Global Experts Are Finalizing a Standardized Approach

The National Institute of Standards and Technology (NIST) has been working hard with other industry experts over the past several years to finalize new PQC standards. The NIST PQC Team has been holding a series of seminars and their goal is to publish finalized standards this year that organizations can implement in the near future.

For example, they've published four draft algorithms (one key encapsulation algorithm and three digital signature algorithms) that are nearing final standardization:

1. CRYSTALS-KYBER (a module lattice-based key encapsulation algorithm that's used for key establishment and encryption)

2. CRYSTALS-DILITHIUM (a module lattice-based general-purpose digital signing algorithm)

3. SPHINCS+ (another digital signature algorithm featuring stateless hash-based security properties)

4. FALCON+ (a third digital signature algorithm, but one that's NTRU lattice-based and will be applicable for more specific use cases)

The first three PQC algorithms are expected to be released sometime this summer (2024). However, the fourth (FALCON+) likely won't be released until later in the year.

2. Enable the Kyber Hybrid Key Exchange Algorithm in Chrome

If you haven't done so already, enable the X25519Kyber768Draft00 algorithm in your organization's Google Chrome web clients. Also, ensure your employees are keeping their endpoint devices' browsers up to date so they have the latest protections and updates.

Of course, once NIST finalizes the PQC standards for its chosen algorithms, be sure to adopt support for the latest version and remove support for X25519Kyber768Draft00 at that time.

3. Upgrade Your Private PKI Certificates to PQC

For enterprises that want to secure their internal IT server infrastructure, software apps, users, and endpoint devices, you don't have to wait to use hybrid cryptographic algorithms. DigiCert Trust Lifecycle Manager offers several certificate templates that support PQC Module Lattice Digital Signature Algorithm (ML-DSA) keys.

Implementing a hybrid approach means that bad guys will have to break not one, but two cryptosystems in order to gain access to your plaintext data.

4. Swap Out Your Long-Term Keys for Ones Generated Using PQC Algorithms

Some digital certificate uses and applications within your organization may entail using certificates with longer device and cryptographic key lifespans than others. For example, IoT devices have lifespans ranging upwards of 20 years!

There are plenty of legitimate reasons why companies may not actively change out their IoT device keys, with reasons ranging from physical logistics to some devices not being capable of over-the-air (OTA) updates. But regardless of the reason why, it means that if those devices rely on classical cryptosystems, they're at risk of store now, decrypt later attacks.

As you can imagine, swapping out the keys for these devices whenever possible is critical, particularly if you're expecting them to remain active on your network or within your IT ecosystem for years to come.

5. **Look Out for Publicly Trusted SSL/TLS Certificates in the Future**

   Unfortunately, PQC SSL/TLS certificates from publicly trusted certificate authorities (CAs) aren't available yet. (Creating an entirely new set of cryptographic algorithms isn't exactly a walk in the park — these things take time, after all!) But once they are available, you'll want to implement these algorithms across your networks and IT infrastructure as soon as possible.

Final Thoughts on Harvest Now, Decrypt Later Attacks

Harvest now, decrypt later attacks are real-world threats that will affect your organization and customers now and more acutely in the future. As you've learned, you can take steps to fight back against these dual-pronged attacks.

CRQCs are coming; few dispute that. But even knowing this, there's no reason to panic. Use the time now to prepare for the worst so that your organization is as prepared as possible. This approach puts you in the best position possible to deal with any curveballs that may come your way.

By implementing hybrid PQC algorithms now within your ecosystem, you're taking steps to prevent bad guys from decrypting and using your sensitive data against you (and your customers) later.

29.Quantum Computing Is Developing Faster Than Expected — QuEra Survey

by Matt Swayne
https://thequantuminsider.com/2024/08/06/quantum-computing-is-developing-faster-than-expected-quera-survey/

New research from QuEra Computing, the leader in neutral-atom quantum computing, reveals that over half of quantum academics, scientists and professionals (51%) believe the technology is making faster progress than they expected, with 40% saying it will become a superior alternative to classical computing for certain workloads within the next five years. The findings also highlight the truly disruptive potential of the technology, with a majority expecting quantum computing to solve problems that were previously unsolvable.

QuEra's research was published today in its 'Current and future state of quantum computing' report and was conducted on over 900 quantum computing academics, scientists and professionals across the globe. The positive outlook highlights the significant progress being made in solving the main barriers to quantum computing development and adoption, which QuEra's research identified as scalability (33%), error correction and fault tolerance (31%), and hardware performance (20%).

However, participants do have concerns. A third (33%) believe it is likely their organization will be caught off guard by the rapid progress being made, while also being wary of a bottleneck similar to the one being experienced with AI. Due to the rapid growth of AI applications, there are widespread reports of difficulties in securing time on GPUs for their projects, and the majority (65%) of respondents are concerned

a similar situation might occur with quantum computers once their value is proven and demand and competition for resources intensifies.

Yuval Boger, Chief Commercial Officer, QuEra, said: “Recent major breakthroughs have significantly accelerated quantum computing development and reduced the timescales for adoption. The first computer capable of achieving quantum advantage is slated to hit the market in 2026 and companies realize they will soon be in a race for first-mover advantage. We’ve seen a huge shift in companies moving from experimenting and educating their workforce, to preparing to capitalize the very minute quantum advantage computers hit the market.”

The race for quantum advantage across the globe

According to the survey, the US is in the pole position to lead the global quantum computing industry, with 82% of US participants believing it is very well positioned to play an important role. While only 42% of European participants share the same sentiment on their own countries, confidence is much higher in France (67%) and the UK (57%), while Germany is close to the average at 45%.

The question of where quantum computers are developed and manufactured has become increasingly important, as nations have recently enacted controls to limit the capabilities of quantum computers they export. Participants in the US and France, both at 34% of respondents, believe it important that the technology be developed in their own country, whereas 24% say the same in Germany and only 14% in the UK.

It is far more important to European Participants that the computers are made by a friendly trading partners, as 60% of UK participants agreed with this, as did those in Germany (54%) and France (49%), compared to 40% in the US.

Boger added: “We have seen nations taking different approaches to developing and adopting quantum computers. Some are keen to integrate both local and global companies to contribute to its quantum ecosystem, while others are far more nationalistic and closed off. It’s clear that survey participants see the US playing a leading role and the UK is one of the most confident European countries, suggesting their strategies may be paying off.”

Methodology

For the research, QuEra surveyed 920 members of the quantum computing community, including academics, scientists and professionals worldwide in June 2024. There were 350 respondents based in Europe and 338 in the US[LA2] [MOU3] . Respondents were sourced from QuEra’s database of contacts via an email invitation and an online survey.

30.NISQ Versus FTQC in the 2025 – 2029 Timeframe

by GQI
https://quantumcomputingreport.com/nisq-versus-ftqc-in-the-2025-2029-timeframe/

At GQI, we see a lot of roadmaps from the quantum providers and fully expect that there will be continuing advances in the capabilities of both quantum hardware and quantum software over the next several years. In fact, we believe that we will soon start seeing organizations utilizing quantum technology for

production purposes within the next few years. (Some call that Quantum Advantage while others call it Quantum Utility, but in this article we will call it Quantum Production to distinguish it from one-off proof-of-concept experiments versus those running the use cases on a repeated, regular basis.)

Although we initially did not expect to see fault tolerant quantum computers until the 2030's recent advances now lead us to believe that we will start seeing what we call early fault tolerant quantum computers (FTQC) available in the second half of this decade. One way we measure the capability of a quantum computer is a measure we call Quops, standing for successful quantum operations. And we classify quantum evolution according to the following eras: Intermediate, Early FTQC, Large Scale FTQC, and mature Turbo FTQC. For error corrected machines, we expect to see Early FTQC machines available within the next five years that can achieve capabilities in the MegaQuops or GigaQuops regimes. These machines will offer a few 100 or so logical qubits and that should be enough to run some useful applications, but still won't be powerful enough to run intensive quantum applications like Shor's algorithm that will require machines with TeraQuops capabilities. We do not expect those Large Scale FTQC machines to be available until the 2030's and they will provide thousands of logical qubits for calculations.

Physical Fidelities	Physical Error Rate (PER)	Surface Code [[n,k,d]]	Distance (d)	Encoding Rate (inc. ancillas)	Logical Error Rate (LER)	Regime	QQI Era
99.5%	5.0E-03	[[144,1,12]]	12	287	1.1E-03	KiloQuop	Intermediate
99.9%	1.0E-03	none	1	1	1.0E-03		
99.99%	1.0E-04	none	1	1	1.0E-04	thousands of quantum operations	
99.999%	1.0E-05	none	1	1	1.0E-05		
99.5%	5.0E-03	[[1024,1,32]]	32	2047	1.1E-06	MegaQuop	Early FTQC
99.9%	1.0E-03	[[81,1,9]]	9	161	1.0E-06		
99.99%	1.0E-04	[[16,1,4]]	4	31	1.0E-06	millions of quantum operations	
99.999%	1.0E-05	[[9,1,3]]	3	17	1.0E-07		
99.5%	5.0E-03	[[2704,1,52]]	52	5407	1.1E-09	GigaQuop	
99.9%	1.0E-03	[[225,1,15]]	15	449	1.0E-09		
99.99%	1.0E-04	[[49,1,7]]	7	97	1.0E-09	billions of quantum operations	
99.999%	1.0E-05	[[25,1,5]]	5	49	1.0E-10		
99.5%	5.0E-03	[[5184,1,72]]	72	10367	1.0E-12	TeraQuop	Large Scale FTQC
99.9%	1.0E-03	[[441,1,21]]	21	881	1.0E-12		
99.99%	1.0E-04	[[100,1,10]]	10	199	1.0E-12	trillions of quantum operations	
99.999%	1.0E-05	[[49,1,7]]	7	97	1.0E-13		
99.5%	5.0E-03	[[8464,1,92]]	92	16927	1.0E-15	PetaQuop	Mature
99.9%	1.0E-03	[[729,1,27]]	27	1457	1.0E-15		
99.99%	1.0E-04	[[169,1,13]]	13	337	1.0E-15	quadrillions of quantum operations	
99.999%	1.0E-05	[[81,1,9]]	9	161	1.0E-16		

On the other hand, we also see advances occurring in more capable NISQ processors along with associated algorithms that may be able to also run useful applications in the 2025-2029 timeframe. We have already seen a few companies demonstrate two-qubit fidelities in greater than 99.9% for their physical gates. And we have also seen advances in algorithms to get the most out of those physical gates. This software includes hybrid classical/quantum architectures, variational quantum algorithms, error mitigation and suppression techniques, circuit knitting, zero noise extrapolation, probabilistic error cancellation, and other classical post processing to improve quantum results. Moreover, the roadmaps we have seen indicate we may have available NISQ processors with 10,000 of physical qubits in the second half of this decade.

So end users may have an interesting choice soon. Do they want to use an Early FTQC machine that

provides about 100 logical qubits with 2Q fidelities of greater than 99.9999% or do that want to use a NISQ machine that contains around 10,000 physical qubits with with 2Q fidelities of 99.9% or perhaps 99.99%?

Many quantum researchers are skeptical that the people will ever be able to run useful applications on a NISQ quantum computer. Besides the fact that these machines still have some remaining noise issues, one of the other reasons is that many of these applications would rely on heuristic algorithms such as QAOA or VQE which no one can theoretically prove will work. People will just need to try them out and see if they work or not. On the other hand, there does exist theoretical proof that certain algorithms, such as Shor's algorithm, can run on a fault tolerant quantum computer and provide an accurate answer. However, we would remind our readers that many of the classical AI algorithms that have become popular in recent days are also heuristic and computer scientists do not yet have a theoretical proof that they should work. Yet, of course, these AI algorithm do work.

We are not at the point yet where we can definitely say which quantum applications will be able to provide commercially useful results on which machines. However, the one thing that makes us optimistic is the diversity of innovative approaches and rapid advances that organizations are making in both hardware as well as software get to where the systems can be used for Quantum Production for useful applications. Although some of these innovative approaches will fail, we fully believe that others will work and start delivering within the next few years on the promise of quantum computer. The applications in production may only be a handful for the next few years, but this initial small number will grow substantially in the 2030's as more Teraquop large scale FTQC system become available enabling many more algorithms to be run successfully.

So while some may be of the belief that there will be a hard demarcation between when the NISQ era will end and the FTQC era begins. In reality, these eras will overlap and we will see a gradual transition between when one ends and the other begins.

31.How to prepare for a secure post-quantum future

by Andy Smith
https://www.techtarget.com/searchsecurity/post/How-to-prepare-for-a-secure-post-quantum-future

The oncoming rise of quantum computing poses serious implications for the cyberthreat landscape. Large-scale quantum supercomputers could compromise the public key cryptographic algorithms that are the foundation of many of our software security controls today -- rendering them ineffective.

The time for organizations to act is now. By taking proactive steps to embrace a post-quantum cryptography (PQC) migration, understanding cryptographic dependency and prioritizing quantum expertise, you can position your company to facilitate smooth transitions into the post-quantum security world.

How quantum computing works

It's important to understand the science behind quantum technology. Classical computers rely on bits, which can represent either a one or a zero, analogous to an on/off switch. Meanwhile, the quantum bits (qubits) used in quantum computers exploit the principles of quantum mechanics to exist in a superposition state.

A qubit can be a one, zero or both simultaneously until measured. Qubits can also be entangled together at a quantum level, whereby the superposition of one depends on the other. This combination of superposition and entanglement enables quantum computers to explore a vast number of possibilities concurrently. Imagine solving a maze: A classical computer explores each path one by one, while a quantum computer could explore all paths simultaneously. This enables people to significantly accelerate solving for specific problems.

Quantum computers won't replace classical computing, however, as it can't make every computation faster. Still, where a suitable quantum algorithm can be written to solve a problem by exploiting qubits and entanglement, the increased speed can be revolutionary. Two such mathematical problems are factoring large primes and computing discrete logarithms, the difficulty of which forms the basis for our current generation of public key cryptography.

The creation of a cryptographically relevant quantum computer with sufficient power to run Shor's algorithm means both problems can be solved exponentially faster than on a classical computer and thus circumvent cryptographic controls.

With large-scale quantum computers potentially online by as early as 2030, the National Security Agency, Cybersecurity and Infrastructure Security Agency and NIST released a joint advisory in August 2023 that called for organizations to begin developing quantum-readiness roadmaps, conducting inventories, applying risk analysis assessments and engaging vendors to future-proof systems against quantum threats.

It underscored why early planning is necessary, highlighting how the lifecycles of most systems in operation today extend into quantum environments and how adversaries could target data with long secrecy lifetimes to carry out harvest now, decrypt later attacks.

How quantum computing impacts cryptography

During a panel discussion at the 2024 World Economic Forum, IBM leaders warned that quantum could create "a cybersecurity Armageddon" environment in the years to come. But is that doomsday narrative our actual reality? If we collectively choose to ignore the threat, then maybe.

But, if we take our heads out of the sand and perform some sensible steps, then probably not. After all, it will be a long time until the average advanced persistent threat group or ransomware operator has access to a quantum machine capable of doing anything of cryptographic relevance. Nation-state adversaries will be the first to leverage cryptographically relevant quantum computers over the next decade, and they're likely to keep that a secret for as long as possible to extend the operational life of such a powerful capability.

That doesn't diminish the importance of preparing your cyberdefenses for the post-quantum era -- especially if nation-states are a realistic part of your threat model. It's important to begin facilitating widespread shifts from classical algorithms to PQC designed to withstand quantum-powered attacks. NIST's first set of standardized PQC algorithms, initially announced in 2022, are slated to be finalized this year, and more are expected to follow. Adopting these algorithms across your security environment will be critical.

While migrating to full PQC is the ultimate end goal, getting there will encompass a long and complicated journey spanning a decade or more and involving several different stakeholders. It's a marathon, not a sprint. Facilitating PQC migration requires effective collaboration among government bodies, global software system developers and cybersecurity leaders to align industry standards and build unified lines of defense.

Those efforts are already underway, and organizations should also be initiating their own programs for the transition to quantum-resistant algorithms now. The sooner you start the journey, the easier it will be.

How to start your post-quantum journey

Preparing for the post-quantum era depends upon a firm commitment to conducting a comprehensive cryptographic inventory by scanning your organization's entire IT infrastructure and cloud services to identify all systems and applications that rely on cryptography. The assessment should include servers, databases, communication channels, email systems, VPNs and security tools.

Each identified system's specific cryptographic algorithms should be documented, ideally including details like key lengths, cipher schemes and implementation library. This provides a baseline for planning your PQC migration and comes in handy the next time a non-quantum cryptographic vulnerability emerges, such as the next Heartbleed.

Once you've conducted a detailed inventory, it's crucial to prioritize migration efforts because you can't do everything at once. Risk assessment becomes paramount. The potential impact of a successful quantum attack on each cryptographic application needs to be analyzed. This enables updates to be prioritized based on the sensitivity of the data they protect, the longevity of that sensitivity and the potential consequences of a breach.

Next comes the migration work itself. For cloud services or third-party software, you need to influence your vendors to adopt NIST-recommended post-quantum algorithms. For in-house applications, the remediation falls to your own development teams. This is a good opportunity not just to implement a stronger algorithm, but also consider if any aspects of the systems can be rearchitected or reengineered to deliver crypto-agility -- the ability to make any further future cryptographic changes a simpler process.

Migrating to PQC is a difficult task, so it makes sense to consider how you can reduce the number of systems needing migration in the first place. Update your procurement requirements to mandate that suppliers commit to adopting quantum-resistant cryptography within an appropriate time frame. This builds a strong commercial incentive for vendors to play a crucial role in the post-quantum journey. For vendors, post-quantum security should be seen as a product differentiator.

The role of quantum security expertise

As with any emerging technology, education and expertise play a key role in effectively navigating the security implications of the post-quantum era. Vendors are already claiming they have best-in-class products that offer a magic bullet for combating quantum-based threats. A solid understanding of post-quantum cryptography helps to determine which vendor's claims present value to an organization and which are expensive distractions. This is one of the reasons I transformed my own PQC learning journey last year into a short series on YouTube.

Skilled practitioners are a cornerstone of any effective security strategy. To navigate the post-quantum landscape, organizations need to identify or upskill individuals with expertise in quantum security principles who can facilitate collaboration with standards bodies, analyze potential quantum threats and help develop comprehensive quantum security roadmaps. Staying informed about advancements in post-quantum security standards is also crucial, as is the ability to communicate those advancements and roadmaps with nonsecurity and senior stakeholders.

Finally, adopting a zero-trust security mindset can contribute to post-quantum resilience. Layering defenses from the inside out under the assumption that a security breach will occur doesn't stop an adversary from bypassing cryptographic protections with a quantum computer, but it does help prevent one breach from leading to a catastrophic incident.

32.Eight Essential Considerations for Post-Quantum Cryptography Migration

by Krupa Patil
https://www.appviewx.com/blogs/8-essential-considerations-for-post-quantum-cryptography-migration/

The United Nations has proclaimed 2025 the International Year of Quantum Science and Technology—and for good reason. Across the globe, the quantum community is making monumental strides toward building stable, commercially viable quantum computers. As the vision of quantum technology entering mainstream applications solidifies, a palpable tension hangs in the air. Knowing that a large-scale quantum computer could effortlessly break today's cryptographic algorithms like RSA, DSA, ECDH, ECDSA, and EdDSA and expose sensitive, confidential data is a looming nightmare for many CISOs. Gartner® predicts that by 2029, quantum computing will be in a position to weaken existing systems to the point that they are considered unsafe to use cryptographically.

The only hope for a secure quantum future lies in Post-Quantum Cryptography (PQC). PQC algorithms are being developed specifically to withstand quantum attacks, ensuring that data remains secure even with a powerful quantum computer. These algorithms are designed using mathematical problems that are believed to be resistant to quantum computing capabilities. The National Institute of Standards and Technology (NIST) has been at the forefront of this effort, leading a global initiative with the international cryptography community to standardize PQC algorithms.

As we already know, after three rounds of evaluation, NIST announced the first four algorithms in July 2022: CRYSTALS-Kyber for key establishment and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures. Additionally, NIST identified four more candidates (subsequently reduced to three now) for further analysis and evaluation in the fourth round.

According to NIST's timeline, the standardization of all post-quantum algorithms is expected to reach the finish line this year (anytime now). This milestone is pivotal, as it will set the stage for organizations worldwide to begin the arduous yet essential process of migrating to post-quantum cryptography, as the PQC algorithms will be integrated into various standards and products worldwide.

PQC Migration Is Not a Mere Technical Upgrade; It Is a Fundamental Shift to a Whole New Generation of Cryptography.

Migration to PQC is a much more complex undertaking when compared to other cryptographic migrations from the past. The new PQC algorithms have significantly different properties from the current algorithms in terms of key sizes, signature sizes, key exchange, computational requirements, entropy, and others. Naturally, the challenges in migration are multifaceted, involving changes to infrastructure, algorithms, applications, and compliance frameworks. Organizations must plan extensively, ensuring that their systems are robust enough to handle the demands of PQC while maintaining seamless operations.

Given the threat of "harvest now, decrypt later" attacks and the estimated migration time for a small-mid size organization of 8-9 years, the need for immediate preparation is clear. Cybersecurity experts and analysts strongly recommend that security and risk management leaders start preparing for a move to PQC today.

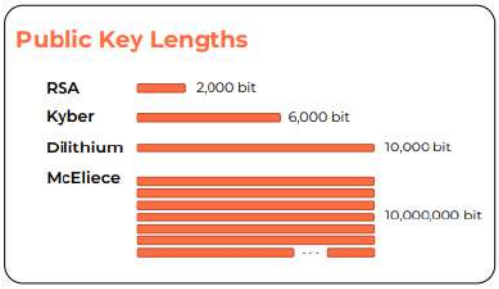
As you start your post-quantum cryptography migration journey, here are eight critical factors you must

consider to ensure a seamless and secure transition:

1. **Bandwidth**

   PQC algorithms typically produce larger key sizes and longer signatures and ciphertexts than conventional algorithms, such as RSA and Diffie-Hellman.

   As stated in Eviden's PQC Migration Guide – The Essentials – "The public keys of CRYSTALS-Kyber (6,000 bit) and CRYSTALS-Dilithium (10,000 bit) are several times larger than the ones of RSA and Diffie-Hellman (2,000 bit). Other proposed post-quantum algorithms even require hundreds of thousands of public-key bits more. The situation is not much different when it comes to private keys."



   As a consequence, data traffic and latency increase. To avoid the impact on network performance, you must ensure your network can handle the additional load. This might require upgrading your network infrastructure, optimizing data flow, and possibly increasing bandwidth capacity.

2. **Storage**

   Again, as PQC algorithms come with larger key sizes, PQC certificates will require more storage space. You may need additional storage for maintaining hybrid and traditional cryptographic systems during the transition. Evaluate your existing storage solutions and plan for expansions to accommodate the increased data volume. Ensure that your data backup and recovery systems can manage the larger volumes efficiently.

3. **Protocols**

   Existing communication protocols, such as TLS, SSH, S/MIME, and IPsec, must be updated to support PQC algorithms. This includes configuring the existing protocols to use PQC algorithms for key exchange and signature mechanisms. Do a comprehensive review of the existing protocols, conduct rigorous testing, and plan for any changes to the underlying infrastructure to ensure secure communication.

4. **Application/Software Upgrades**

   The transition to post-quantum cryptography requires significant updates to software and applications as they need to support PQC algorithms and new cryptographic standards. Existing software may require extensive modifications to ensure compatibility with PQC libraries and protocols. This process can be complex and time-consuming. Start by building a comprehensive inventory of existing cryptography and associated applications and software. Identify mission-critical assets that need to be migrated on priority. Thoroughly test and validate PQC algorithms in these entities to prevent service disruptions and ensure security.

5. **Hardware Upgrades**

   Post-quantum cryptography can impose greater demands on processing power, necessitating hardware upgrades. You may have to invest in new servers and processors that can handle the increased computational load and specialized hardware accelerators to optimize performance. Additionally, you may have to update or replace hardware security modules (HSMs) that currently support classical cryptographic algorithms with models supporting post-quantum algorithms. First, build a thorough inventory of your current hardware and classify components involved in critical data protection for immediate upgrades or replacement.

6. **Third-Party Applications and Services**

   If your organization relies on third-party vendor technology, applications, and services, such as email and VPNs, you must ensure that they support post-quantum cryptography. Engage with your vendors to understand their PQC integration roadmap and timelines. Work with them to get new products/applications delivered with PQC built-in and legacy ones upgraded with PQC. This collaboration is essential to address the performance impact and interoperability issues that may arise during or after PQC migration.

7. **Standards and Guidelines**

   Compliance with emerging PQC-related RFCs, standards, and guidelines will be a crucial step in the transition process. You will need to integrate and maintain up-to-date PQC libraries and random number generators (RNG). So, stay abreast of emerging standards from bodies such as the National Institute of Standards and Technology (NIST) and the European Telecommunications Standards Institute (ETSI). Adhering to these standards ensures interoperability and security across different systems and platforms.

8. **Regulatory Compliance**

   Regulatory bodies will likely update compliance requirements to include post-quantum cryptographic standards. You will need to ensure that your cryptographic practices align with new regulations and standards related to PQC. This involves updating compliance policies, conducting regular audits, and maintaining documentation to demonstrate adherence to post-quantum security standards. Stay informed about evolving regulations and make necessary amends in your security practices to avoid compliance issues.

PQC Migration Solutions from AppViewX

To facilitate a seamless and efficient transition to PQC, AppViewX offers the following solutions:

- **AppViewX PQC Test Center:** A dedicated free online resource built to help organizations assess their PQC readiness by generating and testing quantum-safe certificates prior to their integration into existing systems, workloads and machines. You can quickly set up your own quantum-safe PKI hierarchy and generate PQC ready certificates and keys to test their compatibility in your environment.

- **PQC Certificate Lifecycle Management:** The AVX ONE platform offers a comprehensive certificate lifecycle management solution to help enable PQC readiness and crypto agility with complete certificate discovery and inventory, full certificate lifecycle automation, and total certificate control across the enterprise.

The transition to post-quantum cryptography (PQC) is inevitable. As the countdown to the final round of

NIST's PQC standardization starts, it is time to start getting quantum ready. As NIST's Matthew Scholl said: *"It's no time to panic. It's time to plan wisely."* Investing time and resources now in strategic planning and leveraging solutions like those offered by AppViewX can help greatly resolve the challenges along the migration journey and be secure in the quantum era.

33.BTQ and Id Quantique Sign MoU to Develop Authentication Systems

by Matt Swayne
https://thequantuminsider.com/2024/08/01/btq-and-id-quantique-sign-mou-to-develop-authentication-systems/

BTQ Technologies Corp., a global quantum technology company focused on securing mission-critical networks, is pleased to announce that on Friday, July 19, 2024, BTQ and ID Quantique (IDQ) signed a Memorandum of Understanding (MOU) for joint research, development, and mutual cooperation to create an innovative authentication system combining Quantum Random Number Generators (QRNG) and Post-Quantum Cryptography (PQC).

IDQ is a leading company in the field of quantum cryptography and was the first in the world to commercialize quantum random number generators. Currently, it supplies industry-leading QRNGs to various sectors, including the Samsung Galaxy Quantum phone. Besides quantum random number generators, IDQ also showcases outstanding technology in QKD (Quantum Key Distribution) and SNSPD (Superconducting Nanowire Single Photon Detectors).

BTQ, a Canadian-listed company, developed the PQC quantum signature algorithm Preon, which was selected in the most recent round of the PQC standardization process by the U.S. National Institute of Standards and Technology (NIST) on July 27, 2023. Preon, based on zk-SNARK, is a robust and efficient post-quantum signature scheme characterized by a small key size, fast key generation, minimal assumptions, and flexible functionality. These features provide strong resistance to potential threats from both classical and quantum computers.

Through this agreement, the two companies expect to pioneer a new authentication system market based on QRNG and PQC quantum technologies.

Regarding this agreement, IDQ Korea General Manager, Sangyun Uhm stated that IDQ has set the standard for next-generation security in the post-quantum era through its QRNG technology. He emphasized that through collaboration with BTQ, IDQ aims to develop even stronger authentication systems and bring innovation to the cybersecurity landscape.

Olivier Roussy Newton, CEO of BTQ, added: "Partnering with ID Quantique represents a significant milestone for BTQ. By combining our expertise in post-quantum cryptography with IDQ's leadership in quantum random number generation, we are poised to create state-of-the-art authentication systems that address the security challenges of both today and tomorrow. This collaboration underscores our commitment to pioneering advancements in cybersecurity and ensuring the robustness of mission-critical networks in the quantum era."

34.Let's start treating cyber security like it matters

by Bruce Schneier and Tarah Wheeler
https://www.defenseone.com/ideas/2024/08/lets-start-treating-cyber-security-it-matters/398534/

When an airplane crashes, impartial investigatory bodies leap into action, empowered by law to unearth what happened and why. But there is no such body to investigate CrowdStrike's faulty update that recently ensnarled banks, airlines, and emergency services to the tune of billions of dollars. We need one.

To be sure, there is the White House's Cyber Safety Review Board. On March 20, the CSRB released a report into last summer's intrusion by a Chinese hacking group into Microsoft's cloud environment, where it compromised the U.S. Department of Commerce, State Department, congressional offices, and several associated companies. But the board's report—well-researched and containing some good and actionable recommendations—shows how it suffers from its lack of subpoena power and its political unwillingness to generalize from specific incidents to the broader industry.

Some background: The CSRB was established in 2021, by executive order, to provide an independent analysis and assessment of significant cyberattacks against the United States. The goal was to pierce the corporate confidentiality that often surrounds such attacks and to provide the entire security community with lessons and recommendations. The more we all know about what happened, the better we can all do next time. It's the same thinking that led to the formation of the National Transportation Safety Board, but for cyberattacks and not plane crashes.

But the board immediately failed to live up to its mission. It was founded in response to the Russian cyberattack on the U.S. known as SolarWinds. Although it was specifically tasked with investigating that incident, it did not—for reasons that remain unclear.

So far, the board has published three reports. They offered only simplistic recommendations. In the first investigation on Log4J, the CSRB exhorted companies to patch their systems faster and more often. In the second, on Lapsus$, the CSRB told organizations not to use SMS-based two-factor authentication (it's vulnerable to SIM-swapping attacks). These two recommendations are basic cybersecurity hygiene, and not something we need an investigation to tell us.

The most recent report—on China's penetration of Microsoft—is much better. This time, the CSRB gave us an extensive analysis of Microsoft's security failures and placed blame for the attack's success squarely on their shoulders. Its recommendations were also more specific and extensive, addressing Microsoft's board and leaders specifically and the industry more generally. The report describes how Microsoft stopped rotating cryptographic keys in early 2021, reducing the security of the systems affected in the hack. The report suggests that if the company had set up an automated or manual key rotation system, or a way to alert teams about the age of their keys, it could have prevented the attack on its systems. The report also looked at how Microsoft's competitors—think Google, Oracle, and Amazon Web Services—handle this issue, offering insights on how similar companies avoid mistakes.

Yet there are still problems, with the report itself and with the environment in which it was produced.

First, the public report cites a large number of anonymous sources. While the report lays blame for the breach on Microsoft's lax security culture, it is actually quite deferential to Microsoft; it makes special mention of the company's cooperation. If the board needed to make trades to get information that would

only be provided if people were given anonymity, this should be laid out more explicitly for the sake of transparency. More importantly, the board seems to have conflict-of-interest issues arising from the fact that the investigators are corporate executives and heads of government agencies who have full-time jobs.

Second: Unlike the NTSB, the CSRB lacks subpoena power. This is, at least in part, out of fear that the conflicted tech executives and government employees would use the power in an anticompetitive fashion. As a result, the board must rely on wheedling and cooperation for its fact-finding. While the DHS press release said, "Microsoft fully cooperated with the Board's review," the next company may not be nearly as cooperative, and we do not know what was not shared with the CSRB.

One of us, Tarah, recently testified on this topic before the U.S. Senate's Homeland Security and Governmental Affairs Committee, and the senators asking questions seemed genuinely interested in how to fix the CSRB's extreme slowness and lack of transparency in the two reports they'd issued so far.

It's a hard task. The CSRB's charter comes from Executive Order 14208, which is why—unlike the NTSB—it doesn't have subpoena power. Congress needs to codify the CSRB in law and give it the subpoena power it so desperately needs.

Additionally, the CSRB's reports don't provide useful guidance going forward. For example, the Microsoft report provides no mapping of the company's security problems to any government standards that could have prevented them. In this case, the problem is that there are no standards overseen by NIST—the organization in charge of cybersecurity standards—for key rotation. It would have been better for the report to have said that explicitly. The cybersecurity industry needs NIST standards to give us a compliance floor below which any organization is explicitly failing to provide due care. The report condemns Microsoft for not rotating an internal encryption key for seven years, when its standard internally was four years. However, for the last several years, automated key rotation more on the order of once a month or even more frequently has become the expected industry guideline.

A guideline, however, is not a standard or regulation. It's just a strongly worded suggestion. In this specific case, the report doesn't offer guidance on how often keys should be rotated. In essence, the CSRB report said that Microsoft should feel very bad about the fact that they did not rotate their keys more often—but did not explain the logic, give an actual baseline of how often keys should be rotated, or provide any statistical or survey data to support why that timeline is appropriate. Automated certificate rotation such as that provided by public free service Let's Encrypt has revolutionized encrypted-by-default communications, and expectations in the cybersecurity industry have risen to match. Unfortunately, the report only discusses Microsoft proprietary keys by brand name, instead of having a larger discussion of why public key infrastructure exists or what the best practices should be.

More generally, because the CSRB reports so far have failed to generalize their findings with transparent and thorough research that provides real standards and expectations for the cybersecurity industry, we—policymakers, industry leaders, the U.S. public—find ourselves filling in the gaps. Individual experts are having to provide anecdotal and individualized interpretations of what their investigations might imply for companies simply trying to learn what their actual due care responsibilities are.

It's as if no one is sure whether boiling your drinking water or nailing a horseshoe up over the door is statistically more likely to decrease the incidence of cholera. Sure, a lot of us think that boiling your water is probably best, but no one is saying that with real science. No one is saying how long you have to boil your water for, or if any water sources are more likely to carry illness. And until there are real numbers and general standards, our educated opinions are on an equal footing with horseshoes and hope.

It should not be the job of cybersecurity experts, even us, to generate lessons from CSRB reports based on our own opinions. This is why we continue to ask the CSRB to provide generalizable standards which either are based on or call for NIST standardization. We want proscriptive and descriptive reports of inci-

dents: see, for example, the UK GAO report for the WannaCry ransomware, which remains a gold standard of government cybersecurity incident investigation reports.

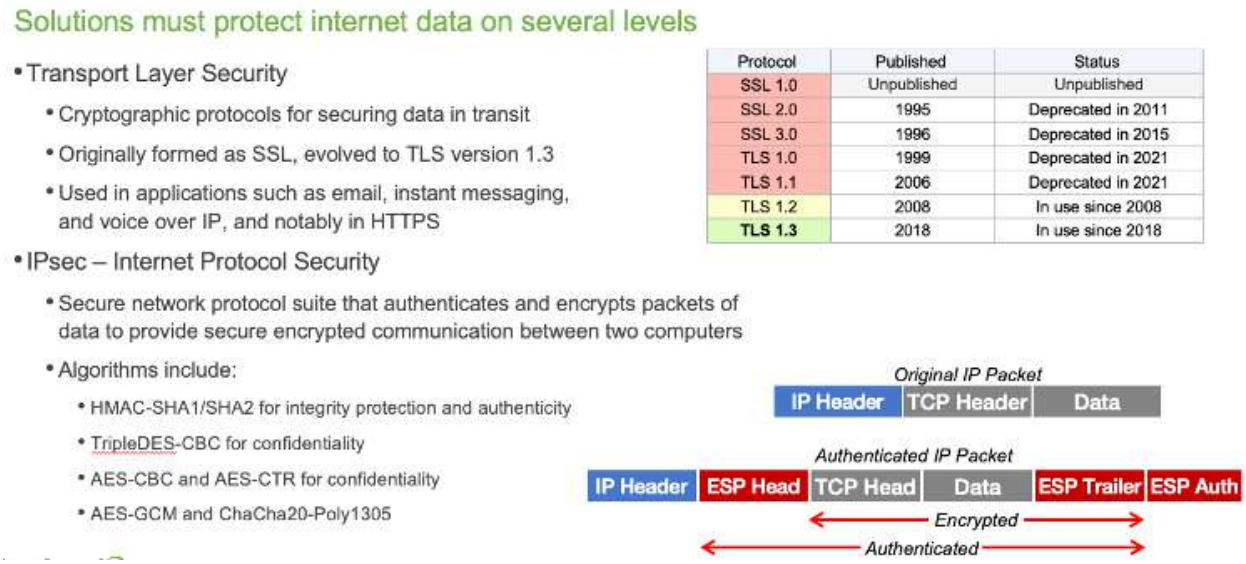
We need and deserve more than one-off anecdotes about how one company didn't do security well and should do it better in future. Let's start treating cybersecurity like the equivalent of public safety and get some real lessons learned.

35.Post-Quantum Computing Threatens Fundamental Transport Protocols

by Karen Heyman
https://semiengineering.com/post-quantum-computing-threatens-fundamental-transport-protocols/

The Transport Level Security (TLS) protocol is one of the few rock-steady spots in the rapidly changing computing industry, but that's about to change as quantum computers threaten traditional encryption schemes.

Because TLS is fundamental to network communications, including allowing Internet of Things (IoT) devices to function properly, researchers already are exploring both hardware and software defenses. Security vendors are preparing to have counter-measures in place before quantum computing becomes more available at some point in the next decade. For chip designers, this means understanding the risks and how best to implement solutions well in advance of actual threats.



If a systems architect or device physicist from 1994 stepped into a time machine and set it for 2024, they would be flummoxed by the new terms and concepts in hardware. But if a network security engineer made the same time trip, most of the basic ideas would be familiar. The security protocols that undergirded the early internet in the 1990s have evolved enough to secure the IoT ecosystem. In 1999, the first official transport layer security (TLS) protocol was published. The previous protocol was the secure sockets layer (SSL), which Netscape introduced in 1994. Starting with SSL 1.0., there have been only six major updates in 30 years. The latest, TLS 1.3 (IETF RFC 8446), was published in 2018.

"These protocols evolve slowly, especially if they're good strong protocols," said Mike Borza, principal security technologist at Synopsys. "Most of the protocol evolution in SSL, and then TLS, has been to fix security problems as they've been found. TLS 1.3 is a huge new version of TLS that changed a lot of the details. It's more efficient for the session negotiation, which is the 'Hello' protocol or session-setup protocol. The actual bulk data part of the protocol is very consistent with other older versions of TLS in terms of the record processing. What has changed is many of the ciphers and modes that were available, against which people found exploits or common misconfigurations that led to blights. These have been eliminated in TLS 1.3."

The fundamental structure of SSL/TLS protocols is a secure end-to-end connection between dedicated endpoints, with security parameters established during the "handshake" when both sides connect. The encrypted packets then appear as gibberish to the rest of the network. "It's a shocking amount of computation that's actually happening," said Scott Best, director of anti-tamper security technology at Rambus.

The security architecture has allowed the protocols to extend beyond their roots from the 1990s, when they were employed only to establish secure sessions on the client side for web browsers. "These days, TLS is being used in a lot of other protocols," said Borza. "For example, Open VPN is built on top of the TLS protocol. It's being used a lot for machine-to-machine communications, which was never what it was envisaged for, but that's now well within the realms of applications for TLS. There's a related protocol called DTLS, which is essentially a packetized version of TLS. TLS operates over continuous streams of data. By contrast, DTLS is designed to operate using packets of data, which is a fundamental distinction."

TLS lives on top of TCP, the transmission control protocol, which operates over a packet layer. At the most fundamental level, networks deliver packets, which are agnostic to each other. On top of that packet protocol, there's TLS, which is designed to be a continuous, reliable stream of data that is independent of, and agnostic to, whatever the underlying network technology is and how it has packetized data. At this level, it's not about including cryptographic schemes. It's about ensuring the packets are assembled correctly.

Applications that are especially latency-sensitive generally employ DTLS (datagram transport layer security), a similar protocol that rides on the UDP (user datagram protocol) layer. "If you're trying to transmit video, TCP/IP can get in the way because it's always looking for a response," said Best. "You don't send your video until it gets all the responses. But all the acknowledgments of the data take up the bandwidth that you could have used to send more video. To avoid that, you use UDP instead of TCP."

DTLS is also generally the chosen protocol for IoT because of how it handles latency. "TCP takes a fair bit of resources to get that illusion of a continuous stream of data," said Borza. "To get an open channel that's reliable — so that when you push bits in at one end and they pop out the other end and they're always in order — takes a fair bit of software and a fair bit of memory to buffer data, to reorder data, etc. As a result, TCP for a lot of IoT devices is more than they can bear to handle. That's why DTLS was created. It operates over an unreliable network that is just capable of delivering, on a best effort basis, a datagram from one place to another."

A relatively recent addition to the functionality is REST (representational state transfer), which works as an API with TLS to create stateless web-based applications.

"When you make a request to a server, the server is supposed to respond to that request. If the client is completely satisfied with the response, they tear down the connection and it starts up later," said Best. "With RESTful APIs, the IoT client can establish a connection to a server and just leave it alone, leave it quiet. It connects, it registers, and says, 'I'm listening, and if you ever need to talk to me, you should respond to the channel.' But otherwise, there's no data actually occurring on the channel, so it's a light-

weight thing for the client and the server to maintain these RESTful connections. The nice thing about it is the IoT device always connects to the server. The server never has to connect to the device. Directionality matters on the internet, so in this type of connectivity the initiator is always the IoT device."

Current TLS vulnerabilities

Authentication is key to TLS security. "The hardest part of TLS is, 'Who am I talking to?'" said Best. Answering that question securely is at the heart of the protocol—and future post-quantum security challenges.

"If I use a URL with an HTTPS, I'm saying I want a secure communication," said Jim Montgomery, principal solution architect of TXOne. "But in order to first establish the communication channel using TLS, there's a certificate exchange, and then the encryption of the data based on that certificate, so that only the originating and the specific points will have the ability to decrypt that traffic based upon the certificate. By encrypting the communication between the nodes, you eliminate vulnerabilities like man-in-the-middle attacks or the ability to view the data in plain text."

The validity of certificates is based on public key encryption. Unfortunately, real certificates can be spoofed, and counterfeit certificates can be issued by attackers who seek either to capture data or completely disrupt a system. Fortunately, successful incidents are now rare, and the IETF has an elaborate system to ensure authenticity.

"There's no reason now for a browser to consume a malicious certificate and get confused about it," said Best. "Once a theft actually happens, there are low-latency ways that that information can be percolated, within minutes, rather than within days. That's a distinct improvement over how people were doing it 20 years ago."

Far less reassuring is the potential ability of quantum computers to break traditional encryption algorithms.

"Quantum cryptographically relevant computers would be able to look at an authentic certificate, which contains a public key and a signature, and from that information — or some combination of other information, like the issuer's public key — they could figure out what the secret signing key is," said Best. "Using that information, a malicious operator that has access to a cryptographically relevant computer would be able to create bogus certificates that look completely authentic."

Cures for contemporary security

In addition to employing quantum-safe algorithms, security can be increased by both software and hardware solutions.

Segmentation and access permissions are primary ways to control access, so that only authenticated devices can communicate with their authorized partners. Currently, most of that work is performed by VLANs. "The positive is that most of the switching equipment at the enterprise level is going to support VLANs," said Montgomery. "The downside is the administrative overhead for VLANs."

The process can be simplified through the creation of automated whitelists, noted Montgomery. "We're introducing specific hardware into the environment that can automate that function, by listening to the traffic, and then creating whitelists based upon the traffic that you approve."

Any of these approaches should be based on zero trust. "Who should be talking to who is foundational to ensuring security, because you're limiting that ability for other devices to either spread lateral movement or to attack the system just because they've been allowed to communicate with devices," he ex-

plained.

Jayson Bethurem, vice president of marketing and business development at Flex Logix, is an advocate of "crypto-agility," which in practice means employing devices like FPGAs that can constantly reprogram themselves to keep up with evolving threats. "Post-quantum computing will render all of the older encryption algorithms useless, whether they're integer factorization, discrete logarithmic, or elliptical curve. All of these types of foundational cryptographic algorithms will become insecure. Crypto-agility is going to be needed to fight this problem."

Bethurem explained that one solution for cryptography is to intercept packets before they even get into the memory subsystem, so security analysis can be done at the transport layer. "As the packets are being dissected, there's an audit where your own algorithms are looking for malicious types of activities. You can use an embedded FPGA to continuously adapt these algorithms because the threats constantly evolve, but you can stop malicious traffic like distributed denial-of-service types of attacks."

Conclusion

To properly address the security issues with transport layer security, experts say the best strategy is to be pragmatic. For example, it's not important for a security engineer to know that the transport layer is Layer 4 of the OSI protocol stack.

"Anybody who knows what TLS is, already knows where it is in the stack," said Best. "And anybody who doesn't know what TLS is won't learn anything from knowing that it's Layer 4. Our customers want to know important, precise details, like the key size that's protecting the TLS, as well as other details. When we're doing the key exchange, what algorithm is being used to establish that session key? What exactly was the algorithm used to sign the certificates? Is it quantum safe, or is it something really weak? Is it a very old version of RSA or the newer version? Engineers get into it pretty quickly about speed, authenticity, and privacy, but nobody says the letters OSI during that conversation."

Synopsys's Borza offered practical advice to avoid unfortunate choices, especially around IoT. "For starters, stick with standards and don't try to invent something that you think seems good enough," said Borza. "A lot of people have made that mistake and left themselves and their products vulnerable to all kinds of things. There are a lot of good, small implementations around these protocols that work. For example, for IoT, where space and cost are always issues, there are well-done small implementations of either TLS or DTLS that are suitable for those devices. Just stick to using those implementations and don't try to do it yourself."

36.Post-Quantum Algebraic Cryptography Trimester in Fall 2024

by Ludovic Perret
https://sites.google.com/view/pqa-ihp-2024

We have the pleasure to announce the Post-Quantum Algebraic Cryptography Trimester at the Institut Henri Poincaré (Paris) in Fall 2024 (September 9th - December 13th, 2024).

https://sites.google.com/view/pqa-ihp-2024

The trimester is structured around four main events:

- A preliminary summer school for preparing the main program and introducing the basic concepts of post-quantum cryptography (September 9th - 13th, 2024).
- Three thematic workshops :
  - Industrial aspects of post-quantum cryptography and fundamental issues related to the deployment of post-quantum (Workshop 1, October 7th-11th, 2024)
  - Emerging topics in the design and cryptanalysis of post-quantum schemes (Workshop 2, November 4th-8th, 2024)
  - Impact of quantum technologies for cryptography (Workshop 3, December 2nd-6th, 2024)

The trimester will also include courses, seminars and general audience talks.

Registration (in-person, on-line) is free but mandatory: https://indico.math.cnrs.fr/event/5771/registrations/442/.

