Crypto News

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

April 01, 2024

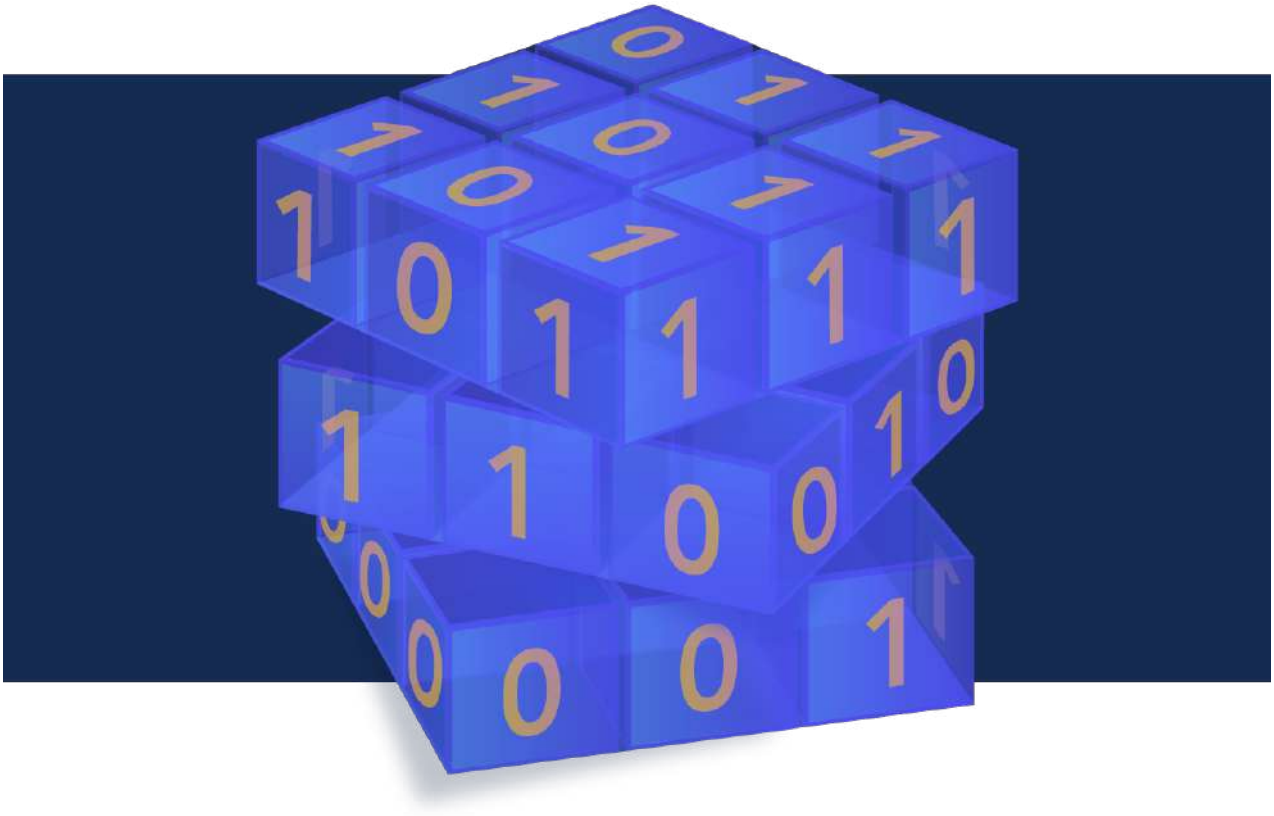


TABLE OF CONTENTS

Editorial

.
.
.

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

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

1.Why our data might need protection from the future: Apple's 'Post-Quantum' security move

by Shaun Chornobroff,
https://techxplore.com/news/2024-03-future-apple-quantum.html

Computing giant Apple recently announced it was taking steps to protect the more than 1 billion people worldwide who use its iMessage app—from a threat that doesn't yet exist. Hackers today might be able to steal your password, but they can't crack the "cryptographic keys" that lock down messages, at least not using the current generation of so-called classical computers, said University of Maryland computer science Professor Jonathan Katz.

But powerful quantum computers—machines that operate on completely different principles that allow them to do some operations exponentially more quickly—widely expected to become available in coming years, could make such security measures vulnerable.

Katz, an expert in quantum-secure cryptography who is a fellow in the Joint Center for Quantum Information and Computer Science, explained in an interview why these new quantum security measures are needed now, and what we may see in the future.

Why is Apple already talking 'post-quantum' when quantum computing is only in its infancy and no powerful, fully programmable quantum computers yet exist?

One thing is the possibility of quantum computers being built in the next decade or so, in which case we need to start being prepared now. But it's even more than that, because there's this issue that can happen where, if I encrypt a message to you today, or governments encrypt messages to each other today, an attacker could theoretically take that communication and just store it on their hard drive.

Then 10 years from now, if quantum computers come out, they can then use a quantum computer to decrypt that message. So that's why you need protection against quantum computers now, even though they may not exist for another decade.

Do hackers really want to dig through our texts? Most of them are pretty trivial.

If we're talking about the average user on the street sending a message to their friend, it's not important that the message remain secret for a decade. But if you have government-level communications, many times those need to remain classified for several decades. Then there's a concern about state-sponsored agencies going after those communications.

It seems likely that the first people who will develop quantum computers will be state-sponsored agencies because of the resources needed to develop them. Once developed, they're likely to remain classified, so that people won't know about them right away.

Is Apple protecting our texts with quantum computing, as some outlets have reported or implied?

No. The new protocol they deployed is entirely classical; it runs on classical computers like current iPhones and iPads. However, even though they are entirely classical, they are intended to provided secu-

rity against adversaries who might use quantum computers to attack them.

How can classical computers of the present fight off futuristic quantum computers?

You must get a little bit into the math, but the point is that there are a couple of examples of classical mathematical problems, where we believe that they're hard, even for quantum computers.

What is the difference between traditional cryptography and quantum cryptography?

At a high level, it comes down to the mathematical problems that they're based on. Classical cryptography algorithms are primarily based on number theoretic-type problems, which involve the relationship between prime numbers, rational numbers and algebraic integers.

Now people are looking at new classes of mathematical problems that are believed to be hard even for quantum computers. One of the leading candidates for those problems is related to something called lattices. This is another mathematical object, but a little bit different from traditional number theory.

What can the public do now to better protect their iMessage communications?

The nice thing about it is that the new protocol will be available by default. Apple rolled out this new protocol and people are going to be using it, and they're protected automatically by using it.

The main thing is, if you care about the privacy of your messages, you need to make sure to use a protocol—a method or technique used to protect networks, systems and data from unauthorized access—that offers you encrypted messaging; not every protocol offers the same level of security. You need to choose one that offers a level of security you're comfortable with.

2.Implementing Quantum Cryptography with Satellite Networks

by Igor Nowacki
https://ytech.news/en/implementing-quantum-cryptography-with-satellite-networks/

In light of recent advancements in computational power, scientists are devising a novel method for securing communications against the potential threat posed by quantum computers. This strategy involves employing quantum cryptography, which uses the principles of quantum mechanics to encode and transmit data using light particles via a satellite network.

Quantum computers have the potential to break current encryption algorithms due to their ability to perform a vast number of calculations in tandem. Quantum cryptography, however, is impervious to this threat. It operates based on quantum mechanical phenomena, which establish a secure environment by allowing the data to be transmitted as encoded light particles. This method, according to Tobias Vogl and his team, ensures that any interception attempt will be detected, since the act of measuring light particles in a quantum state inherently alters their condition.

The satellite-based system known as Quick3, introduced in Advanced Quantum Technologies, aims to overcome the limitations of earthbound quantum cryptography, which traditionally suffers from data signal degradation over long distances. At higher altitudes, where the atmosphere is less dense, signals propagate more efficiently, allowing for extended communication ranges.

By 2025, researchers intend to conduct space-based tests, pointing to a future where a network of potentially hundreds or thousands of satellites could facilitate a robust quantum communications infrastructure. This system, in addition to being innovative, provides a promising safeguard against the decrypting capabilities of future quantum computers.

The advent of quantum computing brings both unprecedented opportunities and significant threats to the cybersecurity landscape. As traditional encryption methods risk becoming obsolete due to the immense processing power of quantum machines, the industry is rapidly pivoting towards quantum-resistant technologies. Quantum cryptography is one of the most promising countermeasures to secure communications in the post-quantum era.

The principle behind quantum cryptography is the use of quantum mechanics to encode information, making it theoretically impossible for an interceptor to breach the communication without alerting the sender and receiver. Tobias Vogl's team is one of many worldwide working on such quantum secure communication systems. These rely on properties such as quantum entanglement and the no-cloning theorem to ensure security.

Regarding the market forecasts, the industry is expecting an exponential growth given the rising concerns over cybersecurity. According to market research, the global quantum cryptography market is projected to grow significantly, driven by the need for secure communication in the sectors of finance, defense, and government.

However, scaling up quantum cryptography comes with its challenges. The need for specialized hardware and the difficulty in maintaining the integrity of quantum states over long distances are key hurdles. The Quick3 satellite-based system is designed to tackle such issues by enabling longer distance quantum communication with reduced signal degradation.

This expansion of quantum cryptography carries the potential to revolutionize the way sensitive data is communicated, ensuring privacy and security amidst an increasingly vulnerable digital environment. The industry must, therefore, confront and resolve infrastructural and technical barriers to implement quantum cryptography effectively and on a global scale.

3.Is Q-Day Closer Than We Think? Ibm Researchers Say Hybrid Quantum-Ai May Pose Near-Term Threats

by Matt Swayne
https://thequantuminsider.com/2024/03/26/is-q-day-closer-than-we-think-ibm-researchers-say-hybrid-quantum-ai-may-poses-near-term-threats/

Q-Day, the time when quantum computers are powerful and stable enough to crack current encryption schemes, is thought to be a near- to far-term concern, but not an immediate concern, depending on who you ask.

Now, a team of IBM researchers report in a pre-print study that a convergence of hybrid quantum-classical computing (HQCC) and artificial intelligence (AI) technologies could be rapidly hacking away at that

deadline of when quantum could undermine current encryption methods.

If that's so, this team of researchers is underscoring the urgency of making a quantum-proof shift.

"The synergistic combination of these technologies presents known and unknown threats that need immediate attention, focus and research," the team reported in their paper.

Advances in quantum computing and AI are increasing rapidly, the researchers point out, and this progress poses both massive benefits, as well as dangers. However, the team highlights that HQCC frameworks augmented by machine learning (ML) algorithms present particularly alarming consequences.

At the top of these concerns lies the evolving capabilities of quantum algorithms like Grover's Adaptive Search (GAS) and the Harrow-Hassidim-Lloyd (HHL) method, the researchers report. GAS couples Grover's quantum algorithm with adaptive techniques, giving it the potential to be exponentially more efficient at breaking encryption through brute-force attacks.

Meanwhile, the HHL algorithm has demonstrated prowess in solving systems of linear equations exponentially faster than classical methods under certain conditions. As the researchers warn, HHL's mathematical faculties could undermine the security foundations of lattice-based cryptography, one of the prime candidates for quantum-resistant encryption.

"Quantum algorithmic improvements, including variants or extensions of the HHL algorithm, could present unforeseen challenges to lattice-based encryption," the paper states.

For instance, new algorithms may become adept at handling the noisy linear equations central to the security of lattice-based systems.

The researchers also report that the integration of AI and ML presents an additional cryptanalytic threat. "AI-driven cryptanalysis" could optimize search algorithms and uncover subtle weaknesses, accelerating the undermining of encryption standards.

This technological convergence has stark implications for PQC migration timelines. Preparing for a quantum future, governments, industries, and academics have collaborated to develop encryption methods impervious to quantum computing's mathematical advantages. However, the IBM researchers argue this evolving threat landscape necessitates expediting these efforts.

"The potential impact on classical cryptography and PQC transition timelines calls for a proactive and coordinated approach to developing and implementing quantum-resistant AI/ML cryptographic solutions," the team urges in their paper.

Among those proactive measures recommended in the paper are accelerated PQC standardization, continuous monitoring of HQCC developments and investment in novel post-quantum cryptographic research to outpace emerging cryptanalytic techniques.

The research team included IBM researchers and consultants Robert Campbell, Whitfield Diffie and Charles Robinson.

The team includes a list of several potential threats. To learn more about the study and its findings in depth, please read the paper.

4.NSA fears quantum computing surprise: 'If this black swan event happens, then we're really screwed'

by Ryan Lovelace
https://www.washingtontimes.com/news/2024/mar/25/nsa-fears-quantum-surprise-if-this-black-swan-even/

A version of this story appeared in the daily Threat Status newsletter from The Washington Times. Click here to receive Threat Status delivered directly to your inbox each weekday.

The National Security Agency fears a quantum computing breakthrough by America's adversaries would jeopardize the security of the global economy and allow foes to peer inside top-secret communications systems.

The agency's concern is that an unforeseen advance in quantum technology would crack encryption systems used to protect everything from financial transactions to sensitive communications involving nuclear weapons, according to NSA Director of Research Gil Herrera.

Speaking at an Intelligence and National Security Alliance event last week, Mr. Herrera said no country has a quantum computer that he would consider useful — yet.

He said there are a lot of teams around the world building with different technologies and someone could achieve a development representing a "black swan" event, an extremely unexpected occurrence with profound — and dangerous — consequences for U.S. national security.

"If this black swan event happens, then we're really screwed," Mr. Herrera said.

Americans could suffer consequences from such a quantum leap in several ways. Mr. Herrera said the world economy, and the U.S. market in particular, are vulnerable because most financial transactions are secured by encryption systems that can't be cracked by non-quantum means.

If quantum tech weakens or eliminates such encryption walls, then financial institutions may have to resort to older transaction methods and banks would look for other means to protect their dealings with other banks, according to Mr. Herrera.

And, he warned, other industries may be even less resilient in the face of the threat. Mr. Herrera said the threat of a quantum computer is not limited to its immediate potential damage, but to the fallout from obtaining encrypted information that was previously recorded.

Drawing on his decades of experience at Sandia National Laboratories, Mr. Herrera said a quantum advance may be able to help people find information on weapons systems that have been in the U.S. arsenal for a significant period of time.

"There are ways that we can communicate with our various partners in nuclear weapon production where public key encryption is utilized to share keys," Mr. Herrera said. "And now, what if somebody's recorded that information and they crack it?"

Details on foreign adversaries' advanced computing capabilities are closely guarded, Federal policy-makers are worried in particular about China's efforts to achieve computing breakthroughs.

Reflecting on supercomputers at a House Armed Services Committee hearing last year, Rep. Morgan Luttrell said he worried Beijing may have already surpassed the U.S. in its supercomputing prowess.

China "should have on board or online another computer that would have trumped us and pushed us back some," the Texas Republican said at the March 2023 hearing. "So the amount of money they're spending in that space as compared to us would make me think that they're ahead of us."

Retired Gen. Paul Nakasone, then in charge of U.S. Cyber Command, cautioned Mr. Luttrell against assuming that outspending America would guarantee an adversary's technological success.

5.Quantum is coming — and bringing new cybersecurity threats with it

https://kpmg.com/xx/en/home/insights/2024/03/quantum-and-cybersecurity.html

The quantum-computing revolution is upon us — a paradigm shift in computing power that harnesses the laws of quantum mechanics to solve problems far too complex for today's classical digital computers.

Quantum computers apply the unique behavior of quantum physics to computing, introducing unprecedented capabilities to traditional programming methods. From transforming drug research, energy use, manufacturing, cybersecurity and communications to enhancing AI applications, autonomous-vehicle navigation, financial modelling and more — quantum is poised to unlock a new reality.

The emerging quantum-computing industry is already making enormous advances — as more organizations discover its potential, the global market is expected to hit US$50 billion by the end of this decade. Major technology companies are rapidly developing their quantum capabilities — Amazon, IBM, Google and Microsoft, for example, have already launched commercial quantum-computing cloud services, and there are significant investments in new players such as Quantinuum and PsiQuantum.

KPMG in Canada surveyed 250 large corporations and found that about 60 percent of organizations in Canada and 78 percent in the US expect quantum computers to become mainstream by 2030. But as quantum proliferates, so do concerns about its potential impact on cybersecurity.

Most businesses surveyed are "extremely concerned" about quantum computing's potential to break through their data encryption. Sixty percent in Canada and 73 percent in the US believe "it's only a matter of time" before cybercriminals are using the power of quantum to decrypt and disrupt today's cybersecurity protocols. At the same time, however, 62 percent in Canada and 81 percent in the US admit that they need to do a better job of evaluating their current capabilities to ensure their data remains secure. KPMG Australia research shows that protecting data and dealing with cyber risks is viewed by C-suite executives and board members from private sector enterprises as a top challenge in 2024 — and for the next 3 to 5 years.

KPMG in Germany conducted research in collaboration with Germany's Federal Office for Information Security (BSI), 95 percent of respondents believe quantum computing's relevance and potential impact

on today's cryptographic security systems is "very high or high," and 65 percent also say the average risk to their own data security is "very high or high." Yet only 25 percent of firms say the threat posed is currently being addressed in their risk management strategy.

Quantum's emerging threats demand solutions

The level of preparation that organizations do today is expected to be critical to limiting their exposure and vulnerability to emerging threats — making quantum risk planning a priority. Quantum computers can break encryption methods at an alarming speed, rendering ineffective encryption tools that are widely used today to protect everything from banking and retail transactions to business data, documents, email and more.

"Harvest-now, decrypt-later" attacks could enable adversaries to steal encrypted files and store them until more advanced quantum computers emerge.

KPMG firms are helping clients take action to understand and respond to the broad and unprecedented quantum-risk environment, as asymmetric encryption is used in multiple applications, from storage to communication. The risk landscape includes the following critical areas:

- Web browsing
- Remote access
- Software
- Digital signatures
- Communication
- Crypto currencies

The quantum-risk landscape at a glance

There is little time to lose for organizations to gain a deeper understanding of the risks quantum may pose to their operations and security. For every organization that holds and processes data, they should consider the lifetime value of the data that they use, and the impact of that data being used or misrepresented by bad actors. For example:

Sensitive organizational data: Highly confidential data held by military services, national intelligence, finance and government organizations.

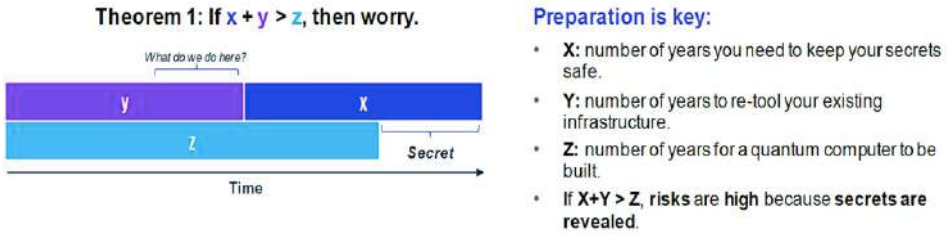
Critical infrastructure providers: Organizations whose complex systems are critical to the functioning of communities, cities, provinces and countries, including healthcare, transportation, utilities and telecommunications. Imagine, for example, the potentially disastrous impact of quantum disrupting the operation of a city's sprawling power grid.

Long-life infrastructure providers: Organizations providing systems that are built to have a long life span for profitability, including satellite communications, payment terminals, Internet of Things (IoT) sensor networks and transportation. Whether data consists of customer information, medical records or government classified data, a breach can have catastrophic financial, reputational and legal consequences. And some organizations are currently unaware of cyber attackers already accessing and storing encrypted company data with the aim of decrypting it in the future using a quantum computer.

Personal data handlers: Organizations managing personal data with a long confidentiality span are required by law to protect such data, including government, healthcare, financial firms and insurance organizations. They need to ensure protection over an extended period of 5, 10, 20 years or more.

> *Quantum computing will upend the security infrastructure of the digital economy. Quantum technology in general promises to disrupt several areas of advanced technology and bring unprecedented capabilities that can be harnessed to improve the lives of people worldwide. At first glance it appears to be a curse to security, as cryptographic algorithms that proved to be secure for decades may be breached by quantum computers. This is in fact a blessing in disguise since this challenge gives us a much-needed impetus to build stronger and more-resilient foundations for the digital economy. — Dr. Michele Mosca, Institute for Quantum Computing, The University of Waterloo*

"Mosca's Theorem", illustrated below, suggests the timeframe required to protect data. Dr. Michele Mosca's theorem stresses the need for organizations to begin applying diligence in the post-quantum space right away. It states that the amount of time that data must remain secure (X), plus the time it takes to upgrade cryptographic systems (Y), is greater than the time at which quantum computers have enough power to break cryptography (Z).



Once organizations are aware of their risk environment, they should be in a position to prioritize activity and mitigate or eliminate risks. However, this may not be a quick or simple process and may take years for each organization.

Managing technical debt, for example, can be a significant challenge for organizations relying on systems that will be incapable of running modern cryptographic profiles. There is now an opportunity to evaluate migration timelines and understand how long it will take to make infrastructure quantum resistant. To do this, organizations should understand the challenge and allocate budgets for both the mitigation and ongoing monitoring that the post-quantum world will require.

It's critical that organizations not only prepare for the quantum threat in their long-term risk planning, but also strengthen data protection now to help minimize quantum's potentially disruptive and costly impacts.

The rules of the game are changing to meet the new risk reality

As quantum emerges and organizations continue to explore and discover both its game-changing advantages and threats, new legislation and regulations are in the works. In 2022, a U.S. law was passed that requires government agencies to take action in using post-quantum cryptography — and encourages the private sector to follow suit.

The National Institute of Standards and Technology (NIST) in December 2023 released two draft publications to guide organizations aiming to redefine their capabilities and combat potential quantum-based attacks. The documents — "Quantum Readiness: Cryptographic Discovery" and "Quantum Readiness: Testing Draft Standards for Interoperability and Performance" — outline concrete issues and potential solutions when migrating to a new post-quantum cryptographic standard.

The growing list of initiatives also includes:

- The *Quantum Computing Cybersecurity Preparedness Act 2022*, advising US federal organizations

to prepare now for a post-quantum cybersecurity (PQC) world;

- National Security Memorandum on "Promoting US Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems";
- White House Memorandum on "Migration to Post-Quantum Cryptography";
- Monetary Authority of Singapore MAS/TCRS/2024/01 : Advisory on Addressing the Cybersecurity Risks Associated with Quantum;
- Quantum Security for the Financial Sector: Informing Global Regulatory Approaches, World Economic Forum in collaboration with the Financial Conduct Authority.

This growing trend is likely to be investigated by other countries as we see a global movement towards identifying the risks and requirements of secure quantum technology.

Act now to help combat quantum's risks

While quantum computing may seem like a futuristic science fiction concept, the technology is indeed poised to exert major consequences across today's cybersecurity capabilities. We believe innovation is needed without delay.

The National Institute of Standards and Technology (NIST) has released a draft of the NIST Cybersecurity Framework 2.0 (CSF 2.0) — a major update to the Cyber Security Framework (CSF) it released in 2014 to help organizations reduce cybersecurity risk. To be finalized and published in early 2024, CSF 2.0 reflects changes in the cybersecurity landscape and will offer additional guidance on implementing the CSF.

The NIST has also chosen four encryption tools that it says are designed "to withstand the assault of a future quantum computer, which could potentially crack the security used to protect privacy in the digital systems we rely on every day." The four encryption algorithms will become part of NIST's post-quantum cryptographic standard and all are expected to be finalized and ready for use in 2024.

Meanwhile, improvements and standards in Quantum Random Number Generators (QRNGs), for entropy enhancement and randomization, and Quantum Key Distribution, a secure communication method for exchanging encryption keys only known between shared parties, also aim to harness the power of quantum technology and protect data.

It's important to note that today's quantum solutions are creating a false sense of security — as we do not know if the quantum algorithms considered resistant will remain that way as quantum computers become larger and more mainstream. The danger is illustrated by the discovery of vulnerabilities in the NIST-selected encryption algorithm CRYSTALS-Kyber.

Where to start as the power of quantum advances

Organizations can start to prepare by gaining a precise understanding of potential risks across their value chain. They should also identify methods to become more cryptographically agile in updating and deploying new cryptographic techniques as they become available. It's also crucial to create end-of-life strategies for the data, products and systems that will become obsolete or unable to support new cybersecurity requirements in a quantum-computing world.

Here are key questions to ask going forward as quantum evolves:

- How long does your data need to be secure and are you liable for its management?
- What is the actual and reputational damage in case of a compromise?
- How long does it take for your system to migrate to quantum secure?
- Do you have an inventory of cybersecurity measures?
- Are you liable for a third-party service or cloud provider and are they are moving to a quantum-safe environment?

Key actions to help mitigate quantum risks:

- Provide insightful awareness training, education and roadmaps to senior leadership;
- Implement roadmaps and solutions to modernize cryptographic environments;
- Provide guidance on investing in quantum-resistant technologies;
- Develop contingency and mitigation plans to prevent a quantum attack; and
- Continuously monitor the fast-evolving quantum and security environment.

6.Hackers can unlock over 3 million hotel doors in seconds

by Andy Greenberg
https://arstechnica.com/security/2024/03/hackers-can-unlock-over-3-million-hotel-doors-in-seconds/

When thousands of security researchers descend on Las Vegas every August for what's come to be known as “hacker summer camp,” the back-to-back Black Hat and Defcon hacker conferences, it's a given that some of them will experiment with hacking the infrastructure of Vegas itself, the city's elaborate array of casino and hospitality technology. But at one private event in 2022, a select group of researchers were actually *invited* to hack a Vegas hotel room, competing in a suite crowded with their laptops and cans of Red Bull to find digital vulnerabilities in every one of the room's gadgets, from its TV to its bedside VoIP phone.

One team of hackers spent those days focused on the lock on the room's door, perhaps its most sensitive piece of technology of all. Now, more than a year and a half later, they're finally bringing to light the results of that work: a technique they discovered that would allow an intruder to open any of millions of hotel rooms worldwide in seconds, with just two taps.

Today, Ian Carroll, Lennert Wouters, and a team of other security researchers are revealing a hotel keycard hacking technique they call Unsaflok. The technique is a collection of security vulnerabilities that would allow a hacker to almost instantly open several models of Saflok-brand RFID-based keycard locks sold by the Swiss lock maker Dormakaba. The Saflok systems are installed on 3 million doors worldwide, inside 13,000 properties in 131 countries.

By exploiting weaknesses in both Dormakaba's encryption and the underlying RFID system Dormakaba uses, known as MIFARE Classic, Carroll and Wouters have demonstrated just how easily they can open a Saflok keycard lock. Their technique starts with obtaining any keycard from a target hotel—say, by booking a room there or grabbing a keycard out of a box of used ones—then reading a certain code from that card with a $300 RFID read-write device, and finally writing two keycards of their own. When they merely tap those two cards on a lock, the first rewrites a certain piece of the lock's data, and the second opens it.

Wouters and Carroll, an independent security researcher and founder of travel website Seats.aero, shared the full technical details of their hacking technique with Dormakaba in November 2022. Dormakaba says that it's been working since early last year to make hotels that use Saflok aware of their security flaws and to help them fix or replace the vulnerable locks. For many of the Saflok systems sold in the last eight years, there's no hardware replacement necessary for each individual lock. Instead, hotels will only need to update or replace the front desk management system and have a technician carry out a relatively quick reprogramming of each lock, door by door.

Wouters and Carroll say they were nonetheless told by Dormakaba that, as of this month, only 36 percent of installed Safloks have been updated. Given that the locks aren't connected to the Internet and some older locks will still need a hardware upgrade, they say the full fix will still likely take months longer to roll out, at the very least. Some older installations may take years.

“We have worked closely with our partners to identify and implement an immediate mitigation for this vulnerability, along with a longer-term solution,” Dormakaba wrote to WIRED in a statement, though it declined to detail what that “immediate mitigation” might be. “Our customers and partners all take security very seriously, and we are confident all reasonable steps will be taken to address this matter in a responsible way.”

The technique to hack Dormakaba's locks that Wouters and Carroll's research group discovered involves two distinct kinds of vulnerabilities: One that allows them to write to its keycards, and one that allows them to know *what* data to write to the cards to successfully trick a Saflok lock into opening. When they analyzed Saflok keycards, they saw that they use the MIFARE Classic RFID system, which has been known for more than a decade to have vulnerabilities that allow hackers to write to keycards, though the brute-force process can take as long as 20 seconds. They then cracked a part of Dormakaba's own encryption system, its so-called key derivation function, which allowed them to write to its cards far faster. With either of those tricks, the researchers could then copy a Saflok keycard at will, but still not generate one for a different room.

The researchers' more crucial step required them to obtain one of the lock programming devices that Dormakaba distributes to hotels, as well as a copy of its front desk software for managing keycards. By reverse-engineering that software, they were able to understand all the data stored on the cards, pulling out a hotel property code as well as a code for each individual room, then create their own values and encrypt them just as Dormakaba's system would, allowing them to spoof a working master-key that opens any room on the property. “You can make a card that really looks as if it was created by the software from Dormakaba, essentially,” says Wouters.

And how did Carroll and Wouters obtain Dormakaba's front desk software? “We nicely asked a few people,” Wouters says. “Manufacturers assume that no one will sell their equipment on eBay, and that no one will make a copy of their software, and those assumptions, I think everyone knows, are not really valid.”

Once they'd managed all that reverse-engineering work, the final version of their attack could be pulled off with little more than a $300 Proxmark RFID read-write device and a couple of blank RFID cards, an Android phone, or a Flipper Zero radio hacking tool.

The biggest caveat to the hackers' Unsaflok technique is that it still requires that they have a keycard—even an expired one—for a room somewhere in the same hotel as the room they're targeting. That's because each card has a property-specific code they need to read and then duplicate on their spoofed card, as well as a room-specific one.

Once they have that property code, the technique also requires using an RFID read-write device to write two cards—one card that reprograms a target lock as well as the second spoofed card that unlocks it.

(An Android phone or a Flipper Zero could also be used to emit one signal after another instead of the two cards, the researchers say.) The researchers hint that the first card allows them to open a target room without guessing its unique identifier in the hotel's system, but declined to say exactly what that first card does. They're holding that element of the technique in confidence to avoid giving too clear a set of instructions to would-be intruders or thieves.

By contrast, one security researcher presented a similar hotel keycard hack that opened locks sold by the firm Onity at the Black Hat conference in 2012 with no such obfuscation, and allowed any hacker to build a device that opened any of Onity's 10 million locks worldwide. When Onity refused to pay for the hardware upgrades necessary to solve the problem and instead put the onus on its customers, the issue remained unfixed in many hotels—and eventually was exploited in at least one hacker's cross-country burglary spree.

Carroll and Wouters say that they're trying to avoid that scenario by taking a more cautious approach, while still warning the public about their technique, given that hundreds of properties will likely remain vulnerable to it even now that Dormakaba has offered its fix. “We're trying to find the middle ground of helping Dormakaba to fix it quickly, but also telling the guests about it," says Carroll. “If someone else reverse-engineers this today and starts exploiting it before people are aware, that might be an even bigger problem.”

To that end, Carroll and Wouters point out that hotel guests can recognize the vulnerable locks most often—but not always—by their distinct design: a round RFID reader with a wavy line cutting through it. They suggest that if hotel guests do have a Saflok on their door, they can determine if it's been updated by checking their keycard with the NFC Taginfo app by NXP, available for iOS or Android. If the lock is manufactured by Dormakaba, and that app shows that the keycard is still a MIFARE Classic card, it's likely still vulnerable.

If that's the case, the two researchers say, there's not much to do other than avoid leaving valuables in the room and, when you're inside, bolt the chain on the door. They warn that the deadbolt on the room is also controlled by the keycard lock, so it doesn't provide an extra safeguard. “If someone locks the deadbolt, they’re still not protected,” says Carroll.

Even without a perfect or fully implemented fix, Wouters and Carroll argue, it's better for hotel guests to know the risks than to have a false sense of security. After all, they point out, the Saflok brand has been sold for more than three decades and may have been vulnerable for much or all of those years. Though Dormakaba says it's not aware of any past use of Wouters' and Carroll's technique, the researchers point out that doesn't mean it never happened in secret.

“We think the vulnerability has been there for a long time,” says Wouters. “It's unlikely that we are the first to find this.”

7.Apple Chip Flaw Lets Hackers Steal Encryption Keys

by Kim Zetter
https://www.zetter-zeroday.com/apple-chips/

A group of researchers has found a serious security vulnerability in Apple’s M-series of chips that would allow attackers to steal secret keys from Mac and iPad devices.

The problem affects Apple M1, M2 and M3 chips — which have been used in Apple desktops, notebooks and tablets since late 2020 — and occurs when they're performing cryptographic functions. Attackers could potentially exploit the issue to steal cryptographic keys from systems — for example, the keys for cryptographic wallets stored on devices or to secure email communication and cloud accounts.

There has been a lot of confusion about the severity and implications of the vulnerability since the researchers published their findings today, so I'm going to try to clarify what the problem entails and what can and cannot be done to mitigate it. I should warn you, though, that this is pretty technical — more technical than I usually publish here at Zero Day. I think it's important to cover this, however, because after I posted about this on Twitter, many people have assumed this is far worse than it is.

reporter Dan Goodin wrote a good original story about the issue, but his piece is even more technical so I'll try to explain it here in language that's simpler. The bottom line for users is that there is nothing you can do to address this. The fix lies with cryptographic application developers, who need to implement mitigations for the problem and then issue updates to their applications.

Robert Graham, CEO of security consultancy Errata Security, says to be on the safe side, anyone with a lot of money in a crypto wallet on their Apple device should probably remove it for the time being. "There are people right now hoping to do this [attack] and are working on it, I would assume," he says.

Background

Apple's chips, and other modern processors, have an optimization technique called prefetching that is designed to speed up processing by looking in the computer's memory for patterns in your activity — functions you frequently perform and data you frequently access. The prefetcher determines what data you've accessed before and places in the system's cache memory a pointer, or address locator, for where that data or function code is located in memory so that the system can find and use it more quickly when you need it. The problem is that the cache can "leak" information stored in it, allowing attackers to grab it in so-called side-channel attacks. Because of this, it's standard to prohibit systems from mixing data with addresses or address pointers; if data gets mixed with an address, then when the user accesses the address, it might get placed in the cache where it could get leaked.

But a team of seven researchers from universities across the U.S. released a paper and video today showing that the Apple M-series chips mix data and addresses, which can be exploited to obtain cryptographic keys. They were able to devise a malicious application that, when downloaded to a user's machine, tricks Apple's prefetcher — known as the Data Memory-Dependent Prefetcher, or DMP — into placing secret key-related material in the cache by tricking it into believing the key material was an address. The research was partially funded by grants from the Air Force Office of Scientific Research and the Defense Advanced Research Projects Agency, according to the researchers' web site.

The cryptographic key itself isn't placed in cache. But bits of material derived from the key gets placed in the cache, and an attacker can piece these bits together in a way that allows them to reconstruct the key, after causing the processor to do this multiple times. The researchers were able to derive the key for four different cryptographic algorithms: Go, OpenSSL, CRYSTALS-Kyber and CRYSTALS-Dilithium. The latter two are considered quantum-resistant algorithms — algorithms believed to be so secure they could not be cracked using a quantum computer. They didn't test their attack against other algorithms but believe it would be successful against others as well.

Goodin noted in his Arstechnica piece that the attack the researchers designed takes less than an hour to extract enough data from the cache to reconstruct a 2048-bit RSA key and "a little over 2 hours to extract a 2048-bit Diffie-Hellman key. The attack takes 54 minutes to extract the material required to assemble a Kyber-512 key and about 10 hrs for a Dilithium-2 key."

Matthew Green, a cryptographer and computer science professor at Johns Hopkins University, calls it a clever attack.

"*The Apple code … has a certain set of criteria that it applies [to determining] what's an address," he says. "The researchers figured out that if [their malware provides] a message to be decrypted, the decryption algorithm at some point will combine the key with part of [that] message…. And it looks enough like an address that it tricks this little prefetcher [into placing it into cache]*."

He adds that determining what is and isn't an address is a tough problem for prefetchers to solve.

"Lots of things look like an address, and [the prefetcher] just kind of has to guess what's actually an address or not, and so [the researchers] are able to squeeze [through] that guess," he says.

The researchers created a malicious program that they call GoFetch that performs this trick, as well as a video demonstrating the attack in action.

Engineers designing applications that perform cryptographic functions implement a technique called constant-time programming, which effectively prevents data from being mixed with addresses and getting placed in the cache and leaked. But in the case of the M-series chips, constant-time programming isn't effective says Daniel Genkin, a cybersecurity and privacy professor at Georgia Institute of Technology and one of the researchers who discovered the flaw.

He says the problem with the prefetcher on the Apple M-series chips exists because unlike other prefetchers in other chips that only examine addresses, the prefetcher in the Apple chips are programmed to also look at values stored inside addresses and this therefore puts them in the vulnerable position of confusing a value with an address and placing it into the cache.

"If a value looks like an address, then [the prefetcher] might decide to treat it like an address," he says.

The M3 chip does have a special bit in the processor that programmers can set to disable the prefetcher for cryptographic functions and preventing cryptographic data from being placed in the cache; but the M1 and M2 do not allow the prefetcher to be disabled.

Attack Vector

How does an attacker trick the processor? They can do this by slipping malicious code into an application that a user downloads to their computer. The GoFetch attack code they created doesn't require root access on a machine to work; it can trick the processor into doing this with just the same level of access that any third-party application has on a machine.

It could also be conducted on a cloud server hosting virtual machines used by multiple parties.

"If I'm on Amazon on a cloud server using a virtual machine and there's another virtual machine using keys there, that's another example of a case where this could be a problem," says Green. But he cautions that it's not an easy attack to pull off.

It's also theoretically possible for an attacker to pull this off by embedding malicious code into Javascript on a web site so that when a computer with an M-series chip visits the site, the attacker's malicious code can conduct the attack to grab data from the cache. The researchers didn't test a web site attack, but Green says the scenario is plausible. It would also be a more concerning attack, he notes, because attackers could scale it to attack thousands of computers quickly.

Green says the risk for most people from the GoFetch application-style attack is probably low.

“We’re talking about high-end users, like someone who has a cryptocurrency wallet with a lot of money,” he says. But he notes that in theory this attack might be used to break the TLS cryptography that a computer’s browser uses to encrypt communication between their computer and web sites, which could allow attackers to decrypt that communication to extract a user’s session cookie for their Gmail or other web-based email account and use it to log into the account as them.

“I’m not saying it’s a practical attack I’m just saying that’s the kind of threat you might be worried about,” he says, “You can get [other] very high-valued keys potentially” including their iCloud keys to access backed up data.

The researchers reported the issue to Apple in December, but other than thanking them for their work, Genkin says Apple didn’t indicate what, if anything, it might do to address the problem.

The Fix

Because this is not a flaw in the Apple operating system but instead is a hardware issue in the chip, Apple can’t just release a patch the way it would for software flaws. It could, however, address the problem in subsequent chip designs.

Asked for comment about the problem, an Apple spokesman didn’t answer my questions directly but said only, “We want to thank the researchers for their collaboration as this research advances our understanding of these types of threats.” He also sent me a link to an Apple site for application developers.

The site includes an instruction to developers of cryptographic applications to include code in their program that causes the processor to implement data-independent timing, or DIT, that effectively disables the prefetcher when the computer is performing cryptographic functions for their application. It’s not clear how long this instruction has been on Apple’s developers site; there’s no date on the page.

There are two issues with the DIT fix, however. 1) Disabling the prefetcher will likely slow down the processor during cryptographic functions, the researchers say. By how much, they don’t know. 2) The DIT works only for Apple’s M3 chips; as noted above, the M1 and M2 chips don’t have the ability to disable the prefetcher. Apple only debuted the M3 chip recently – the first Macbooks with M3 chips became available last October. This suggests that Apple may have become aware of the problem on its own, sometime after products with M1 and M2 chips were sold (and before the researchers notified them about the issue in December), and added this ability to disable the prefetcher in the M3 chip as a result. If this is the case, then it means Apple made the change without telling consumers about the issue with their M1 and M2 chips. But this is only speculation at this point.

Green says he was never aware of this instruction to developers to implement DIT.

“I implement crypto, and this is literally the first time I’ve heard of it,” he says, noting that other cryptographers have likely missed it as well. “I would say that the number of crypto libraries that are doing this has to be pretty low. Zero.”

[After this story published, Apple told me they just posted the instruction about the DIT to their web site yesterday, timed to the public release of the researchers' findings, which means that developers were not told to do this fix prior to yesterday's release and explains why Green had not heard of it before.]

Genkin says that Apple’s own crypto library, Core Crypto, does disable the prefetcher for the M3 chip. He doesn’t know if developers of other cryptography applications have followed the instructions on Apple’s developer page to implement the DIT fix. But he says the message to enable the DIT to avoid

this problem makes it clear that developers shouldn't consider it optional.

"To experienced application developers, if you say enable DIT to enable constant time, what I'm hearing is if you don't do this it will be bad," he says. "For cryptographic engineers that know the literature well, it's more than sufficient."

The researchers suggest some other mitigations that developers can implement in their cryptographic programs to protect the secret key data when a system performs cryptographic functions. But Green says they're not clean fixes to address the problem in M1 and M2 chips.

UPDATED 3.22.23: To add speculation about when Apple may have learned about this issue and to add Apple's statement about when the DIT instruction to developers got added to its web site.

8.Unpatchable vulnerability in Apple chip leaks secret encryption keys

by Dan Goodin
https://arstechnica.com/security/2024/03/hackers-can-extract-secret-encryption-keys-from-apples-mac-chips/2/

A newly discovered vulnerability baked into Apple's M-series of chips allows attackers to extract secret keys from Macs when they perform widely used cryptographic operations, academic researchers have revealed in a paper published Thursday.

The flaw—a side channel allowing end-to-end key extractions when Apple chips run implementations of widely used cryptographic protocols—can't be patched directly because it stems from the microarchitectural design of the silicon itself. Instead, it can only be mitigated by building defenses into third-party cryptographic software that could drastically degrade M-series performance when executing cryptographic operations, particularly on the earlier M1 and M2 generations. The vulnerability can be exploited when the targeted cryptographic operation and the malicious application with normal user system privileges run on the same CPU cluster.

Beware of hardware optimizations

The threat resides in the chips' data memory-dependent prefetcher, a hardware optimization that predicts the memory addresses of data that running code is likely to access in the near future. By loading the contents into the CPU cache before it's actually needed, the DMP, as the feature is abbreviated, reduces latency between the main memory and the CPU, a common bottleneck in modern computing. DMPs are a relatively new phenomenon found only in M-series chips and Intel's 13th-generation Raptor Lake microarchitecture, although older forms of prefetchers have been common for years.

Security experts have long known that classical prefetchers open a side channel that malicious processes can probe to obtain secret key material from cryptographic operations. This vulnerability is the result of the prefetchers making predictions based on previous access patterns, which can create changes in state that attackers can exploit to leak information. In response, cryptographic engineers have devised constant-time programming, an approach that ensures that all operations take the same amount of time to complete, regardless of their operands. It does this by keeping code free of secret-dependent memory accesses or structures.

The breakthrough of the new research is that it exposes a previously overlooked behavior of DMPs in Apple silicon: Sometimes they confuse memory content, such as key material, with the pointer value that is used to load other data. As a result, the DMP often reads the data and attempts to treat it as an address to perform memory access. This "dereferencing" of "pointers"—meaning the reading of data and leaking it through a side channel—is a flagrant violation of the constant-time paradigm.

The team of researchers consists of:

- Boru Chen, University of Illinois Urbana-Champaign
- Yingchen Wang, University of Texas at Austin
- Pradyumna Shome, Georgia Institute of Technology
- Christopher W. Fletcher, University of California, Berkeley
- David Kohlbrenner, University of Washington
- Riccardo Paccagnella, Carnegie Mellon University
- Daniel Genkin, Georgia Institute of Technology

In an email, they explained:

> *Prefetchers usually look at addresses of accessed data (ignoring values of accessed data) and try to guess future addresses that might be useful. The DMP is different in this sense as in addition to addresses it also uses the data values in order to make predictions (predict addresses to go to and prefetch). In particular, if a data value "looks like" a pointer, it will be treated as an "address" (where in fact it's actually not!) and the data from this "address" will be brought to the cache. The arrival of this address into the cache is visible, leaking over cache side channels.*
>
> *Our attack exploits this fact. We cannot leak encryption keys directly, but what we can do is manipulate intermediate data inside the encryption algorithm to look like a pointer via a chosen input attack. The DMP then sees that the data value "looks like" an address, and brings the data from this "address" into the cache, which leaks the "address." We don't care about the data value being prefetched, but the fact that the intermediate data looked like an address is visible via a cache channel and is sufficient to reveal the secret key over time.*

In Thursday's paper, the team explained it slightly differently:

> *Our key insight is that while the DMP only dereferences pointers, an attacker can craft program inputs so that when those inputs mix with cryptographic secrets, the resulting intermediate state can be engineered to look like a pointer if and only if the secret satisfies an attacker-chosen predicate. For example, imagine that a program has secret s, takes x as input, and computes and then stores $y = s \oplus x$ to its program memory. The attacker can craft different x and infer partial (or even complete) information about s by observing whether the DMP is able to dereference y. We first use this observation to break the guarantees of a standard constant-time swap primitive recommended for use in cryptographic implementations. We then show how to break complete cryptographic implementations designed to be secure against chosen-input attacks.*

Enter GoFetch

The attack, which the researchers have named GoFetch, uses an application that doesn't require root access, only the same user privileges needed by most third-party applications installed on a macOS system. M-series chips are divided into what are known as clusters. The M1, for example, has two clusters: one containing four efficiency cores and the other four performance cores. As long as the GoFetch app and the targeted cryptography app are running on the same performance cluster—even when on separate cores within that cluster—GoFetch can mine enough secrets to leak a secret key.

The attack works against both classical encryption algorithms and a newer generation of encryption that has been hardened to withstand anticipated attacks from quantum computers. The GoFetch app requires less than an hour to extract a 2048-bit RSA key and a little over two hours to extract a 2048-bit Diffie-Hellman key. The attack takes 54 minutes to extract the material required to assemble a Kyber-512 key and about 10 hours for a Dilithium-2 key, not counting offline time needed to process the raw data.

The GoFetch app connects to the targeted app and feeds it inputs that it signs or decrypts. As it's doing this, it extracts the app secret key that it uses to perform these cryptographic operations. This mechanism means the targeted app need not perform any cryptographic operations on its own during the collection period.

The RSA and Diffie-Hellman keys were processed on implementations from Go and OpenSSL and the Kyber and Dilithium from CRYSTALS-Kyber and CRYSTALS-Dilithium. All four implementations employ constant-time programming, proving that the DMPs in Apple silicon defeat the widely deployed defense.

Cryptography	Online Time (minutes)			Offline Time (minutes)
	❶	❷	❸	
RSA-2048	5	18	26	~0
DH-2048	5	6	127	~0
Kyber-512	6	10	43	286
Dilithium-2	5	13	577	274

Experimental results of four cryptographic attack PoCs. This show the mean of three runs of each PoC. Online time refers to the required time for a co-located attacker process, which includes (1) standard eviction sets generation; (2) compound eviction set finding; and (3) DMP leakage. Offline time is the post-processing (e.g. lattice reduction) time to complete secret key recovery. The time for the offline signature collection phase of Dilithium-2 is not included.

GoFetch isn't the first time researchers have identified threats lurking in Apple DMPs. The optimization was first documented in 2022 research that discovered a previously unknown "pointer-chasing DMP" in both the M1 and Apple's A14 Bionic chip for iPhones. The research, from a different assemblage of academics, gave rise to Augury, an attack that identified and exploited a memory side channel that leaked pointers. Ultimately, Augury was unable to mix data and addresses when constant-time practices were used, a shortcoming that may have given the impression the DMP didn't pose much of a threat.

"GoFetch shows that the DMP is significantly more aggressive than previously thought and thus poses a much greater security risk," the GoFetch authors wrote on their website. "Specifically, we find that any value loaded from memory is a candidate for being dereferenced (literally!). This allows us to sidestep many of Augury's limitations and demonstrate end-to-end attacks on real constant-time code."

Penalizing performance

Like other microarchitectural CPU side channels, the one that makes GoFetch possible can't be patched in the silicon. Instead, responsibility for mitigating the harmful effects of the vulnerability falls on the people developing code for Apple hardware. For developers of cryptographic software running on M1 and M2 processors, this means that in addition to constant-time programming, they will have to employ other defenses, almost all of which come with significant performance penalties.

One of the most effective mitigations, known as ciphertext blinding, is a good example. Blinding works by adding/removing masks to sensitive values before/after being stored to/loaded from memory. This effectively randomizes the internal state of the cryptographic algorithm, preventing the attacker from controlling it and thus neutralizing GoFetch attacks. Unfortunately, the researchers said, this defense is both algorithm-specific and often costly, potentially even doubling the computing resources needed in

some cases, such as for Diffie-Hellman key exchanges.

One other defense is to run cryptographic processes on the previously mentioned efficiency cores, also known as Icestorm cores, which don't have DMP. One approach is to run all cryptographic code on these cores. This defense, too, is hardly ideal. Not only is it possible for unannounced changes to add DMP functionality to efficiency cores, running cryptographic processes here will also likely increase the time required to complete operations by a nontrivial margin. The researchers mention several ad-hoc defenses, but they are equally problematic.

The DMP on the M3, Apple's latest chip, has a special bit that developers can invoke to disable the feature. The researchers don't yet know what kind of penalty will occur when this performance optimization is turned off. (The researchers noted that the DMP found in Intel's Raptor Lake processors doesn't leak the same sorts of cryptographic secrets. What's more, setting a special DOIT bit also effectively turns off the DMP.)

Readers should remember that whatever penalties result will only be felt when affected software is performing specific cryptographic operations. For browsers and many other types of apps, the performance cost may not be noticeable.

"Longer term, we view the right solution to be to broaden the hardware-software contract to account for the DMP," the researchers wrote. "At a minimum, hardware should expose to software a way to selectively disable the DMP when running security-critical applications. This already has nascent industry precedent. For example, Intel's DOIT extensions specifically mention disabling their DMP through an ISA extension. Longer term, one would ideally like finer-grain control, e.g., to constrain the DMP to only prefetch from specific buffers or designated non-sensitive memory regions."

Apple representatives declined to comment on the record about the GoFetch research.

End users who are concerned should check for GoFetch mitigation updates that become available for macOS software that implements any of the four encryption protocols known to be vulnerable. Out of an abundance of caution, it's probably also wise to assume, at least for now, that other cryptographic protocols are likely also susceptible.

"Unfortunately, to assess if an implementation is vulnerable, cryptanalysis and code inspection are required to understand when and how intermediate values can be made to look like pointers in a way that leaks secrets," the researchers advised. "This process is manual and slow and does not rule out other attack approaches."

9.Cybersecurity's Future: Facing Post-Quantum Cryptography Peril

by Joao-Pierre S. Ruth
https://www.informationweek.com/cyber-resilience/cybersecurity-s-future-facing-post-quantum-cryptography-peril#close-modal

Google published a threat model recently for the coming era of post-quantum cryptography (PQC), putting into perspective potential vulnerabilities that may surface if there is not a migration from "classical cryptographic algorithms to PQC." The risk of "store-now-decrypt-later" style attacks, where bad actors harvest data they cannot read currently with the intent of breaking the encryption in the future,

intensifies with the expected advent of quantum-grade resources at their disposal.

It begs the question of how vulnerable organizations will become if they do not make such a transition fast enough? Will it be open season on their data without quantum encryption? Does the post-quantum future mean quantum encryption will be mandatory for even the most basic forms of cyber resilience?

The Quantum Clock Is Ticking

The National Institute of Standards and Technology (NIST) issued guidance that calls for migration of federal government systems to post-quantum cryptography by 2035, which motivated other stakeholders to set comparable transition timetables, says Richard Searle, vice president of confidential computing with multi-cloud security company Fortanix.

“Often when people are talking about post-quantum cryptography, they’re talking about two different time horizons,” he says. One of those timeframes is based on when a cryptanalytically relevant quantum computer is established and proven, Searle says. While that has been expected to happen on a 10-year horizon, he says that does not seem to be the case anymore. The other timeframe is a deadline for when post-quantum cryptography migration must be achieved. “It does create this sort of cliff-edge mentality about the transition, but inevitably it’s not going to be anything like that,” Searle says. “It’s going to be a piecemeal migration.”

A gradual approach seems likely, he says, because of two fundamental reasons. Companies and organizations currently use cryptography in a raft of different tasks within their business, Searle says, and often that cryptography is shared with a third party. “Establishing which elements of those business processes need to be migrated first comes down to a risk management-based approach,” he says. “You’re not going to be able to do this sort of ‘Big Bang’ transition. It’s going to have to be done on a process-by-process, data-by-data basis.

From Worse to Worse

Though there is some time to develop quantum encryption resources, the potential risks of not shoring up such defenses may lead to severe consequences.

“Do you remember Heartbleed?” asks, Kevin Bocek, chief innovation officer, with cybersecurity company Venafi, referring to the infamous vulnerability in an older OpenSSL cryptographic library -- dubbed by some at the time as one of the most dangerous security risks to the web. “Imagine a Heartbleed happening every day and imagine Heartbleed getting worse and worse and worse every day starting with a little bleed, getting to a big bleed.”

Quantum compute resources to break encryption might be initially hard to come by for bad actors, but aggressor states that want to launch damaging attacks could hasten the availability of such tools. “What we’ll see as the quantum capabilities move from the most sophisticated adversaries -- that of course is nation states, and generally that’s a small set of nation states -- as that moves down, that becomes more available to a broader set of adversaries,” says Bocek. This also means the most sophisticated adversaries will become even more capable as well, he says.

Rather than one linear threat in the post-quantum world, Bocek says, the threat will look more like a curve. “You can imagine Heartbleed, or really bad Heartbleed, and then really, really bad, bad, bad Heartbleed, and then it keeps on getting worse and worse as the various sets of adversaries gain capabilities.” He says this crescendo set of security challenges may continue as the world goes post-quantum. “We’ve been fortunate,” Bocek says. “We’ve been reliant on a type of technology for over 35 years that has allowed us to do what we’re doing right now, and to do so privately and to know that one ma-

chine talking to another machine is authentic, and that's going to go away."

A Gradual Erosion of Encryption

Min-Hank Ho, vice president of products with Baffle, a data protection provider for cloud environments, says there might not be a drastic turn where current encryption fails the moment quantum compute arrives on the scene -- it could be more complex. "Encryption, I think to a lot of people, is what you see in the movies with switching codes and bites," he says.

In reality, Ho says, there are different types of encryptions. Asymmetric encryption is currently used for SSL/TLS communication to the web and is used for identifying services, he says. Encryption for data protection -- as it is being stored and even for data as it is being used by a computing system -- is symmetric encryption, according to Ho.

Such forms of encryption might not be immediately made obsolete by quantum computers -- at least for the moment. "As far as the current state-of-the-art, what everybody knows today, symmetric encryption is generally pretty resistant to quantum computing attacks," Ho says. "That's because the algorithms available to quantum computers today to target symmetric encryption is not that great."

Quantum computers are expected to deliver tremendous compute power that would reduce the time needed to crack encryption, but for the moment current algorithms still pose a challenge. "When they designed this algorithm, the key size is so large, even if you were to cut it by a square root, it's like, 'Oh man, it's gonna take forever,'" Ho says. A standard that could be relevant post-quantum is CNSA (Commercial National Security Algorithm) 2.0, he says, which includes AES (Advanced Encryption Standard) with 256 bit keys.

"Where things go off the rails a little bit is the asymmetric algorithms," he says. "RSA and DSA by far are the most widely used today." For a while, Ho says, the sense was that if there was a large enough key size it might not be so dire -- but there may actually be a threat.

"Network communication like the ones that we do over the web, they're kind of ephemeral and they're generally pretty easy to upgrade, relatively speaking, because we've done this many times before," Ho says. "Your web browser automatically updates. The websites automatically update. That's not so bad." Managing identities with those updates can get a little tricky. "Somewhere stored in these computing systems is a certificate assigned by an old algorithm," he says. "Everybody has to find all of those, update all of those."

To put in perspective what a daunting task that can be, Ho says not too long back there were still ATMs that used Windows XP. "You would think a system that is trying to process money would be the most secure, but it's not."

The post-quantum cryptography era might not be open season on unprepared systems, he says, but rather an uneven landscape. There are layers of concerns to consider. "What I think scares me a little bit is that this type of attack is somewhat quiet," Ho says. "The people who are going to be taking advantage of this -- the few people initially who have quantum computers as you can imagine, probably state actors -- will want to keep this on the downlow. You wouldn't know it, but they probably already have access."

Attacks From Many Sides

Michael Osborne, CTO IBM Quantum Safe / Security Research, says many may be limiting their concerns to attacks that harvest data to decrypt at some point in the future with quantum machines. "Actu-

ally, we do not think that is a good reflection of the threat scenario," he says.

Lower hanging fruit may be available for bad actors to launch cyberattacks, even those who may play the long game. "There's not going to be one date where all of a sudden there will be a cryptographically relevant quantum computer," Osborne says. "There will be an evolution of capability over the years. The first attacks are going to be very, very expensive. They're going to be probabilistic. They might take weeks or months for a single attack."

Given the options, he says attackers that want results are not likely to spend time scouring through terabytes of encrypted communications in the hope they fish out one that might have something interesting inside. "Attackers are going to choose their targets very carefully, and if you're an attacker it has to have a certain value," Osborne says. "That might be a key which is still trusted for software updates." This could mean inserting malware into a software update that no one will notice and then gaining access to all the current communications, not data harvested from 10 years prior.

Defenders, Bad Actors, and Costs

"At some point -- and it'll be quite some time after the first capability -- it will be cost-effective to start decrypting a large amount of information, but that's way downstream compared to some of the attacks that we're going to see," he says.

It may be possible to shore up certain cyber defenses while quantum computers continue their development and evolution, and before bad actors start to leverage their capabilities. "There is time to the extent that obviously things which are not protected with quantum-safe mechanisms -- they are lost to a quantum future," Osborne says.

Basic cybersecurity hygiene will still be relevant, he says, while preparing for that quantum future because other types of attacks are not expected to simply disappear as technology advances.

For many enterprises and organizations, cybersecurity represents a cost -- in time, money, and resources. The notion of needing to develop a whole new type of defense might make the C-suite grumble out the bottom line, but the need for protection will persist and the development of quantum safety may just become part of the overall security budget.

"It's a cost," Osborne says. "It's an insurance. Security is an insurance cost. It's very difficult to compete today with the ransomware threat, but because that's the priority today. CSOs have so many priorities, and money is a finite resource. What does the strategy become? To just hook on to the things you have to do anyway to take you on that journey rather than as a separate initiative."

The risks of a post-quantum future might seem a distant problem, but the repercussions could be dramatic for those who go unprepared or try to cut corners on such defenses.

The Pass-Fail Security Dilemma

"From a technical perspective … being quantum-safe -- it's a binary thing. You either are or you're not," says Duncan Jones, head of quantum cybersecurity with quantum computing company Quantinuum.

If there is a particular computer system that an organization fails to migrate to new standards and protocols, he says that system will be vulnerable. However, the barrier to entry for access to quantum compute resources may limit the potential for early attackers who already have pockets deep enough to procure the technology. "The capability to mount attacks with quantum computers is going to be -- when it

first arrives, it's going to be only available to the wealthiest," Jones says. "This is a nation state capability when it first arrives."

He explains that it is unlikely there would be a singular day when all bets are off, and everyone would be equally targeted hackers armed with quantum power. "It's going to be very selective at first," Jones says, "but over time, as we get past 'Q-Day' and powerful quantum computers are commonplace, then yes -- if you leave a system undefended, it can be attacked with a quantum computer."

Attackers would still need to work on gaining access to a system, but he calls it "a big mistake to leave systems unprotected" from such newer types of breaches.

There is a fair amount of uncertainty in all aspects of the PQC future, for attackers and defenders. "On the threat side, the time scales are not clear and also, we never quite know what other people will do with quantum computers," Jones says. "It may even be the case that Shor's algorithm, which is the main threat we're thinking about, isn't the only thing that can threaten us." Other algorithms may yet be developed that get put to work in quantum hacking, Jones says.

"On the defense side, I see there are two things you can do to be quantum-safe," he says.

One of them is the algorithms, Jones says, which includes NIST's efforts in this evolving space. "We think that's gonna be a big part of the solution but it's one part of the solution."

The other idea builds on a desire to fight quantum with quantum. "We work with organizations who want to use quantum technology to strengthen their keys today, so that's using quantum techniques to produce unpredictable keys that even quantum computers can't sort of predict as well," he says. "And then there's other people looking at QKD (quantum key distribution) as an alternative or a companion. There's lots of things that are in flux."

10.DSA advances cryptographic processing and ZK-proof computation

by Roxanne Williams
https://www.cryptonewsz.com/dsa-advances-cryptographic-processing-and-zk-proof-computation/

DSA, an acronym for the Decentralized Storage Alliance, has announced the release of cryptographic processing improvements. This officially marks a leap forward in the ZK Proof Computation to enhance the performance by almost 80%. At the core are computational algorithms and processing flows, both of which are slated for improvement within the Filecoin Network.

Project components relying on zk-SNARK, a variant of ZK proof, will experience the enhancements to a far greater extent. Advancement is designed to optimize more than 100,000 GPUs that are in use, representing approximately $100 million of deployed capital.

Three computations have been selected to achieve the goal of 80% higher efficiency. These include MSM, NTT, and Poseidon hashing.

MSM, or Multi-Scalar Multiplication, is the key computational primitive in zk proofs. Their utility extends to two aspects: committing to polynomials in SNARK systems and calculating the sum of multiple scalar

multiplications. NTT, or Number Theoretic Transformations, are known to facilitate efficient polynomial multiplication. They leverage the potential of Fast Fourier Transform-style algorithms.

Poseidon Hashing, a SNARK-friendly cryptographic hash function, is known to require 8 times fewer constraints per message bit than previous hashes like Pedersen hash.

Moving forward, DSA has plans in the pipeline to improve efficiency further and simplify operations in the Filecoin ecosystem. It also plans to enable a higher number of specializations. DSA may employ different algorithmic enhancements and circuit-specific implementations.

Kelly Olson, a member of the team and one of the leaders, appreciated the software for being efficient and delivering results at a lower cost. Kelly also acknowledged that the work done on the project was pretty intensive, yielding a reduced concern when it comes to storage providers.

Daniel Leon, the founding advisor of the DSA, appreciated the advancements, citing that they would reduce the cost not for select aspects but for the entire network. Daniel added that the benefit will extend to end users of decentralized storage technologies.

The development comes months after DSA unveiled a reimagined website that captivated AI-generated visuals to carry forward its mission of empowering enterprises to utilize decentralized data storage along with processing capabilities. This dates back to the middle of 2023 and was done in association with Supranational.

Their collaboration has reportedly reduced the cost of the data onboarding process by 90%. Another notable development in which DSA emphasized bringing down the decentralized storage cost was the announcement of the Golden Gate upgrade.

Simply put, DSA has previously worked to cut costs and continues to do so without compromising on other feats that it can achieve. For instance, a lead forward in zk proof computation. Select zk-proof advancements have been integrated into Filecoin to improve the performance by ~80%. There are plans to improve the performance further and increase efficiency.

11.Where are the Worldwide Quantum Networking Testbeds?

by Amina Bashir and Doug Finke
https://quantumcomputingreport.com/where-are-the-worldwide-quantum-networking-testbeds/

One of the key applications of quantum technology is to create a quantum network that can communicate messages and quantum states in a way that gives them more protection and other properties due to the laws of physics. Although this research is still very early, a number of organizations have started to create quantum testbeds to try out these quantum networks in order to continue developing them and advancing the technology. Most of these testbeds are used for Quantum Key Distribution, which one might argue as the simplest application for a quantum network. However, later on there can be a range of new applications including quantum sensor networks, distributed quantum computing, and blind quantum computing that are more complex, and can bring completely new capabilities.

To get a handle on the testing that is going on, we curated a list of all public mentions of quantum network testbed activity going on worldwide to show the scope of the activity and where it is happening.

We should say that this research is very dynamic, and our listing is only a snapshot of a moment in time, so there may be some changes after we publish this. We welcome any comments or updates from people involved with these projects.

The table below shows a listing of 44 testbeds that we found along with a link to a description of them available on the internet along with the country they are located in and our best determination of the status. Notably, some of these testbeds may have been created only for temporary use and may have already been retired. Some of them may have been announced and are under construction. In the table below, we have noted both these cases if we are aware of it.

For more details about quantum networking in general, you can obtain a report written by Global Quantum Intelligence titled Quantum Safe Outlook that provides additional technical details on quantum networking as well as the software based Post Quantum Cryptography (PQC), which is another approach to providing encryption that is safe from quantum computer based attacks.

Table of Known Quantum Networking Testbeds

Network Name	Country	Status
Brookhaven National Laboratory Quantum Network Facility & The Long Island Quantum Information Distribution Network (LiQuiDNET) Testbed	US – New York	Development
GothamQ	US – New York	Development
Chicago Quantum Exchange (CQE) + Toshiba	US – Illinois	Active
The Washington Metropolitan Quantum Network Research Consortium or DC-Qnet	US – Washingt	Development
EPB Quantum Network	US – Tennesse	Active
Public Quantum Network	US – Illinois	Active
Advanced Quantum Networks for Scientific Discovery (AQNET-SD) project	US – Illinois,	Announced
Illinois-Express Quantum Network (IEQNET) & FQNET	US – Illinois	Active
Quantum Networks to Connect Quantum Technology (QuaNeCQT) Project & MARQI Expansion	US – Maryland	Active
DARPA QN	US – Massachu	Retired
Distributed Quantum Network by QUANT-NET	US – California	Active
Hybrid Quantum Architectures and Networks (HQAN) Networks	US – Illinois	Active

Quantum Encryption and Science Satellite (QEYSSat)	Canada, UK	Development
Quebec Quantum Communication Testbed	Canada – Quebec	Announced
Luxembourg Quantum Communication Infrastructure Laboratory (LUQCIA)	Luxembourg	Development
QuTech, Eurofiber and Juniper Networks Netherlands Network	Netherlands	Active
SEcure COmmunication Project – The SECOQC quantum key distribution network	Austria	Active
SwissQuantum quantum key distribution network	Switzerland	Retired
EuroQCI initiative: Inter-European Quantum Network	Italy, Slovenia,	Active
Quantum Internet Alliance	Europe	Active
OpenQKD Project	Europe	Active
Cambridge quantum network/ Metro Network	UK	Active
Bristol Quantum Network	UK	Active
The UK Quantum Network between Cambridge and Bristol (UKQN)	UK	Active
UKQN Extension (UKQNTel) Between Cambridge and BT labs	UK	Active
Quantum-Secured Network Across London	UK	Active
Twin Field QKD System	UK	Active
Mission 2 of the National Quantum Strategy	UK	Announced
Tokyo QKD Network	Japan	Active
Toshiba	Japan	Active
Singapore's National Quantum-Safe Network (NQSN)	Singapore	Active

AWS Testbed	Singapore	Active
National Quantum-Safe Network Plus (NQSN+)	Singapore	Announced
QuantumCity network in South Africa	South Africa	Active
Interuniversity Quantum Network in Moscow	Russia	Active
Quantum Computing-based Telecom Network Link in New Delhi	India	Active
Zhucheng- Huanshang QKD Link	China	Active
Quantum Network by University of Science and Technology of China	China	Active
Hefei metro network	China	Active
HCW Intercity Link	China	Active
Wuhu Metro Network	China	Active
Post-Quantum Cryptography on SK Telecom	Korea	Announced
Nation-wide QKD Network	Korea	Active
Rockabill Subsea Network	Ireland, UK	Experimental

12.Surviving the "quantum apocalypse" with fully homomorphic encryption

by Nigel Smart
https://www.helpnetsecurity.com/2024/03/19/quantum-apocalypse/

In the past few years, an increasing number of tech companies, organizations, and even governments have been working on one of the next big things in the tech world: successfully building quantum computers.

These actors see a lot of potential in the technology. Quantum computing spreads across a wide range of disciplines both on the hardware research and application development fronts, including elements of computer science, physics, and mathematics. The goal is to combine these subjects to create a com-

puter that utilizes quantum mechanics to solve complex problems faster than on classical computers.

Despite this description evoking images and scenarios fit for a sci-fi blockbuster, it is still hard to pinpoint what a quantum computer would do. Indeed, it seems that the only major application which people have identified is that of cryptanalysis.

Quantum computing has the potential to break cryptosystems that are the foundations of the technology protecting the privacy of data and information created and shared every day. When (and if) an applicable quantum computer is created, we will need to upgrade all our digital security protocols.

What is a quantum computer?

A traditional (digital) computer processes zeros and ones, so called bits. These, to a first order approximation, are represented as on/off electrical signals. A quantum computer, though, processes quantum states; these are units that can be thought of as being both zero and one at the same time. Such a state is called a quantum bit, or qubit.

If you hold n bits in a traditional computer then these *n* bits can represent any number between zero and *2^n-1*, but a single bit can only represent one number at a time. If you had n qubits, then the quantum computer can represent EVERY number between 0 and *2^n-1* simultaneously.

The physics of quantum phenomena is counter-intuitive. For example, two qubits can be "entangled" so that even though they can be separated by a large distance, an operation performed on one of the entangled qubits can have an instantaneous effect on the other qubit.

This is where the privacy concern around quantum computers comes from: they not only store data differently, but also process it differently, giving users a very different form of computational model. With this model, quantum computers could be faster than traditional ones with regards to a few known tasks: unluckily, the two main tasks which quantum computers are good at are factoring large numbers and solving so-called discrete logarithm problems. I say "unluckily," as it is precisely these two hard mathematical problems which lie at the base of all current security protocols on the internet.

The ability of a quantum system to solve these two mathematical problems will break the internet and all the systems we use day to day. The advent of a quantum computer and its effect on cybersecurity and data privacy is often dubbed the "quantum apocalypse".

Cryptography to the rescue

Thankfully, the advent of a suitably powerful quantum computer capable of breaking current cryptographic solutions does not yet seem to be on the horizon. But organizations and businesses that truly care about the privacy of their users and customers should start preparing for the worst by looking to integrate existing technologies and solutions in their operations and processes.

There are currently two distinct approaches to face an impending "quantum apocalypse". The first uses the physics of quantum mechanics itself and is called **Quantum Key Distribution (QKD)**. However, QKD only really solves the problem of key distribution, and it requires dedicated quantum connections between the parties. As such, it is not scalable to solve the problems of internet security; instead, it is most suited to private connections between two fixed government buildings. It is impossible to build internet-scale, end-to-end encrypted systems using QKD.

The second solution is to utilize classical cryptography but base it on mathematical problems for which we do not believe a quantum computer gives any advantage: this is the area of post-quantum cryptography (**PQC)**. PQC algorithms are designed to be essentially drop-in replacements for existing algo-

rithms, which would not require many changes in infrastructure or computing capabilities. NIST (the US standards institute) has recently announced standards for public key encryption and signatures which are post-quantum secure. These new standards are based on different mathematical problems, the most prominent of which is a form of noisy linear algebra, called the Learning-with-Errors problem (LWE).

The unbreakable power of FHE

NIST's standards only consider traditional forms of public key encryption and signatures. Fully homomorphic encryption (FHE) is different from traditional public key encryption in that it allows the processing of the data encrypted within the ciphertexts, without the need to decrypt the ciphertexts first.

As a first approximation, one can view traditional public key encryption as enabling efficient encryption of data in transit, whilst FHE offers efficient encryption of data during usage. Most importantly, with FHE nobody would be able to see your data but you because they wouldn't have your key.

All modern FHE encryption schemes are based on the LWE problem, thus FHE is already able to be post-quantum secure. So, if you deploy an FHE system today, then there is no need to worry about the future creation of a quantum computer.

13.Q Got Mail: Tuta Launches Post Quantum Cryptography For Email

by Matt Swayne
https://thequantuminsider.com/2024/03/18/q-got-mail-tuta-launches-post-quantum-cryptography-for-email/

Tuta reported it launched its latest security feature, **TutaCrypt**, a post-quantum encryption protocol designed to protect emails against potential quantum computer attacks, according to a company blog post. Tuta Mail reports that it is the first email provider globally to integrate quantum-safe algorithms alongside traditional algorithms such as AES and ECC, ensuring enhanced security for email communication.

Arne Möhle, CEO of Tuta Mail said in the post: "With TutaCrypt we are revolutionizing the security of email. For the first time, people can now send and receive emails that are encrypted so strongly that not even quantum computers will be able to break the encryption and decipher the messages. At Tuta, we see ourselves as pioneers in secure communication. Back in 2014, we published Tutanota, the first automatically encrypted email service. Today, ten years later and ten million users more, we are delighted to be paving the way for quantum-safe emails! We want to help as many people as possible communicate easily and securely – now and in the future. With the release of TutaCrypt in Tuta Mail, we have now reached another milestone to future-proof the security of online communication."

The introduction of TutaCrypt signifies a shift from the conventional asymmetric cryptography, RSA-2048, to a quantum-safe hybrid encryption protocol, according to the post. TutaCrypt employs a combination of CRYSTALS-Kyber, a post-quantum Key Encapsulation Mechanism, and an Elliptic-Curve-Diffie-Hellman key exchange (x25519) for encrypting emails, calendar sharing, sharing of contact lists and forthcoming file sharing services. This hybrid approach aims to fortify Tuta Mail's encryption against the potential for quantum computers to hack current encryption schemes.

Since its inception in March 2014, Tuta Mail, initially known as Tutanota, has provided end-to-end en-

crypted email services. The platform has undergone several security enhancements over the years, transitioning from AES 128 to AES 256 encryption, which already secures all at-rest encryption against quantum attacks. Furthermore, Tuta Mail upgraded its password-based key derivation function from bcrypt to Argon2, bolstering the security of passwords and encryption keys.

Addressing the challenges of securing email communication in the quantum computing era, Tuta Mail has responded to the need for quantum-resistant asymmetric encryption and public key cryptography. The National Institute of Standards and Technology (NIST) has recognized the urgency of this issue, selecting CRYSTALS-KYBER for standardization in key establishment and CRYSTALS-Dilithium for digital signatures, according to the post.

In addition to upgrading its cryptographic protocols, Tuta Mail reports it is collaborating with the University of Wuppertal on a research project funded by the German government. This project focuses on developing post-quantum secure drive and file sharing services, further extending Tuta Mail's commitment to quantum-resistant security solutions.

For users, enabling quantum-safe encryption requires no action other than updating to the latest version of the Tuta apps. This new protocol will be gradually introduced to all existing users, safeguarding their emails, calendars, and contact lists against both contemporary and future cryptographic threats. This initiative not only enhances the security of Tuta Mail's services but also sets a precedent in the ongoing effort to protect digital communication in the quantum computing age. The project's developments and implementations are available as open source, demonstrating Tuta Mail's commitment to transparency and collaboration in enhancing digital privacy and security.

14.The future for customer data security: post-quantum cryptography

https://www.santander.com/en/stories/the-future-for-customer-data-security-post-quantum-cryptography

More than 3 billion people will use internet banking this year safe in the knowledge that cryptography, highly complex algorithms that convert data into an unreadable format, will keep their personal and financial information safe. However, current encryption standards could soon become obsolete, and Santander is among the leaders of a global effort to push online security to a new level of sophistication.

The advent of quantum computers, with their ability to solve some problems too complex for classical ones, could result in systems powerful enough to defeat the current generation of cryptographic algorithms. The technology is still in its infancy, yet there is a need to anticipate the beginning of a new world.

Santander is at the forefront of international efforts to respond to this cryptography challenge and has established a Quantum Threat Group (QTG) to develop new ways of countering the challenges and protect its systems and customer data.

What is cryptography?

Cryptography is the guardian of every internet user's online experience. Algorithms ensure all digital information – every bank transaction completed, message sent, and online purchase made – is kept safe from unauthorized access, interception, or manipulation.

However, sensitive data it can protect today might become vulnerable in the future against the processing power available to quantum cyber hackers. Developing new protections for all parts of the digital world is key – and cannot be delayed. Post-quantum cryptography are systems that are secure against both quantum and classical computers.

Changing cryptographic algorithms is a complex task that has, historically, taken several decades. That is why governments and regulators are already establishing deadlines to secure a timely transition to quantum-safe cryptography.

Santander is working with several partners to help shape global standards to counter the threats and develop new security measures that are resistant to future quantum computer attacks while maintaining the security of traditional systems.

Working with US Cybersecurity Center of Excellence

Santander is collaborating with the National Cybersecurity Center of Excellence (NCCoE) of the US National Institute of Standards and Technology (NIST) on the Migration to Post-Quantum Cryptography project.

The goal is to raise awareness of the issues involved in the transition to post-quantum cryptography and develop best practices to ease the future migration tasks for organizations.

“With the advent of quantum computing and its potential to compromise many of the current cryptographic algorithms, it is critical that organizations begin to plan for many of the technological and operational challenges that a migration to post-quantum cryptography will present,” says William Newhouse, Cybersecurity Engineer & Project Lead at NIST NCCoE. “This project aims to help organizations in that effort.”

Santander's involvement in this initiative is acknowledgement of its commitment to digital security. “Our Quantum Threat Group is helping define detection tools and guidelines for quantum-vulnerable cryptographic algorithms,” says Daniel Cuthbert, Global Head of Cybersecurity Research at Santander.

Santander, GitHub and Microsoft alliance focused on the future

Santander is also working with GitHub, a platform at the forefront of software development and security, to tackle the challenges presented by the quantum cryptography world.

The companies, along with Microsoft, created CodeQL a powerful tool designed to assist developers in identifying vulnerabilities that could be exploited by hackers.

Santander was instrumental in developing a Cryptography Bill of Materials, called Cryptobom-Forge, which leverages GitHub's CodeQL output and enables developers to dissect and understand the components of their software. This gives them an unprecedented level of insight into their vulnerability to quantum attack.

Santander is involved in other collaborations with the World Economic Forum and the Spanish chapter of the European Quantum Communications Infrastructure project. It is also part of the Caramuel project, a consortium of Spanish companies led by Hispasat aiming at providing quantum-based secure communications supported by a geostationary satellite.

While the arrival of these next-generation super computers poses a challenge to the security of digital communications, the standardization of new quantum-safe cryptography will guard sensitive informa-

tion.

Crucially, it will allow people to continue navigating the Internet securely and help banks protect their customers' personal data and financial information.

15.Post-Quantum Cryptography: Six French Cyber Players Join Forces To Design The Secure Communication Networks Of Tomorrow

https://www.thalesgroup.com/en/worldwide/security/press_release/post-quantum-cryptography-six-french-cyber-players-join-forces

The RESQUE consortium brings together six French companies and organisations with complementary roles in the cybersecurity field: technology leader **Thales**, the consortium's coordinator; **TheGreenBow**, an SME dedicated to software development for secure communication systems; **CryptoExperts**, an SME specialising in cryptography; the start-up **CryptoNext Security**; the French information system security agency **ANSSI**; and **Inria**, the French national research institute for digital science and technology, which also represents six academic institutions, namely the University of Rennes, ENS (École Normale Supérieure) Rennes, the French national scientific research centre (CNRS), ENS Paris-Saclay, Université Paris-Saclay and Université Paris-Panthéon-Assas.

Over the next three years, the RESQUE project (RÉSilience QUantiquE or quantum resilience) will work to develop a post-quantum cryptography solution capable of protecting the communications, infrastructure and networks of businesses and local governments against future attacks carried out using quantum computers. With their vastly increased computing power, quantum processors could break the encryption algorithms that are widely used today, potentially compromising the security of the most sensitive data and representing a threat to national sovereign interests.

The project is funded by the French government as part of the France 2030 investment plan and by the European Union's Next Generation EU scheme under the France Relance recovery programme, with €6 million of additional financing from Bpifrance. It will focus on two key use cases:

- A hybrid post-quantum virtual private network (VPN) to provide simple, safe and quantum-resistant user access to information systems;
- A high-performance post-quantum hardware security module (HSM) to secure whole systems and for integration with other products.

Within the consortium, TheGreenBow's expertise in VPN and software development will complement the capabilities of CryptoExperts and CryptoNext Security in encryption and both standard and advanced algorithmic cryptography, with Thales providing leadership in algorithm integration and a holistic vision of the applications ecosystem. ANSSI (a non-financed project partner) will provide a research framework and assess the validity criteria for the use cases, and all partners will benefit from Inria's fundamental research into post-quantum cryptography.

16.Are private conversations truly private? A cybersecurity expert explains how end-to-end encryption protects you

by Robin Chataut
https://theconversation.com/are-private-conversations-truly-private-a-cybersecurity-expert-explains-how-end-to-end-encryption-protects-you-224477

Imagine opening your front door wide and inviting the world to listen in on your most private conversations. Unthinkable, right? Yet, in the digital realm, people inadvertently leave doors ajar, potentially allowing hackers, tech companies, service providers and security agencies to peek into their private communications.

Much depends on the applications you use and the encryption standards the apps uphold. End-to-end encryption is a digital safeguard for online interactions. It's used by many of the more popular messaging apps. Understanding end-to-end encryption is crucial for maintaining privacy in people's increasingly digital lives.

While end-to-end encryption effectively secures messages, it is not foolproof against all cyberthreats and requires users to actively manage their privacy settings. As a cybersecurity researcher, I believe that continuous advancements in encryption are necessary to safeguard private communications as the digital privacy landscape evolves.

How end-to-end encryption works

When you send a message via an app using end-to-end encryption, your app acts as a cryptographer and encodes your message with a cryptographic key. This process transforms your message into a cipher – a jumble of seemingly random characters that conceal the true essence of your message.

This ensures that the message remains a private exchange between you and your recipient, safeguarded against unauthorized access, whether from hackers, service providers or surveillance agencies. Should any eavesdroppers intercept it, they would see only gibberish and would not be able to decipher the message without the decryption key.

When the message reaches its destination, the recipient's app uses the corresponding decryption key to unlock the message. This decryption key, securely stored on the recipient's device, is the only key capable of deciphering the message, translating the encrypted text back into readable format.

This form of encryption is called public key, or asymmetric, cryptography. Each party who communicates using this form of encryption has two encryption keys, one public and one private. You share your public key with whoever wants to communicate securely with you, and they use it to encrypt their messages to you. But that key can't be used to decrypt their messages. Only your private key, which you do not share with anyone, can do that.

In practice, you don't have to think about sharing keys. Messaging apps that use end-to-end encryption handle that behind the scenes. You and the party you are communicating securely with just have to use the same app.

Who has end-to-end encryption

End-to-end encryption is used by major messaging apps and services to safeguard users' privacy.

Apple's iMessage integrates end-to-end encryption for messages exchanged between iMessage users, safeguarding them from external access. However, messages sent to or received from non-iMessage users such as SMS texts to or from Android phones do not benefit from this level of encryption.

Google has begun rolling out end-to-end encryption for Google Messages, the default messaging app on many Android devices. The company is aiming to modernize traditional SMS with more advanced features, including better privacy. However, this encryption is currently limited to one-on-one chats.

Facebook Messenger also offers end-to-end encryption, but it is not enabled by default. Users need to start a "Secret Conversation" to encrypt their messages end to end. End-to-end encrypted chats are currently available only in the Messenger app on iOS and Android, not on Facebook chat or messenger.-com.

WhatsApp stands out for its robust privacy features, implementing end-to-end encryption by default for all forms of communication within the app.

Signal, often heralded by cybersecurity experts as the gold standard for secure communication, offers end-to-end encryption across all its messaging and calling features by default. Signal's commitment to privacy is reinforced by its open-source protocol, which allows independent experts to verify its security.

Telegram offers a nuanced approach to privacy. While it provides strong encryption, its standard chats do not use end-to-end encryption. For that, users must initiate "Secret Chats."

It's essential to not only understand the privacy features offered by these platforms but also to manage their settings to ensure the highest level of security each app offers. With varying levels of protection across services, the responsibility often falls on the user to choose messaging apps wisely and to opt for those that provide end-to-end encryption by default.

Is end-to-end encryption effective?

The effectiveness of end-to-end encryption in safeguarding privacy is a subject of much debate. While it significantly enhances security, no system is entirely foolproof. Skilled hackers with sufficient resources, especially those backed by security agencies, can sometimes find ways around it.

Additionally, end-to-end encryption does not protect against threats posed by hacked devices or phishing attacks, which can compromise the security of communications.

The coming era of quantum computing poses a potential risk to end-to-end encryption, because quantum computers could theoretically break current encryption methods, highlighting the need for continuous advancements in encryption technology.

Nevertheless, for the average user, end-to-end encryption offers a robust defense against most forms of digital eavesdropping and cyberthreats. As you navigate the evolving landscape of digital privacy, the question remains: What steps should you take next to ensure the continued protection of your private conversations in an increasingly interconnected world?

17.Google's Threat Model for Post-Quantum Cryptography

by Sophie Schmieg, Stefan Kölbl, and Guillaume Endignoux
https://bughunters.google.com/blog/5108747984306176/google-s-threat-model-for-post-quantum-cryptography

If we do not encrypt our data with a quantum-secure algorithm right now, an attacker who is able to store current communication will be able to decrypt it in as soon as a decade. This store-now-decrypt-later attack is the main motivator behind the current adoption of post-quantum cryptography (PQC), but other future quantum computing threats also require a well-thought out plan for migrating our current, classical cryptographic algorithms to PQC.

This is the first of a series of blog posts in the Bug Hunters blog, dedicated to the topic of PQC, where we in Google's Cryptography team share our latest thoughts and reasons about the PQC migration, starting with the threat model we are working with.

Given the long timelines, our stances may evolve over time, with this blog post reflecting our understanding at the beginning of 2024.

Prioritization Considerations

The main considerations for prioritizing quantum threats that we will explore more deeply in this post are:

- Feasibility of the quantum attack in question.
- Existence of store-now-decrypt-later attacks.
- Use cases that require fixed public keys with decades of lifetime.
- Need for exploratory research on systems that might require substantial redesign to work with post-quantum algorithms, especially where wider industry collaboration is required.

Background

Quantum computers threaten cryptography mainly through two algorithms: Shor's algorithm for factoring integers and solving discrete logarithms and Grover's search, which can invert a black-box function. As mentioned, a major consideration for prioritization is whether a system **today** is already at risk if an adversary will get access to a quantum computer in the **future**. Storing ciphertexts now and decrypting them later is a prime example for this, requiring a PQC deployment well before the advent of quantum computers.

Based on this we can roughly group cryptography into four different technologies:

- **Asymmetric encryption and key agreement**, using a private/public key pair to establish a key that can then be used for symmetric cryptography. Impacted by Shor's algorithm, and vulnerable to store-now-decrypt-later attacks.

- **Digital signatures**, using a private/public key pair to authenticate data and provide non-repudiation. Impacted by Shor's algorithm, but not vulnerable to store-now-decrypt-later attacks.

- **"Fancy" cryptography**: This category depends on the specific algorithm and use case, but many

privacy preserving techniques (e.g. blind signatures, ORPF, …), will be impacted by Shor's algorithm, and are partially vulnerable to store-now-decrypt-later. Many of these techniques require further research. We recommend a careful assessment of the impact of quantum threats on these schemes.

- **Symmetric cryptography**, using a single secret key to encrypt and authenticate data: In our current understanding, symmetric cryptography is not impacted by quantum computers for all practical purposes. Grover's algorithm could be used as an attack here, but is currently considered infeasible for even medium-term quantum computers. (See "Reassessing Grover's Algorithm, 2017")

Algorithms

Thankfully, NIST has been working on standardizing new, quantum-safe algorithms that will address asymmetric encryption and key agreement, as well as digital signatures. As a quick overview, the algorithms look as follows, for our chosen security level.

Algorithm	Type	Public Key Size	Ciphertext/ Signature Size
ECDH (classical algorithm)	Key Agreement	32 bytes	32 bytes
ECDSA (classical algorithm)	Digital Signature	32 bytes	64 bytes
Kyber-768/ML-KEM-768	Key Agreement	1184 bytes	1088 bytes
Dilithium3/ML-DSA-65	Digital Signature	1952 bytes	3309 bytes
SPHINCS+-128s/SLH-DSA-128s	Digital Signature	32 bytes	7856 bytes

NIST is planning to release more standards (see here and here), both for key agreement and signatures in order to have schemes based on a wider set of mathematical assumptions and allowing different trade-offs between public key size and ciphertext/signature size. Note that any such future standards will take multiple years to be finalized.

Hybrid deployment

While the currently proposed PQC algorithms have received a lot of cryptanalysis over the last decade, they are still somewhat less mature than classical cryptography, and our recommendation is to use them in a hybrid fashion, which requires an attacker to break both the classical and the post-quantum algorithm. There are some caveats on this topic that we will explore in a future blog post.

Use Cases

Classical Cryptography is pervasively used in modern software and infrastructure. Post-quantum cryptography will impact many existing deployments. With the information from the *Background* section

above in mind, the following use cases are primary concerns and each comes with its own difficulties. While we give our recommendations for the different use cases, please note that standards are still being developed and will be the more definitive guidance for which algorithms to use.

Encryption in Transit

Encryption in transit primarily includes TLS, SSH, secure messaging (like Signal, which is used in RCS, and MLS), and, for Google, ALTS. The main threat here is store-now-decrypt-later. As such, deployment of PQC key encapsulation schemes like Kyber (ML-KEM, FIPS 203) is urgent. In order to mitigate this threat, we only need to add an ephemeral PQC key to the initial key agreement. Long-term PQC keys (e.g. public or private CAs) fall under Public Key Infrastructure and will require community consensus before meaningful deployments can happen.

The good news with encryption in transit is that there are a limited number of stacks. Most relevant to Google are, as mentioned above, TLS, SSH, Signal, and ALTS, which at the time of writing all have started to roll out PQC algorithms. The ephemeral nature of the keys needed for encryption in transit further works in our favor, making this use case, while the most urgent, also the comparatively easiest for both technical and social reasons.

Our current recommendation for encryption in transit is to use Kyber768 for key agreement in hybrid with X25519 or P256.

Firmware Signatures

Firmware signatures are used to secure the root of the secure boot trust chain. The public key for these signatures usually has to be burned into silicon or is otherwise protected from being changed and tampered with. This makes changing the signature scheme for this use case impossible in most cases. For devices with a decade or longer lifespan, we end up in a similar situation as with store-now-decrypt-later attacks, where we need to implement the quantum-safe algorithms now, since we will not be able to change them at a later date. This is further complicated by the long production timelines often involved with hardware implementations of cryptographic algorithms.

Our current recommendation for firmware signature is to use the stateless hash-based signature scheme SPHINCS+ (FIPS 205, SLH-DSA)

Software Signatures

Software signatures are similar to firmware signatures and are needed to guarantee secure boot and make deployments resistant to tampering with binaries and source code. Unlike firmware signatures, the public key for software signature can usually be updated and rely on the lower level signatures for authenticity. On top of that, both binaries and source code are usually fairly large, and both signing and verification are not particularly resource constrained. This gives this use case the most flexibility and a relatively relaxed timeline.

This use case is seeing a lot of development, and even though the timeline is relatively relaxed, it might make sense to already include PQ signatures in the standards that are currently being written.

Our current recommendation is to use either Dilithium3 (FIPS 204, ML-DSA) in hybrid with ECDSA/EdDSA/RSA, or SPHINCS+ (FIPS 205, SLH-DSA) for this use case.

Public Key Infrastructure

Public key infrastructure is the infrastructure used to provide authenticity for encryption in transit, as well

as reliable identities for machines and people.

PKI usually relies on chains of certificates, i.e. public keys with an attached signature verifiable by a key higher in the chain. This makes PKI in its current form extremely susceptible to size increases from post-quantum schemes. A single Dilithium3 signature + public key is larger than 5kB, making any PKI deployment with intermediaries very expensive. For the Web PKI in particular, we know some devices start failing when packets grow beyond 10 - 30 kB. This problem might be fixable, but a severe performance penalty remains in any case.

There are several alternatives to simply replacing classical signatures with quantum-safe signatures, which could address the performance issues when it comes to PKI. We are currently looking to experiment in this space to gather data for more solid recommendations, which we will share in a future blog post.

Tokens

Another widespread use of digital signatures is stateless asymmetric tokens, such as JSON Web Tokens (JWT). Tokens that use symmetric cryptography, or that use stateful techniques as a defense-in-depth measure are not affected by quantum threats. For asymmetric tokens, the main difficulty is the size constraints that they often come with. For example, a token that is supposed to be saved as a cookie has an upper limit of 4096 bytes available for the entire token. A Dilithium3 signature would take up 3309 of those bytes, if encoded in binary, and at 4412 bytes would not fit with this requirement when base64 encoded.

Stateless tokens come with independent security concerns, and moving towards stateful tokens is prudent just to ensure more robust systems. Some of the schemes in the second onramp of the NIST competition have very small signatures, but large public keys; this approach could be another tool to address this use case.

Our main recommendation is to use stateful tokens where possible, given their additional security benefits. Additionally, we want to experiment in this space to gather data for more solid recommendations.

Other

There are some other use cases that do not fit into any of these categories. For example, in some cases, documents have to be encrypted asymmetrically; separately from encryption in transit. This use case mainly includes emails encrypted and signed via S/MIME, but also various protocols using HPKE or PGP, or using digital signatures directly.

Another one of the more important asymmetric encryption protocols is key import for HSMs.

These use cases are less sensitive to ciphertext size, so using Kyber (FIPS 203/ML-KEM) in hybrid with ECDH/X25519 should not pose many challenges. For S/MIME in particular, additional difficulties might arise from the multi recipient setting.

Another use case that is related to, but not equal to the HSMs discussed above are hardware roots of trust such as security keys or TPMs, which face their own difficulties regarding their hardware constraints.

Privacy preserving and other fancier schemes will require additional research to safely deploy. We plan to give an overview and a call to action in a future blog post.

Threat actors and Timelines

Both lack of quantum-safe confidentiality and lack of quantum-safe authenticity can be exploited by threat actors. While the threats to confidentiality are more direct, the threats to authenticity are often far more wide-reaching and devastating.

Threat Actors

Nation States

Nation states are the most likely to first arrive at a cryptographically relevant quantum computer. They will most likely try to deploy the quantum computer in a deniable fashion, in order to avoid tipping off adversaries of their capabilities. Nation states are most likely to target the Cloud deployments of other nation state customers, and may target political dissidents and other targets for surveillance. Nation states might also target Google or other infrastructure providers for military or economic reasons.

While building a cryptographically relevant quantum computer is hard, once the machine is built, it should not be very expensive to break any given public key. Given the ephemeral nature of encryption in transit keys, the most likely first targets would be more static keys as required for e.g. PKI, as well as breaking stored communication that is considered of high interest. As quantum computers get cheaper, they might target wider and wider sets of victims.

Some have raised concerns that nation states might try to backdoor or weaken the algorithms NIST releases, as has been done in the past in the case of Dual_EC_DRBG. To preempt such concerns, the NIST standards were designed in a public competition. In addition, if most deployments are in a hybrid fashion, being able to break the PQC algorithm by itself would not help until a quantum computer is available, giving the public several years to discover any potential backdoors.

Insider Threats

Google and other companies are working to build a quantum computer, which eventually might become cryptographically relevant. As with other prized technologies, insider threats remain a vector. To that end, companies will need to take necessary precautions to protect their crown jewels to avoid theft or exploitation by a nation state threat and other motivated attackers.

Ransomware and other financially motivated threat actors

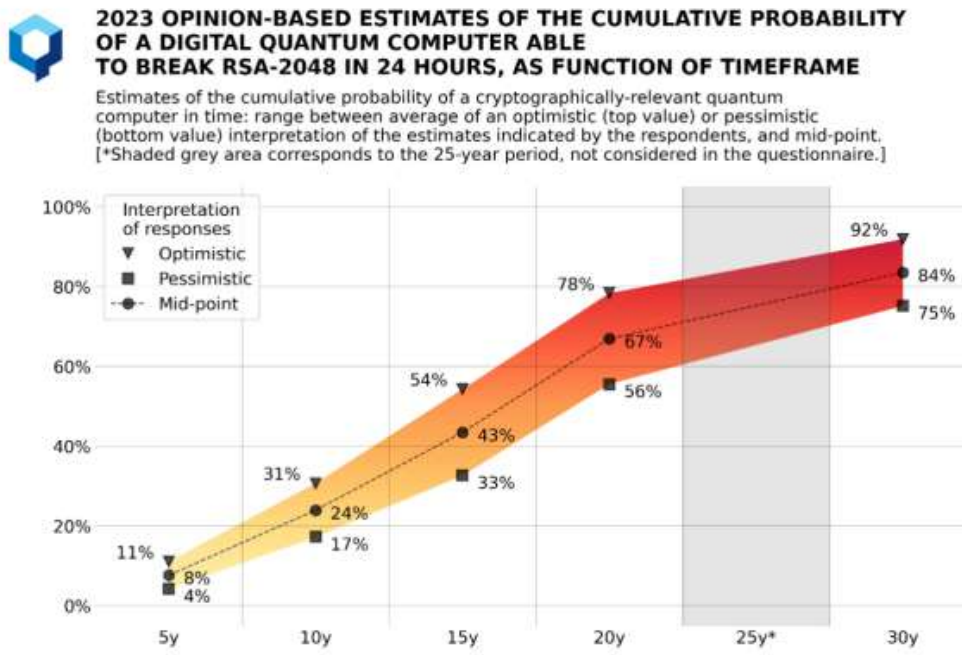
For financially motivated threat actors, the main consideration will be the availability of quantum computers. If use cases for quantum computers remain limited, access to them might be too difficult for a financially motivated threat actor to obtain. If they are available for relatively cheap prices, either directly, or via Cloud deployments, we are likely to see them used to extract ransoms, or commit industrial espionage, by exploiting areas that have not migrated to quantum-safe protocols.

Regulatory Landscape

PQC has become a hot topic with various executive orders in the US, requiring the US government to work towards deploying quantum-safe cryptography. Regulatory frameworks such as CNSA 2.0 outright require the use of PQC on fairly short timelines, with other compliance frameworks such as FIPS being soon to follow. Beyond the US, BSI and ANSSI have also been active in this space and have been starting to ask for PQC roadmaps for longer term deployments.

Timelines

The best aggregate timeline estimates for the risk from quantum computers we have can be summed up in this graphic by the global risk institute.



Based on this timeline, and corroborated by Google's quantum computing team, Google Quantum AI, the main risk for a cryptographically relevant quantum computer is within a ten to 15 year timeframe. We expect significant improvements in the field by 2030, which should serve as a good midpoint check on the timeline.

Conclusion

Despite the long timelines until the prevalence of cryptographically relevant quantum computers can be expected, we hope that the overview given in this blog post will help you understand which areas are most at risk, and where you should start focusing your attention at the present time.

18.The S in IoT stands for security. You'll never secure all the Things

by Steven J. Vaughan-Nichols
https://www.theregister.com/2024/03/09/opinion_column_security_sjvn/

I was one of the first people to use an Internet of Things (IoT) device. It was Carnegie-Mellon's Computer

Science Department's Coke machine[1]. True, I didn't need to check on it since my school, West Virginia University, was 77 miles from CMU, but I thought it was really cool back in the day is that I could see what was what with the coke machine over the Internet. That was then. This is now. Today. I'm less than thrilled by the IoT.

You see, while it wasn't true that smart toothbrushes were behind a reported Distributed Denial of Service (DDoS) attack, they could have been. More to the point, some DDoS attacks already start from the gadgets on your wrist, in your pocket, and scattered around your home.

For example, last year, Nokia noted in its 2023 Nokia Threat Intelligence Report that IoT botnet DDoS attacks increased fivefold from 2022 to 2023. Indeed, more than 40 percent of all DDoS traffic today comes from IoT botnets.

We should have seen this coming. The first significant IoT botnet DDoS attacks, which used the Lizard-Stresser DDoS tool, wrecked the 2015 holiday season for many Xbox Live users when it knocked the service offline for days during the peak Christmas season. In 2016, LizardStresser hackers followed up with a 400Gbps attack backed by more than 1,200 video cameras.

It's only got worse since then. A lot worse. You might not think that small gadgets like smart lightbulbs, thermostats, and, yes, toothbrushes, could do that much damage, and you'd be right. Individually, they don't count for much. But, when you coordinate some of the more than 5 trillion - that's trillion with a T - IoT devices, it's another story entirely.

So, why is IoT security that bad? Let me count the ways.

First, IoT devices tend not to have operating systems as such, but rather firmware that also acts as an operating system. In short, any security problems in the firmware are easily accessible to a would-be attacker. Additionally, far too often, firmware hasn't been as security-hardened as operating systems.

In fact, way too many "smart" devices are using old, dumb software with known security problems. As the FBI noted in 2022, many medical IoT devices run outdated, insecure software.

How many? According to Armis, a security company, 39 percent of nurse call systems have critical, unpatched common vulnerabilities and exposures (CVEs). Oh, and infusion pumps, which provide fluids to patients? 30 percent of them have unpatched CVEs.

Would it surprise you to know that 19 percent of medical IoT units run on no longer supported versions of Windows? I didn't think so. I'd rather not go to the hospital anyway, but knowing that some of the equipment my life may depend on is unsafe? No, just no.

Making IoT attacks even easier, junkier IoT devices don't use secure networking. Insecure networks are also especially vulnerable to man-in-the-middle (MITM) attacks. That makes stealing credentials mindlessly simple.

All this stems from the simple fact that IoT security is an afterthought

A more obvious but all too common problem is that many IoT devices come with weak default pass-

[1] Yep, Carnegie-Mellon's Computer Science Department already had an internet-connected Coke machine back in 1992, and from the '70s, you could keep tabs on it from the university's server (
EMPTY EMPTY 1h 3m COLD COLD 1h 4m
).

words or, worse still, shared hardcoded passwords. Yes, it makes it easier for Joe public to set the gadget up, but it's also an open invitation for any hacker to enlist your device in a botnet.

Of course, these vulnerabilities could be fixed… if IoT manufacturers gave a damn about security. Many don't. Many don't update their firmware at all.

To them, your security is a cost. You bought the gadget, it's your problem now.

What can you do about it? Not a lot, to be honest. So, I prefer never to buy any "smart" device. You see, there is no "S" for security in IoT. Never has been, and I doubt very much there ever will be.

You can only buy from vendors that prioritize security. Finding out which ones do that can be almost impossible, as they don't make it easy to find.

I can say one thing, though: If an IoT device runs Windows, just say no. Windows is hard enough to secure in a computer; in standalone hardware, it's almost impossible. The simple fact that medical devices, of all the things you'd want to really secure, frequently run obsolete versions of Windows says everything I need about how seriously their manufacturers take security.

It all comes down to the bottom line. What truly matters to the many who make IoT devices is the M for money. They couldn't care less about securing software, especially keeping it patched and secure after it's in your hands. You're much safer with dumb devices than you ever will be with smart ones.

19.HP introduces business PCs with quantum-resistant security chips

by Nancy Liu
https://www.sdxcentral.com/articles/news/hp-introduces-business-pcs-with-quantum-resistant-security-chips/2024/03/

HP introduced its new business PCs equipped with quantum-resistant chips at the company's annual Partner Conference 2024. The company built its upgraded Endpoint Security Controller (ESC) chip into select PCs to protect firmware against potential quantum computer attacks.

The potential introduction of cryptographically relevant quantum computers has been a growing concern for cybersecurity experts. According to recent research, 27% of experts predict a 50% likelihood of a cryptographically relevant quantum computer emerging by 2033, challenging the security of existing digital signatures on firmware and software and dissolving digital trust.

Government and industry are making progress in moving the digital world to a new cryptographic standard. For example, the U.S. government has outlined specific recommendations around migrating to quantum-resistant cryptographic algorithms for firmware signing, recommending that post-quantum cryptography (PQC) be used from 2025. The National Institute of Standards and Technology (NIST) is expected to release the PQC standard this year.

However, "while software can be updated, hardware can't. And that includes some of the cryptography that protects PC firmware," HP warns. "With no cryptographic protections in place, no device would be safe – attackers could access and modify the underlying firmware and gain total control."

Introducing 5th generation ESC chip

In response to these challenges, HP launched its 5th generation ESC chip. This upgraded chip is designed to protect PC firmware integrity with quantum-resistant cryptography and provide a foundation for software PQC upgrades on PCs in the future, the company claims.

"The ESC is a chip that implements HP's platform root of trust, designed to protect platform firmware integrity and provide a range of other security capabilities," Boris Balacheff, chief technologist for system security research and innovation at HP Inc., told SDxCentral.

The ESC chips are isolated from the CPU and operating systems, which offers a hardware platform root of trust designed to reduce risks of breaches and improve productivity by preventing downtime, Balacheff explained. "The ESC firmware signatures, including those using new quantum-resistant cryptographic algorithms, are validated by the hardware before the firmware can run. Thus, a quantum computer attacker cannot defeat the signature protection to run modified firmware."

HP's upgraded ESC chips use quantum-resistant cryptography

The upgraded ESC chips do not use quantum technology itself, but quantum-resistant cryptography instead, according to Balacheff. The chips have adopted the standardized quantum-resistant Leighton-Micali Signature algorithm to protect firmware integrity by verifying a digital signature.

This is in addition to the RSA cryptography already in hardware in previous chip generations, resulting in two parallel digital signature mechanisms being used to protect the integrity of HP PC firmware.

This move ensures HP maintains the hardware maturity and Federal Information Processing Standards (FIPS)-certified protection provided by the RSA (Rivest-Shamir-Adleman) public-key cryptosystem, while offering security against "a future attacker equipped with a sufficiently powerful quantum computer to break classical asymmetric cryptography like RSA," Balacheff explained.

"This will prevent that platform firmware [from being] maliciously modified, helping protect the rest of the PC software, security functionality and sensitive data – both now and in the future," he added.

Building the foundation to support software PQC updates

The quantum-resistant chips also established a hardware foundation to support the PQC migration strategy and ensure the migration can be treated as a software update problem, Balacheff said.

Then, "customers will be able to plan, according to their own use-case priorities and timeline, working with software vendors who are themselves planning migration to post-quantum cryptography," he added.

"Without the innovation introduced by HP this year, customers would have to plan a full hardware change in order to implement a migration to post-quantum cryptography, since a software update alone would remain undermined by risks to their PC firmware, which could lead to compromise of the whole device software and data if an attacker becomes equipped with a sufficiently powerful quantum computer," Balacheff said.

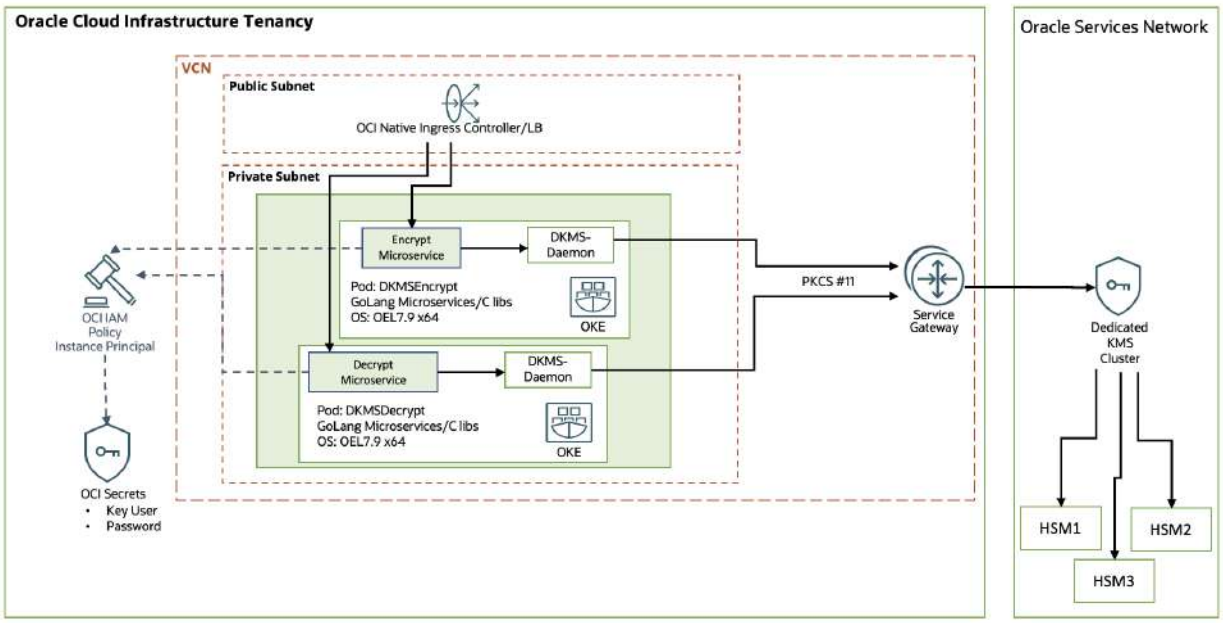
20.Building scalable cryptographic applications using OCI Dedicated Key Management Service (DKMS)

by Ty Stahl
https://blogs.oracle.com/ateam/post/building-a-cryptographic-application-using-oci-dedicated-key-management-service-dkms

Every journey to the cloud has moments when you need to look across your entire application portfolio and answer a simple question – "can I do that in the cloud?" For the majority of those moments, the answer is an unequivocable – yes. Additionally, you are able to capitalize on a series of added benefits such as modernized cloud-native solutions, performance improvements, and built-in management tools. However, there can be that one bespoke application or service in your architecture that does something "special" – say, for example - it performs cryptographic operations against a dedicated FIPS 140-2 Level 3 device? Oh, and did I mention - it has to be extremely fast, as well?

Fortunately if you have found yourself in that very situation, then this blog is going to be for you. The past year has been very active for the OCI Key Management and Encryption services portfolio; more specifically about what I will cover today - is the realease of the OCI Dedicated Key Managed Serviced(DKMS).

The reference use case that I will demonstrate is focused on showing a secure architecture while running a scalable microservice deployment for simple cryptographic, high-volume transactions with DKMS. In this case, I simply built two RESTful microservices – encryption and decryption of a string passed in via a HTTP header. Nothing incredibly flashy; keep in mind – this is a blog about cryptography.



Architecture

I chose to build this application to run in an Oracle Kubernetes Engine(OKE) cluster for a few reasons. First, I wanted to leverage a few of the features of running this application at-scale. To do that, I needed to build the container images by installing the DKMS daemon – which is crucial for programmatically interfacing using PKCS#11. I also wanted to test out the OKE Native Ingress Controller to handle the URL path-driven traffic being directed appropriately to the 2 backend microservices.

Components:

- **DKMS Cluster** – this is the HSM cluster deployed that can only be accessed from the Oracle Services Network though a Service Gateway. First you will need to provision DKMS cluster, if you do not have one already - follow this documentation.
- **Oracle Kubernetes Engine (OKE)** – I used a custom created OKE cluster using the OCI workflow which created a private subnet where the worker nodes will reside and have access to the Service Gateway. It also created a public subnet so that I can access my web services via the internet
- **OKE Native Ingress Controller** – Using this blog, I was able to create an ingress with a single OCI Load Balancer which attaches certificates to the listeners from the OCI Certificates Services
- **DKMS Client** – Within the OKE pods, I needed to install the DKMS client which is used by the application to communicate via PKCS#11 to the DKMS service. I installed the DKMS client RPMS while building the container image using the docker file.
- **OCI Secrets in Vault** – Since the DKMS is basically network attached hardware, the authentication mechanisms rely on a combination of mTLS for channel authentication -and Username/Password for application users. Application users are further referred to as CryptoUser(CU). Secure programming principles state that I need to store these sensitive credentials as a protected secrets. From there, I can authorize my applications/pods to have access the credentials to use for authentication to the DKMS cluster controlled via IAM Policy.

One last component not depicted is the management client interface, which I actually had installed on an OCI compute instance separately.

Setup and Microservice Creation

The setup for this application was pretty simple. First thing that I need to do is to setup the DKMS cluster using the client utilities that come with the DKMS services. To do that, I used the following to create my CU:

```
Command:  loginHSM -u CU -s crypto_user
Enter password:
KeyMgmtUtilsLoginHSM returned: 0x00 : HSM Return: SUCCESS
Cluster Status:

Node id 0 status: 0x00000000 : HSM Return: SUCCESS
Node id 1 status: 0x00000000 : HSM Return: SUCCESS
Node id 2 status: 0x00000000 : HSM Return: SUCCESS
```

Reference the DKMS documentation for User Account Management to learn more about the different types of users for DKMS and how to manage them. You will create a CryptoUser - which is the application account that will be used from the microservice to connect to the HSM.

Now, you can login as the newly created CU and create the first key using the following steps for the - 'crypto_user':

Reference the DKMS documentation for the Key Management Utility which explains how manage the various key operations and cryptographic options. For this demo, I just simply used an AES 32-bit Symmetric key.

```
Command:  genSymKey -l oci-key -t 31 -s 32
       KeyMgmtUtilGenerateSymmetricKey returned: 0x00 : HSM Return: SUCCESS
       Symmetric Key Created.  Key Handle: 129
       Cluster Status:
       Node id 0 status: 0x00000000 : HSM Return: SUCCESS
```

You need to make a note of the Key Handle - that is how you will refer the application to what key to encrypt the plaintext. Subsequently, to successfully decrypt the cipher text - you must use the same key handle to get the correct plaintext back.

Next, you will need to build you application which is going to use the PKCS#11 interfaces to work with DKMS. For that, I chose to use a combination of native languages- GOLang and C - to create the sample microservice. Since I am building a RESTful HTTP service, I need to ensure I am able to pass around friendly HTTP characters. For that, I built-in some base64 encoding/decoding to ensure I can safely pass parameters.

```
1   FROM oraclelinux:7-slim as build-stage
2   WORKDIR /function
3
4   ADD  startDaemon.sh  /function/
5   ADD  HSMfiles.zip  /function/
6   ADD  src/dkms-go-example/* /function/
7
8   FROM oraclelinux:7-slim
9   WORKDIR /function
10  COPY --from=build-stage /function /function
11
12  RUN yum -y install libedit.x86_64
13  RUN yum -y install unzip.x86_64
14  RUN yum -y install sudo.x86_64
15  RUN yum -y install oracle-golang-release-el7.x86_64
16  RUN yum -y install golang-1.19-1.0.1.el7.x86_64
17
18  RUN yum -y install oci-hsm-client
19  RUN yum -y install oci-hsm-pkcs11
20
21  RUN cd /function/
22
23  RUN unzip HSMfiles.zip
24  RUN cp -rf /function/hsm_bkup/data/ /opt/oci/hsm/
25  RUN ls -al /opt/oci/hsm/data/certs/
26
27  RUN cp -rf libencrypt.so /usr/lib64/
28  RUN cp -rf /function/startDaemon.sh /opt/oci/hsm/bin/
29
30  EXPOSE 8080
31
32  ENTRYPOINT sudo /opt/oci/hsm/bin/startDaemon.sh && nohup go run main.go && sleep infinity
```

Once we have the microservice working locally, I need to package it up into a a container so that I can deploy it to my OKE cluster. To build the container, I used the following example docker file to create the

image for upload to the repository. The key part that I wanted to show was the installation of the DKMS client and PKCS#11 daemon within the container. This ensures that the application can find load the shared libraries when the microservice is started.
Once the image has successfully been built, the last thing to do is simply deploy it onto OKE cluster. As a reminder, I am using the OCI Native Ingress Controller to achieve this deployment model. As you can see in the following snippet, I have registered 2 services - one for encrypt and one for decrypt which will route based off of the URL paths.

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: native-ic-lb
  annotations:
     oci-native-ingress.oraclecloud.com/certificate-ocid: ocid1.certificate.oc1.iad.xxxxxx
     oci-native-ingress.oraclecloud.com/protocol: HTTP2
     oci-native-ingress.oraclecloud.com/policy: "ROUND_ROBIN"
     oci-native-ingress.oraclecloud.com/healthcheck-protocol: "TCP"
     oci-native-ingress.oraclecloud.com/healthcheck-port: "8080"
     oci-native-ingress.oraclecloud.com/healthcheck-interval-milliseconds: "10000"
     oci-native-ingress.oraclecloud.com/healthcheck-timeout-milliseconds: "3000"
     oci-native-ingress.oraclecloud.com/healthcheck-retries: "3"
spec:
  rules:
  - host: app1.xxxxx.com
    http:
      paths:
      - pathType: Prefix
        path: "/encrypt"
        backend:
          service:
            name: dkmsapplbencrypt
            port:
              number: 443
      - pathType: Prefix
        path: "/decrypt"
        backend:
          service:
            name: dkmsapplbdecrypt
            port:
              number: 443
  defaultBackend:
    service:
      name: httpd-service-nautilus
      port:
        number: 443
~
```

The last step is to ensure that we have the credentials stored in the OCI Vault. As I mentioned before, the application will need to use the CU username and password in order to issue PKCS#11 operations to the HSM. Fortunately, this is easy through the help of the OCI SDK - and there are several blogs that refer how to achieve this. As an example, I will refer the following blog because it shows the setup of both the Secret and the OCI IAM Instance Principal policy.

Note: Since this OKE cluster is only a demo designed to showcase the value of DKMS - all services in my cluster can access the OCI Vault Secret. Therefore, the use of Instance Principal is a shortcut. However, if your OKE clusters have a variety of services running - you may only want to restrict Secret retrieval to those who actually need it. To solve that problem, take a look into OKE Workload Identity which will allow a fine-grained access control capability for OCI services from pods.

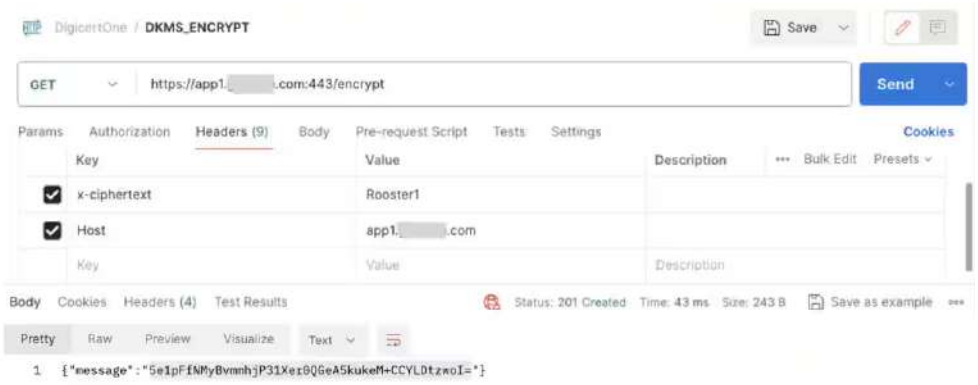
Testing the crypto microservices

Once all of the prerequisite components are now in place - we can test our services using any simple HTTP tool - such as postman. As you can see, the microservice is pretty straight forward considering what is required to validate the functionality.

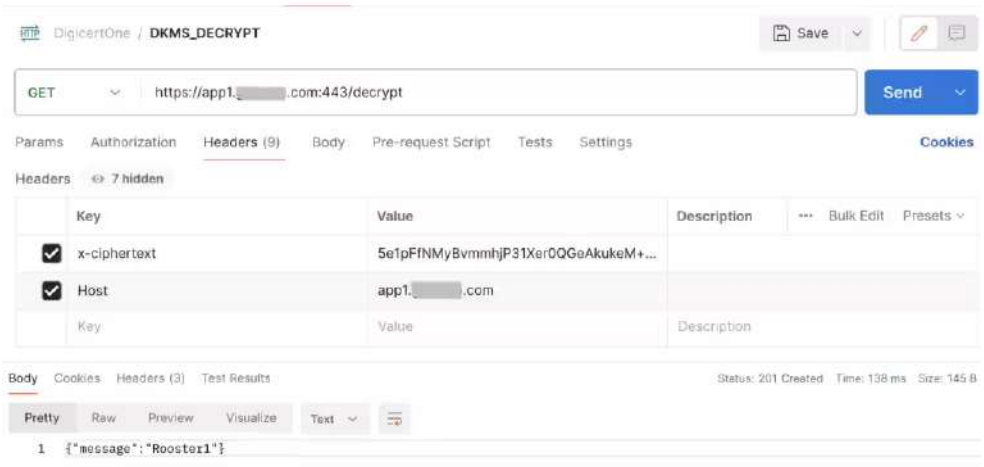
I am passing in two HTTP headers. Firstly, the Host header is required to ensure that Ingress Routing conditions are identify this string. In addition to the host header, the **/encrypt** path is the key condition for the ingress controller to route it to the appropriate microservice/pod in OKE. Lastly, I am using the

HTTP header **x-ciphertext** as my input to the encryption service.

Upon sending this request, a JSON response is returned with base64 encoded string embedded in the payload. Again, this is because the service would return a series of unfriendly characters outside of the ASCII world - which would not allow this service to be very portable or usable.



For testing the decyption - you can duplicate the previous call and simply substitute the path with **/decrypt**. This will - you guessed it - ensure that our service invocation is directed to the decryption microservice. From the previous output, copy the base64 encoded string into the **x-ciphertext** header - and voila.



As a final observation, I want to highlight the response times for each of the microservice invocations. Both are showing under 140 milliseconds, which is a variable response time given a lot of contributing factors that go into this particular test that I am executing from my local desktop. More importantly, this also does not consider the lazy and inefficient coding I created for this demo microservice.

So, if you find yourself stuck in limbo asking yourself the question - "will my application be able to perform high-performance cryptography in Oracle Cloud?" - I hope this blog has answered that question - with a resounding yes.

21.French Government Launches the PROQCIMA Program for Quantum Computing Development with Phase 1 Funding of €500 Million ($546M USD)

by GQI
https://quantumcomputingreport.com/french-government-launches-the-proqcima-program-for-quantum-computing-development/

In a bid to make France the center of gravity of the global quantum industry, the government has launched a French National Strategy for quantum that included projected investments of €1 billion ($1.1B USD) from the government over a four year period with additional investments being made by the private sector. France has made considerable progress is enjoying significant quantum startup activity and private funding in the country as well as gains in attracting and developing talent.

To further accelerate progress in French quantum technology, the government has launch the PROQCIMA program to achieve two prototype fault tolerant quantum computers of French design with at least 128 logical qubits by 2032. A follow-on goal would be to have fault tolerant quantum computers with at least 2048 logical qubits by 2035.

The PROQCIMA program is structured as a competition that will occur in three phases (concept, maturation, and industrialization) over the next several years. The program will start with five teams developing their technology for the first four years. The teams selected for this first phase includes Alice & Bob, C12, Pasqal, Quandela, and Quobly with a total funding of €500 million ($546M USD). At the end of that first period three teams will be selected to continue on for the next four years in the second phase. And after that, two teams will be selected for continued development and commercialization in the final phase.

The French government has posted an announcement (in French) regarding the launch of the PROQCIMA program on their website that can be accessed here. Another press release from Alice & Bob can be seen here.

22.Ericsson Gives PQC Progress Report at Mobile World Congress

by Berenice Baker
https://www.iotworldtoday.com/quantum/ericsson-gives-pqc-progress-report-at-mobile-world-congress#close-modal

Telecommunications operators are incorporating post-quantum cryptography (PQC) and quantum-enabled security measures into their networks. A panel hosted by GSMA, the organizer of Mobile World

Congress Barcelona, assessed the current status across the industry.

One of the panelists was Taylor Hartley, a network security solutions architect at Ericsson U.S., who offered lessons from Ericsson's experience that other organizations could benefit from in their own PQC journey.

"At Ericsson, we've been tracking this quantum threat for quite a while and our research departments have been working on post-quantum cryptography (PQC). But in the U.S. specifically, we have a very strict timeline that's been put upon us to begin this migration to PQC," she said.

Hartley's role has seen her driving executive engagement to get the C-suite on board with the measures they need to take. The most frequent question is whether PQC is "a standards thing or a technical thing," with a view that if it is just standards, it will work itself out over time, but a technology change needs more investment.

The next step is to create a strategy team of cryptography, security and quantum experts to build a roadmap and ensure internal messages align. Then organizations need to take a complete cryptographic inventory.

"For a large company like Ericsson, we have to create a clear scope. How are we going to attack this? Is it going to be by customer, by product or a little bit of both?" Hartley said. "We have the Ericsson Security Manager cybersecurity tool that does a compliance scan so we can check what protocols we're using, manage our public key infrastructure and get the tools together so we can become more crypto agile."

Hartley said the biggest challenge to PQC migration, both from the perspective of Ericsson and also from the partners to whom the company provides equipment, is the hardware.

"As we move more into digitization and virtualization, software is going to be a far easier lift. There's not going to be that much change except bigger key sizes, but I think a lot of use cases are already built to be able to handle larger key sizes," she said.

"But hardware lacks the crypto agility software has. You won't have to uplift all your hardware, some of it you can patch once or twice. We call this crypto flexible rather than agile. But the reality is there will have to be an uplift and there will have to be modernization that happens to some hardware, and I think that might be the biggest challenge so far."

23.FIDO Alliance ensures long-term value of its specifications in post quantum era

by Abhishek Jadhav
https://www.biometricupdate.com/202403/fido-alliance-ensures-long-term-value-of-its-specifications-in-post-quantum-era

Cryptography plays a fundamental role in securing data within computer systems, particularly those involving biometric technologies. It ensures that confidentiality, integrity and authenticity of sensitive data, whether it's processed locally at the edge or sent to cloud servers for further analysis and storage.

However, with the introduction of quantum computing, which has rapidly advanced in computational capabilities, present a significant threat to these cryptographic methods. Large-scale quantum computers have the potential to break several established cryptographic algorithms, including RSA and ECC, by solving the complex mathematical problems upon which their security relies.

In response to the threats, the cryptographic community and various organizations are actively developing post-quantum cryptographic (PQC) algorithms. These algorithms are designed to withstand quantum computing attacks, offering a replacement for existing algorithms and ensuring continued security in the quantum era.

In a parallel effort, the FIDO Alliance is working to address the impact of quantum computing on its specifications, aiming to preserve the long-term value efficacy of products and services built on these specifications. The specifications are expected to rely on standards developed by other organizations such as NIST and ISO, which are monitoring the process of PQC algorithms and their implications for existing specifications.

FIDO Alliance has outlined a strategy for integrating post-quantum cryptography into its standards. The Alliance aims to facilitate a smooth transition from current cryotpgraphic algorithms to post-quantum croyptographic algorithms. Despite the fact that the timeline for availability of quantum computers capable of breaking a classical cryptographic algorithm is debatable, but experts believe this can happen within 10 years. However, FIDO Alliance believes that the migration of security strategies take time, and a post-quantum strategy for migration is necessary.

As part of its strategy, the Alliance will monitor the development of various PQC algorithms, including lattice-based systems, coding-based systems, supersingular isogenies, and hash-based signatures. They acknowledge that not every PQC algorithms will be compatible with their specifications, and they plan to assess the recommendations of security agencies such as NIST to determine the effectiveness for integration into FIDO standards.

The FIDO Alliance also intends to form working groups tasked with understanding the implications of transitioning to PQC algorithms and crypto-agility. The crypto-agility here refers to the ability to manage multiple algorithms for the same function. These working groups will be charged with developing strategies for migration.

Furthermore, an additional objective of the FIDO Alliance for post-quantum cryptography is to provide guidance to its members and stakeholders as the development and standardization of PQC algorithms advnace.

Earlier this year, Prove Identity has joined the FIDO Alliance Board of Directors. Prove will be expected to contribute in developing future standards for authentication and identity authentication and identity attestation.

24.QuSecure's Leading Post-Quantum Cryptography Solution Wins Zero Trust Security Excellence Award

by Dan Spalding

https://www.businesswire.com/news/home/20240305779774/en/QuSecure%E2%80%99s-Leading-Post-Quantum-Cryptography-Solution-Wins-Zero-Trust-Security-Excellence-Award

QuSecure™, Inc., a leader in post-quantum cryptography (PQC), today announced that its QuProtect PQC software solution has earned a Zero Trust Security Excellence Award. The award, presented by TMCnet, recognizes the leaders and pioneers in the industry with the best and the brightest providers, offering the most innovative and effective solutions.

"We are honored to be recognized for our Zero Trust innovations in post-quantum cryptography, and to win this Zero Trust Security Excellence Award," said Rebecca Krauthamer, QuSecure co-founder and Chief Product Officer. "QuProtect's post-quantum technologies are paving the way for organizations to adopt protections where they are most critical, providing cryptographic agility and orchestration without requiring the removal or replacement of existing encryption or infrastructure. QuProtect uniquely offers secure, interoperable cybersecurity enabling a zero-trust network architecture providing protection from today's classical and emerging AI and quantum threats."

QuSecure's QuProtect software is available to test and deploy in production and enables organizations to leverage quantum-resilient technology to prevent today's cyberattacks, while future-proofing networks and preparing for quantum cyberthreats. It provides quantum-resilient cryptography, anytime, anywhere, and on any device including network, cloud, edge devices, and satellite communications. Using QuProtect, organizations can implement PQC on the network with minimal disruption to existing systems since existing, standard encryption remains in place. QuProtect software uses end-to-end quantum-security-as-a-service architecture that addresses the digital ecosystem's most vulnerable use-cases, uniquely combining zero-trust, next-generation post-quantum cryptography, crypto-agility, high availability, easy deployment, and active defense into a comprehensive and interoperable cybersecurity suite. The end-to-end approach is designed to protect the entire information lifecycle as data is communicated, used and stored.

"It gives me great pleasure to honor the recipients of the TMCnet Zero Trust Security Excellence Award," said Rich Tehrani, CEO, TMC. "The award recognizes solutions providers championing the 'Trust Nothing, Verify Everything' mantra of a Zero Trust approach to security at a time when businesses are facing more complex and frequent threats than ever."

25.Assessing the post-quantum threat – 3 tips to be ready

by David Senf and Marcus Mesan
https://www.sdxcentral.com/articles/contributed/assessing-the-post-quantum-threat-3-tips-to-be-ready/2024/03/

The very foundation of cybersecurity is at risk as quantum computers become more advanced. The ability of threat actors to access otherwise secure digital communications and data is known as the ``post-quantum threat." This threat has been thoroughly covered by government agencies, in the media and by analyst firms over the past decade. This brief offers an update on the topic and outlines actions that organizations can take today given recent research breakthroughs.

Quantum Computing and its positive impact

Quantum computing has transformative potential across many industries. In the pharmaceutical space, for example, it could significantly accelerate drug discovery. In finance, quantum algorithms could model market dynamics with unprecedented precision. Quantum computing could also generate innovations in material science, supply chain management and weather forecasting. Artificial intelligence, meanwhile, stands to benefit from this technology as it becomes capable of processing vast datasets far more efficiently than what today's classical computers can achieve.

The urgency of the threat

Several technical issues are currently limiting the scalability of quantum computing. If solved, we'll witness a new era of computing that is more significant even than the recent rise of generative artificial intelligence. Within the next decade, or sooner, it's possible that a quantum computer powerful enough to become a serious cybersecurity threat could be built.

A fully functional quantum computer capable of breaking current cryptographic systems is not yet a reality. The threat is imminent enough, however, to cause some to take action in anticipation of nation state and other threat actors gaining access to quantum computing. The idea of hackers using a "harvest now, decrypt later" tactic poses an immediate risk. Adversaries could be collecting encrypted data with the purpose of decrypting it once quantum computing becomes sufficiently advanced.

This would especially affect sensitive data intended to remain confidential for many years, such as state and military secrets, proprietary research (from universities, government, corporations, etc.), health data and more. Organizations in industries such as finance, governments and verticals involved in critical infrastructure are beginning to plan for the threat.

Organizations like IBM, Google, and various vendors and consultancies are making significant progress towards a functional quantum computer. Recent research led by a team at Harvard University demonstrated promising new techniques for a far more scalable quantum computer (e.g., far more logical qubits operating on physical qubits). Their work could have the unintended side effect of dramatically accelerating the timeline of the post-quantum threat.

Getting ready, just in case

In response to these challenges, the security industry, researchers and cryptographers are actively working on developing post-quantum cryptographic algorithms. These new algorithms are designed to be secure against both classical and quantum computing threats. The National Institute of Standards and Technology (National Institute of Standards and Technology (NIST)) in the United States is leading an initiative to standardize post-quantum cryptography. Their work will allow the flexible and scalable forms of encryption we need to continue to operate over the public internet.

Certain forms of encryption are more vulnerable to the quantum threat. Asymmetric encryption, the underlying form of encryption used for browsing, online shopping and doing most everything over the internet, is particularly vulnerable. This is due to quantum computers' potential ability to solve problems, such as factoring large numbers, used in asymmetric encryption such as RSA that are currently not possible for classical computers.

Symmetric encryption, on the other hand, appears to be more resistant to the quantum threat. Algorithms like advanced encryption standard (AES(AES) are not based on the same mathematical problems as asymmetric algorithms. Symmetric encryption, however, does not have the scalability of asymmetric encryption, making it unsuitable for ecommerce and most common B2C and B2B use cases.

Transitioning to post-quantum cryptography is not just a technical challenge but also an operational and logistical one. It requires updating and replacing a vast array of technologies currently in use, including those embedded in our everyday lives, like web browsers, email servers, and Virtual Private Network (virtual private network (VPN)). The transition also involves a learning curve for cybersecurity professionals, who must familiarize themselves with the new tools, processes and their implementation / operations.

In addition to quantum-resistant algorithms, techniques such as Quantum Key Distribution (QKD) can use the properties of quantum mechanics to secure communications.

As the quantum threat advances, your organization should consider the following actions:

1. **Quantum risk assessment**: Start with a risk assessment to understand the potential impact of quantum computing on your organization's data security. This involves identifying sensitive data that could be at risk as well as understanding its lifespan. Consider how long data needs to be secure and whether it could be a target for future quantum attacks.

2. **Inventory of current cryptographic systems**: Take inventory (and assess the capabilities) of your current cryptographic systems. This includes understanding which systems rely on quantum vulnerable algorithms and key management. The goal is to identify where cryptographic changes are required and to prioritize the systems that handle the most sensitive information.

3. **Research and adopt Post-Quantum Cryptography (PQC)**: Start researching and gradually adopt post-quantum cryptographic algorithms (much of which will come by way of technology vendors). Keep up with emerging standards from NIST, which is in the process of standardizing PQC algorithms. Create a transition plan for migrating to post-quantum algorithms.

Continue to monitor advancements in quantum computing and engage with the security community for best practices and emerging technology to stay ahead of potential risks.

Get ready for the opportunities and challenges of quantum computing

Quantum computing promises impressive breakthroughs in many aspects of industry and our daily lives, but it also presents a significant challenge to cybersecurity. As the advances in quantum computing accelerate, the need for robust post-quantum secure systems becomes more urgent. This transition requires monitoring and early efforts from government, industry and academia in order to develop secure cryptographic standards and implement them effectively.

While quantum computing has the potential to affect the very foundation of cybersecurity, we have time to approach this evolving field carefully and to make needed changes and updates.

