Crypto News

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

March 01, 2024

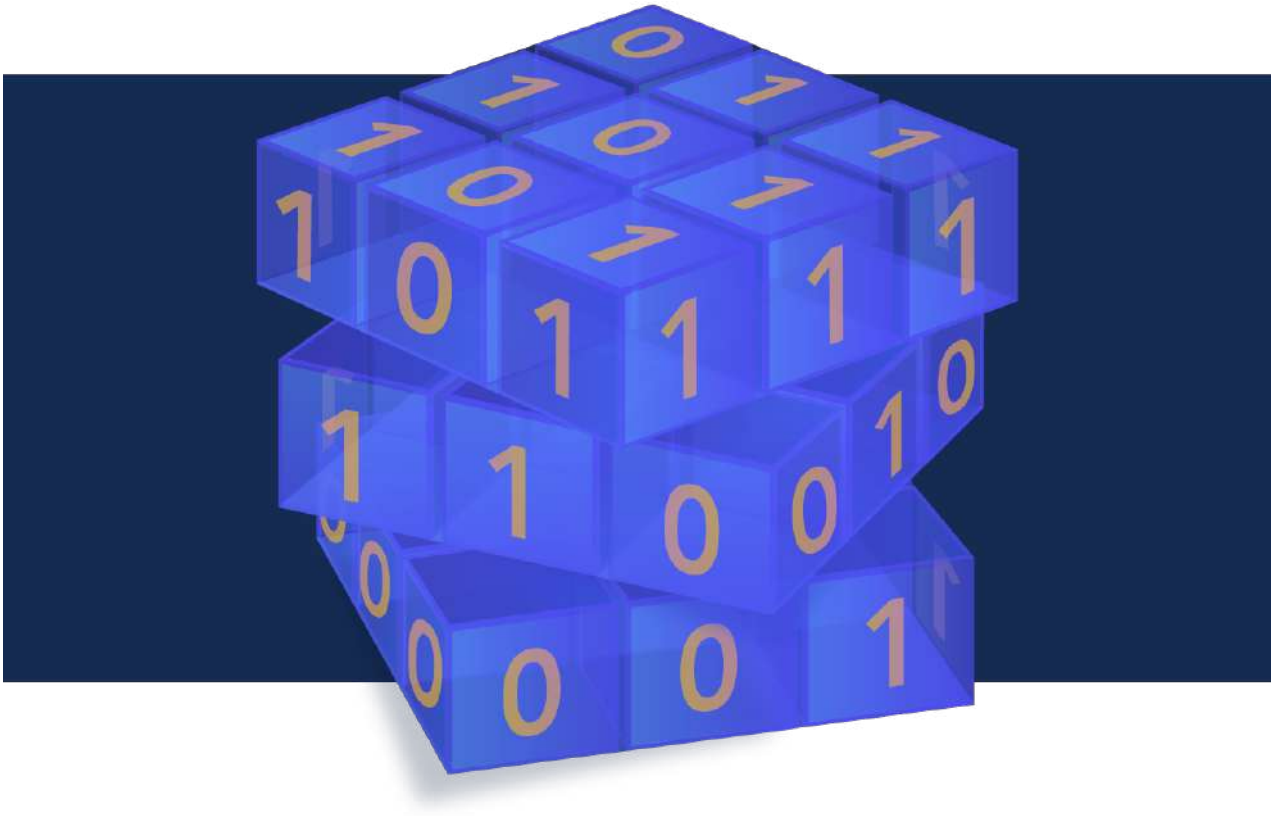


TABLE OF CONTENTS

Editorial

Dear Quantum-Safe aficionados,

Here is your monthly allowance of Crypto News, brought to you as usual by Dhananjoy, our most avid reader.

This month, we see an interesting implementation of post-quantum crypto in Apple phones. Apple will use PQ3 in its iMessage communications. This is reported in Article 3, Article 5 and in Article 5.1 by the QSS member Roger Grimes. Post-Quantum crypto has truly entered the implementation stage.

The quantum solutions to the quantum threat are also mentioned this month, with Article 6 reporting on the release by ETSI of the first protection profile for QKD. This will undoubtedly facilitate the adoption of this new technology.

Both of the above clearly demonstrate that the quantum threat is now taken seriously. So, we should all agree that the quantum computer era is already upon us. However, this is not so clear yet. If you read Article 7 and Article 8, you will see that the fight for supremacy between classical and quantum computers is still on. This reminds me of the battle between ADSL and optical fiber to the home. We all thought that optical fibers would quickly replace ADSL everywhere, but progress with twisted pairs delayed this for a long time. Somehow, progress in quantum computing is also bringing new results in classical computing. We will all profit from this.

Have a good read, and stay Quantum-Safe!

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security-Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA 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.The keys to protecting the Army's fire-power

by Kathryn Bailey
https://www.army.mil/article/274092/the_keys_to_protecting_the_armys_firepower

To reverse an old adage, sometimes the best offense is a good defense.

One of the most effective defensive maneuvers attributed to the U.S. Army depends upon the security of its highly advanced information networks, which are protected by cryptographic technologies and policies that block attacks of potential adversaries,

The digital armor protecting network enabled weapons systems is the cryptographic key material, provided by the National Security Agency (NSA) via the Key Management Infrastructure (KMI), which generates the unique keys. The NSA keys must be delivered to Army users wherever secure communications are required. Traditionally, Communications Security (COMSEC) personnel securely download the keys in safe locations and then loaded the keys onto portable storage devices, called Simple Key Loaders (SKLs), for transport to end users.

However, the process for delivering and managing keys to an operational environment is complex, leading to delays, safety concerns for the couriers and opportunities for adversaries to physically intercept this mission critical information.

"Nothing could be more critical than assuring commanders have the most secure and relevant information from which to base their decisions," said Mike Badger, product lead for COMSEC, assigned to the Program Executive Office Command, Control, Communications-Tactical (PEO C3T). "The Army's COMSEC modernization effort is systematically addressing these concerns, with two networked KMI capabilities available today that are easing the burden, and peril of COMSEC key delivery and management."

The first, Intermediary Application (iApp), is a tested and proven key management software-only application that securely manages and distributes Over the Network Key (OTNK) to geographically separated users for real-time, networked Encrypted Key Distribution (EKD).

The Army co-funds the development of the Navy-developed iApp.

"Historically, the SKLs were hand carried to the encryption device, which could be as easy as walking across the hall or as arduous as traveling across the world, putting both the carrier and encrypted information at risk with each passing mile – especially if those miles cross a combat zone," said Jeremy Pilkington, deputy product lead for PdL COMSEC.

Soldiers who hand carried an SKL to the weapon system, satellite modem, radio, or command vehicle loaded the keys onto the end user device for encryption and decryption of mission critical information.

"With iApp, we don't have to go to a KMI account manager, which provides us the advantage of speed and takes away the opportunity for physical interception," said Brian Finley, assistant program manager for Army Key Management Infrastructure, assigned to PdL COMSEC.

The ONTK capabilities of iApp are used by all the DOD and civil agencies that perform crypto key distribution, including U.S. Southern Command, Joint Special Operations Command, U. S. Indo-Pacific

Command, and Special Operations Command, supporting more than 200 elements. It is available for download to any crypto key managers and users through the Army's Mission Command Support Center.

iApp was put into practice during Typhoon Khanun, which was a powerful and long-lasting tropical cyclone that moved along Okinawa, Japan and the west coast of the Korean Peninsula in August 2023.

As a result of the storm, the 78th Signal Battalion in Camp Zama, Japan, experienced a KMI outage, which prevented them from receiving COMSEC keys through the traditional hand-carried method.

"As a workaround, the Network Enterprise Center in Okinawa, Japan used iApp to deliver COMSEC keys using iApp's OTNK capabilities to the 78th Signal Battalion, which ensured the continued operation of secure communications for the unit's Pacific area of operations," Finley said.

Complimenting iApp's rapid and safe OTNK transfer is the second COMSEC key-related capability, called the Common High-Assurance Internet Protocol Encryptor (HAIPE) Interoperable Manager for Efficient Remote Administration (CHIMERA).

For economic competitiveness, the Army procures INEs from three encryption vendors, each with their own proprietary management software and interfaces. The CHIMERA dashboard simplifies key management by providing a common user interface for remotely managing these three unique families of encryptors, reducing complexity for the user and overall costs.

"This is the single pane of glass, or in this case, the single app at a single location that allows users to determine how the network is functioning according to NSA high assurance defense networking products for both classified and unclassified network and assets," said Kimoanh Le, assistant product manager for COMSEC Cryptographic Systems PdL COMSEC.CHIMERA quickly identifies and remedies network threats and outages to provide situational awareness of the entire cryptographic network from a single host. Like iApp, CHIMERA enhances user safety since a single operator can operate complex INE-heterogeneous networks from one location.

"Without CHIMERA, users had to piece together bits of network information from across all three vendor-proprietary networked laptops," Le said.

Information includes error warnings such as battery life or key expiration dates. With one interface, users can perform device-to-device key transfers, with immediate confirmation of the transfer.

As a government off the shelf product, CHIMERA is free for any U.S Government organization.

Providing secure and interoperable cryptographic key generation, distribution, and management capabilities that support mission-critical systems is a continual requirement for the Army's COMSEC professionals.

"In cryptography the adversary is always advancing," Badger said. "It's a force-on-force engagement where they are trying to decrypt your information and undermine your confidentiality," Badger said. "Networked KMI is one of the defenses the Army will use to stay ahead of the threat."

2.Deutsche Telekom Commits to Global Title Leasing Code That Stops Phone Spies

by Eric Priezkalns

https://commsrisk.com/deutsche-telekom-commits-to-global-title-leasing-code-that-stops-phone-spies/

Some important news was announced at Mobile World Congress on 27 Feb 2024, but it will not receive much publicity because the detail is too complicated to interest the public and the proposed change will not boost revenues, although it addresses a problem that can have fatal consequences. It seems counterintuitive that the failings of a comms provider on the far side of the planet can help murderers locate their target, but that appears to have been the case in the 2022 assassination of Mexican journalist Fredid Román Román (pictured). Investigative journalists Crofton Black and Omer Benjakob set the scene for an exposé published by *Haaretz* last year.

A day before he was shot dead getting into his car outside his home in Chilpancingo, the capital of the southern Mexican state of Guerrero, journalist Fredid Román Román's phone number was silently pinged in what confidential data seen by Lighthouse Reports, Haaretz and partners seems to suggest was an attempt to geolocate the reporter using a loophole in the mobile phone system.I hope that most readers of Commsrisk already know about the harm that can be caused when bad actors exploit vulnerabilities inherent to global title, the addresses used when routing signals for SS7 networks. Scammers and spammers who flood networks with dangerous and unwanted SMS messages often evade detection by hiding behind somebody else's global title. That is the side of global title abuse that affects very many people. Other forms of abuse are more particular, but with potentially devastating consequences. The telecoms industry has successfully implemented the means to allow mobile phones to connect to networks worldwide, but this puts individuals at risk when a bad actor uses this global infrastructure to locate and spy upon a phone user.

Several concerned parties have shown leadership by writing an industry code of conduct on the leasing of global titles. Criminals and spies want to hide in the shadows, and leasing global title gives them access to SS7 whilst allowing them to obscure their true identities by hiding behind the comms provider who owns the global title. Some comms providers are too easily tempted by the additional revenues generated by renting out global title to others, and do not make enough effort to verify who they are dealing with, or to monitor how the global title is being used in practice. The code of conduct, published by the GSMA, would tackle those issues if adopted widely.

That, as usual, is where the most challenging work begins. It is difficult to write and publish an industry code of conduct, although it is only a series of words. Getting a lot of businesses to respect the code of conduct is much harder, especially in the beginning. That is why it is a significant development that Deutsche Telekom announced they will comply with the code at Mobile World Congress yesterday. Per their slide pack, which was shared with Commsrisk in advance, Deutsche Telekom is the first operator to endorse the new code. Johannes Opitz, Vice President of Commercial Roaming and International Mobile Wholesale at Deutsche Telekom, joined Stephen Ornadel, the editor of the code, in outlining a five-point industry plan for tackling the abuse of global title leasing.

1. Eliminate excuses and ignorance through education
2. Set reasonable standards of behaviour through a CoC
3. Flush out bad behaviour whilst protecting helpful solutions.
4. Drive up standards by enabling operators to publicly declare support and compliance
5. Link standard roaming agreements to the CoC

Deutsche Telekom has gone first by declaring their support. Perhaps that was inevitable, given the apparent importance that Germans attach to privacy compared to some other nationalities. But this problem cannot be solved by a single telco working in isolation. Success will be determined by how many voluntarily follow, and how soon they choose to follow. Associations like the GSMA are willing to bring people together to draft codes of conduct, but they will not take any steps to enforce them until majority support is clearly established. To do otherwise would put the GSMA's own revenues at risk, with nothing gained because bad actors will continue to misbehave as they did before. The onus must be on other

big telcos to loudly and prominently commit to obeying the global title leasing code.There have recently been quite a few big telcos claiming they fully support international collaboration against scams. This is one opportunity to distinguish between those who really mean it and those who are just mouthing platitudes about consumer protection when put under pressure. And whilst scam reduction is an important reason to tighten controls around global title, we should be equally mindful of the tragic implications when the intelligence-gathering capabilities of comms networks are commandeered by spies and thugs who intend to hurt somebody. Please encourage the adoption of this code, and let us all keep a watchful eye on those telcos that promise to obey it, and those which choose to ignore it.

3.Apple, Signal Debut Quantum-Resistant Encryption, but Challenges Loom

by Jai Vijayan
https://www.darkreading.com/cyber-risk/as-quantum-resistant-encryption-emerges-so-do-worries-about-adoption-challenges

Apple's new PQ3 post-quantum cryptographic (PQC) protocol introduced last week is the latest manifestation of a trend that will accelerate over the next few years as quantum computing matures and takes root in a variety of different industries.

Protocols like PQ3, which Apple will use to secure iMessage communications, and a similar encryption protocol that Signal introduced last year called PQXDH, are quantum resistant, meaning they can — theoretically, at least — withstand attacks from quantum computers trying to break them.

A Vital, Emerging Requirement

Many consider that capability will become vital as quantum computers mature and give adversaries a trivially easy way to crack open even the most secure current encryption protocols and access protected communications and data.

Concerns over that potential — and of adversaries already harvesting sensitive encrypted data and storing them for future decryption via quantum computers — prompted a National Institute of Standards and Technology initiative for standardized public key, quantum-safe cryptographic algorithms. Apple's PQ3 is based on Kyber, a post-quantum public key that is one of four algorithms that NIST has chosen for standardization.

Rebecca Krauthamer, chief product officer at QuSecure, a company that focuses on technologies that protect against emerging quantum computing-related threats perceives Apple's announcement will drive further momentum in the PQC space.

"We have been implementing with a number of well-known organizations in the space, and I can say firsthand that Apple's announcement is the first of many to come in the next four months," Krauthamer says. She anticipates similar moves from developers of other messaging apps and social media platforms.

Up until now, the government, financial services, and telecom sectors have driven early adoption of PQC. Telecom companies in particular have been at the forefront in experimenting with quantum key distribution (QKD) for generating encryption keys, she says. "But in the past 18 months, we've seen

them migrate towards PQC as PQC is digitally scalable, while QKD still has significant scalability limitations," Krauthamer adds.

Long and Complicated Migration Path

For organizations, the shift to PQC will be long, complicated, and likely painful. Krauthamer says post-quantum encryption algorithms will redefine the landscape of authentication protocols and access controls. "Current mechanisms heavily reliant on public key infrastructures, such as SSL/TLS for secure Web communications, will require reevaluation and adaptation to integrate quantum-resistant algorithms," she says. "This transition is crucial for maintaining the integrity and confidentiality of mobile and other digital interactions in a post-quantum era."

The migration to post-quantum cryptography introduces a new set of management challenges for enterprise IT, technology, and security teams that parallels previous migrations, like from TLS1.2 to 1.3 and ipv4 to v6, both of which have taken decades, she says. "These include the complexity of integrating new algorithms into existing systems, the need for widespread cryptographic agility to swiftly adapt to evolving standards, and the imperative for comprehensive workforce education on quantum threats and defenses," Krauthamer says.

Quantum computers will equip adversaries with technology that can relatively easily strip away the protections offered by the most secure of current encryption protocols, says Pete Nicoletti, global CISO at Check Point Software. "The 'lock' in your browser bar will be meaningless as quantum computer-equipped criminals will be able to decrypt every banking transaction, read every message, and gain access to every medical and criminal record in every database everywhere, in seconds," he says. Critical business and government communications conventionally encrypted in site-to-site VPNs, browsers, data storage, and email are all at risk of "harvest now, decrypt later" attacks, he says.

Harvest Now, Decrypt Later

"Right now, in certain verticals, business leaders should assume that all of their encrypted traffic is being harvested and stored for when quantum encryption is available to crack it," Nicoletti says. Even though such attacks might be a while away, business and technology leaders need to be aware of the issue and start preparing for it now.

The goal should be to not impact users when transitioning to PQC, but every indication is that it will expensive, chaotic, and disruptive, he says. Messaging apps like Apple's PQ3 are relatively easy to deploy and manage. "Consider the chaos when your corporate firewall or cloud provider does not support a certain post-quantum encryption algorithm with a partner or a customer, and you can't communicate securely," he says, by way of an example. Unless vendors of browsers, email, routers, security tools, database encryption, and messaging are all on the same page, enterprise IT teams will have their hands full making the switch to PQC, he cautions.

Grant Goodes, chief innovation architect at mobile security vendor Zimperium, advocates that organizations take a measured approach to implementing PQC, considering the enormity of the task and the fact it's unclear when in the future many of the most feared security consequences of quantum computing will come to pass. Like others, he concedes that when quantum computers finally come of age, they will make even the most secure RSA encryption trivial to break. But breaking an RSA-2048 key would require some 20 million qubits, or quantum bits, of processing power. Given that current practical quantum computers only have around 1,000 qubits, it's going to take at least another decade for that threat to become real, Goodes predicts.

"Second, there is the concern that these proposed post-quantum ciphers are very new and have yet to

be truly studied, so we don't really know how strong they are," he notes. As a case in point, he cites the example of SIKE, a post-quantum encryption algorithm that NIST approved as a finalist for standardization in 2022. But researchers quickly broke SIKE shortly thereafter using a single-core Intel CPU.

"New ciphers based on novel mathematics are not necessarily strong, just poorly studied," Goodes says. So a more measured approach is likely prudent for adopting PQC, he adds. "Post-quantum cryptography is coming, but there is no need to panic. Doubtless they will start to make their way into our devices, but existing algorithms and security practices will suffice for the immediate future."

4.Is hybrid encryption the answer to post-quantum security?

by Peter Wayner
https://www.csoonline.com/article/1307682/is-hybrid-encryption-the-answer-to-post-quantum-security.html

Proponents believe hybrid encryption compensates for weaknesses in single post-quantum algorithms, but performance, complexity, and security concerns remain.

If you wear suspenders, do you need a belt? If you have one parachute, do you need a reserve? Many CISOs, security teams, and cryptographers are asking a similar question about encryption algorithms when they choose the next generation of protocols. Do users need multiple layers of encryption? Do they want the complexity and cost, too?

What is hybrid encryption?

Many discussions of “hybrid encryption” begin with some debate about just what this means. Hybrid encryption in general refers to the combined use of public-key (asymmetric) cryptography with symmetric encryption. Systems that combine multiple algorithms are common and mathematicians have been marrying different algorithms to leverage their advantages for some time. For instance, many public-key systems use the public-key algorithms only to scramble a symmetric key that is then used to encrypt the data. Symmetric algorithms like AES are generally dramatically faster, and the hybrid approach captures these benefits.

The topic is receiving plenty of attention now because of the rollout of the post-quantum algorithms developed through **NIST’s post-quantum cryptography (PQC) competition**. Some wonder if the new approaches are trustworthy, and they’re hoping that some kind of hybrid approach will bring more assurance during any transition.

Adding layers is not a new solution. When Stuart Haber and Scott Stornetta designed a **time-stamping service** that became the company Surety, they used two different hash functions in parallel. They also designed the protocols so that newer, better hash functions could be **added later**. “In the face of unexpected algorithmic advances in cryptanalysis, we wrestled with the problem of how best to swap in a new hash function in an existing widely deployed authentication system,” Haber tells CSO. “We didn’t want to stake everything on just one algorithm.”

Google is already proceeding down the path of using hybrid algorithms. Last year, Chrome and some servers started negotiating session keys using a combination of two algorithms:

- X25519 – A common choice of TLS that uses elliptic curves
- Kyber-768 – a quantum-resistant key encapsulation method and **NIST's PQC winner**

In a recent **announcement**, Devon O'Brien, technical program manager for Chrome security, said that the extra Kyber-encapsulated key material added about 1,000 bytes to each TLS ClientHello message, an overhead that was not an issue for the "vast majority" of users.

Post-quantum cryptography solutions not foolproof

The post-quantum rollout has been both exciting and frustrating. NIST has extended deadlines multiple times before settling on potential solutions. It's also added new rounds to encourage developing more approaches in case some of the other techniques prove insecure. Anyone who expected the competition to produce one perfect solution to carry us safely into the future was disappointed. The competition easily produced as many questions as answers.

The danger of choosing a new algorithm with hidden flaws isn't a theoretical threat. Already, several algorithms that made it into the final rounds showing plenty of promise turned out to be easily broken. The **Rainbow signature scheme** and **Supersingular Isogeny Diffie-Hellman protocol (SIDH)** have both been compromised, for instance.

Hybrid encryption a hedge against weaknesses

If hidden weaknesses are always a potential threat, then hybrid solutions seem like an ideal approach. Instead of just swapping out a perfectly good but aging algorithm like RSA or AES and replacing it with a new but barely tested version, why not use both? Or even three or more? Why not compute several signatures or encrypt the data again and again?

Whitfield Diffie, a cryptographer who's worked on developing some of the widely used public key encryption algorithms, believes in the hybrid approach. "It's indispensable for a transition to PQC," he tells CSO.

The downsides of hybrid encryption

The critics, though, offer these reasons why hybrid solutions may not be ideal:

- **Increased complexity:** They need at least twice as much code to write, debug, audit and maintain.
- **Decreased efficiency:** They need at least twice as much computational overhead for encrypting or decrypting any data or the session key.
- **Inconsistent structures:** The algorithms are not easy drop-in replacements for each other. Some signature algorithms, for example, have single-use keys while others don't.

"It's hard enough to implement one standard correctly. Using two in parallel opens up more risk of implementation errors or creating new types of attacks." Steve Weis, a principal engineer at Databricks, tells CSO. "Also, performance still matters in many contexts where incurring two times or more the computation costs and payload size is a non-starter."

One of the most prominent critics of the new approach is the National Security Agency (NSA), the United States government entity with a longstanding interest in developing secure encryption. Over the last few

years, the NSA has discouraged the push for hybrid algorithms, citing many of the reasons given above. They were also joined by **GCHQ**, the British group that often works together with the Americans through an alliance that is loosely known as the "Five Eyes."

"Do not use a hybrid or other non-standardized QR solution on NSS [national security system] mission systems," the NSA wrote in an FAQ on the transition to post-quantum algorithms. "Using non-standard solutions entails a significant risk of establishing incompatible solutions."

The NSA, though, has a Janus-faced mission. On one side, they're responsible for ensuring that the country's communications are secure. On the other side, they also routinely break codes to gather intelligence. Many wonder which mission the NSA may be serving.

Other national cryptographic agencies like France's ANSSI and Germany's BSI (Federal Office for Information Security), though, are taking a different approach. They encourage the assurance that comes from using multiple layers. "The secure implementation of PQC mechanisms, especially with regard to side-channel security, avoidance of implementation errors and secure implementation in hardware, and also their classical cryptanalysis are significantly less well studied than for RSA- and ECC-based cryptographic mechanisms." concluded the German Federal Office of Information Security (BSI). "Their use in productive systems is currently only recommended together with a classic ECC- or RSA-based key exchange or key transport."

For some internal classified work, the NSA also pushes multiple layers of encryption. Their guidelines for using commercially available software in classified environments frequently encourage using multiple "layers" of independent packages.

How much security does hybrid encryption provide?

One of the biggest debates is how much security hybridization offers. Much depends on the details and the algorithm designers can take any number of approaches with different benefits. There are several models for hybridization and not all the details have been finalized.

Encrypting the data first with one algorithm and then with a second combines the strength of both, essentially putting a digital safe inside a digital safe. Any attacker would need to break both algorithms. However, the combinations don't always deliver in the same way. For example, hash functions are designed to make it hard to identify collisions, that is two different inputs that produce the same output: (x_1 and x_2, such that h(x_1)=h(x_2)).

If the input of the first hash function is fed into a second different hash function (say g(h(x))), it may not get any harder to find a collision, at least if the weakness lies in the first function. If two inputs to the first hash function produce the same output, then that same output will be fed into the second hash function to generate a collision for the hybrid system: (g(h(x_1))= g(h(x_2)) if h(x_1)=h(x_2)).

Digital signatures are also combined differently than encryption. One of the simplest approaches is to just calculate multiple signatures independently from each other. They can be tested independently afterwards. Even this basic approach raises many practical questions. What if one private key is compromised? What if one algorithm needs to be updated? What if one signature passes but one fails?

Cryptography is a complex subject where many areas of knowledge are still shrouded in a deep cloud of mystery. Many algorithms rest upon assumptions that some mathematical chores are too onerous to accomplish but there are no rock-solid proofs that the work is impossible.

Many cryptographers who embrace hybrid approaches are hoping that the extra work more than pays off should a weakness appear. If it's worth putting in the time to get one layer right, it's often worth it to

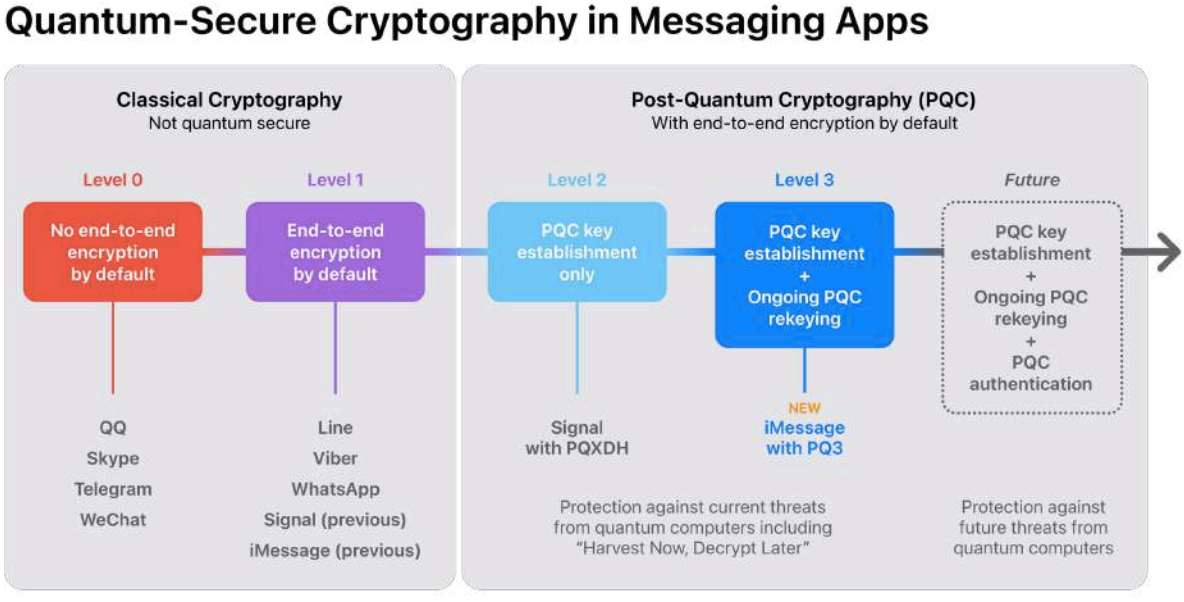
do it again. The high-performance applications can turn it off, but those that need it want extra assurance.

“We’re stuck with an argument from ignorance and an argument from knowledge,” explains Jon Callas, distinguished engineer at VATIK security. “It’s taken us decades just to get padding right. You can say RSA [cryptography] is broken, but we don’t know anything about the new algorithms.”

5.iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

by Apple Security Engineering and Architecture (SEAR)
https://security.apple.com/blog/imessage-pq3/

Today (21 Feb 2024) we are announcing the most significant cryptographic security upgrade in iMessage history with the introduction of PQ3, a groundbreaking post-quantum cryptographic protocol that advances the state of the art of end-to-end secure messaging. With compromise-resilient encryption and extensive defenses against even highly sophisticated quantum attacks, PQ3 is the first messaging protocol to reach what we call Level 3 security — providing protocol protections that surpass those in all other widely deployed messaging apps. To our knowledge, PQ3 has the strongest security properties of any at-scale messaging protocol in the world.



Note: This comparison evaluates only the cryptographic aspect of messaging security, and therefore focuses on end-to-end encryption and quantum security. Such a comparison doesn’t include automatic key verification, which we believe is a critical protection for modern messaging apps. As of the time of this writing, only iMessage and WhatsApp provide automatic key verification. The iMessage implementation, called Contact Key Verification, is the state of the art – it provides the broadest automatic protections and applies across all of a user’s devices.

When iMessage launched in 2011, it was the first widely available messaging app to provide end-to-end encryption by default, and we have significantly upgraded its cryptography over the years. We most recently strengthened the iMessage cryptographic protocol in 2019 by switching from RSA to Elliptic Curve cryptography (ECC), and by protecting encryption keys on device with the Secure Enclave, making them significantly harder to extract from a device even for the most sophisticated adversaries. That protocol update went even further with an additional layer of defense: a periodic rekey mechanism to provide cryptographic self-healing even in the extremely unlikely case that a key ever became compromised. Each of these advances were formally verified by symbolic evaluation, a best practice that provides strong assurances of the security of cryptographic protocols.

Historically, messaging platforms have used classical public key cryptography, such as RSA, Elliptic Curve signatures, and Diffie-Hellman key exchange, to establish secure end-to-end encrypted connections between devices. All these algorithms are based on difficult mathematical problems that have long been considered too computationally intensive for computers to solve, even when accounting for Moore's law. However, the rise of quantum computing threatens to change the equation. A sufficiently powerful quantum computer could solve these classical mathematical problems in fundamentally different ways, and therefore — in theory — do so fast enough to threaten the security of end-to-end encrypted communications.

Although quantum computers with this capability don't exist yet, extremely well-resourced attackers can already prepare for their possible arrival by taking advantage of the steep decrease in modern data storage costs. The premise is simple: such attackers can collect large amounts of today's encrypted data and file it all away for future reference. Even though they can't decrypt any of this data today, they can retain it until they acquire a quantum computer that can decrypt it in the future, an attack scenario known as *Harvest Now, Decrypt Later*.

To mitigate risks from future quantum computers, the cryptographic community has been working on post-quantum cryptography (PQC): new public key algorithms that provide the building blocks for quantum-secure protocols but don't require a quantum computer to run — that is, protocols that can run on the classical, non-quantum computers we're all using today, but that will remain secure from known threats posed by future quantum computers.

To reason through how various messaging applications mitigate attacks, it's helpful to place them along a spectrum of security properties. There's no standard comparison to employ for this purpose, so we lay out our own simple, coarse-grained progression of messaging security levels in the image at the top of this post: we start on the left with classical cryptography and progress towards quantum security, which addresses current and future threats from quantum computers. Most existing messaging apps fall either into Level 0 — no end-to-end encryption by default and no quantum security — or Level 1 — with end-to-end encryption by default, but with no quantum security. A few months ago, Signal added support for the PQXDH protocol, becoming the first large-scale messaging app to introduce post-quantum security in the initial key establishment. This is a welcome and critical step that, by our scale, elevated Signal from Level 1 to Level 2 security.

At Level 2, the application of post-quantum cryptography is limited to the initial key establishment, providing quantum security only if the conversation key material is never compromised. But today's sophisticated adversaries already have incentives to compromise encryption keys, because doing so gives them the ability to decrypt messages protected by those keys for as long as the keys don't change. To best protect end-to-end encrypted messaging, the post-quantum keys need to change on an ongoing basis to place an upper bound on how much of a conversation can be exposed by any single, point-in-time key compromise — both now and with future quantum computers. Therefore, we believe messaging protocols should go even further and attain Level 3 security, where post-quantum cryptography is used to secure both the initial key establishment and the ongoing message exchange, with the ability to rapidly and automatically restore the cryptographic security of a conversation even if a given key becomes compromised.

iMessage now meets this goal with a new cryptographic protocol that we call PQ3, offering the strongest protection against quantum attacks and becoming the only widely available messaging service to reach Level 3 security. Support for PQ3 will start to roll out with the public releases of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4, and is already in the corresponding developer preview and beta releases. iMessage conversations between devices that support PQ3 are automatically ramping up to the post-quantum encryption protocol. As we gain operational experience with PQ3 at the massive global scale of iMessage, it will fully replace the existing protocol within all supported conversations this year.

Designing PQ3

More than simply replacing an existing algorithm with a new one, we rebuilt the iMessage cryptographic protocol from the ground up to advance the state of the art in end-to-end encryption, and to deliver on the following requirements:

- Introduce post-quantum cryptography from the start of a conversation, so that all communication is protected from current and future adversaries.
- Mitigate the impact of key compromises by limiting how many past and future messages can be decrypted with a single compromised key.
- Use a hybrid design to combine new post-quantum algorithms with current Elliptic Curve algorithms, ensuring that PQ3 can never be less safe than the existing classical protocol.
- Amortize message size to avoid excessive additional overhead from the added security.
- Use formal verification methods to provide strong security assurances for the new protocol.

PQ3 introduces a new post-quantum encryption key in the set of public keys each device generates locally and transmits to Apple servers as part of iMessage registration. For this application, we chose to use Kyber post-quantum public keys, an algorithm that received close scrutiny from the global cryptography community, and was selected by NIST as the Module Lattice-based Key Encapsulation Mechanism standard, or ML-KEM. This enables sender devices to obtain a receiver's public keys and generate post-quantum encryption keys for the very first message, even if the receiver is offline. We refer to this as initial key establishment.

We then include — within conversations — a periodic post-quantum rekeying mechanism that has the ability to self-heal from key compromise and protect future messages. In PQ3, the new keys sent along with the conversation are used to create fresh message encryption keys that can't be computed from past ones, thereby bringing the conversation back to a secure state even if previous keys were extracted or compromised by an adversary. PQ3 is the first large scale cryptographic messaging protocol to introduce this novel post-quantum rekeying property.

PQ3 employs a hybrid design that combines Elliptic Curve cryptography with post-quantum encryption both during the initial key establishment and during rekeying. Thus, the new cryptography is purely additive, and defeating PQ3 security requires defeating both the existing, classical ECC cryptography and the new post-quantum primitives. It also means the protocol benefits from all the experience we accumulated from deploying the ECC protocol and its implementations.

Rekeying in PQ3 involves transmitting fresh public key material in-band with the encrypted messages that devices are exchanging. A new public key based on Elliptic Curve Diffie-Hellman (ECDH) is transmitted inline with every response. The post-quantum key used by PQ3 has a significantly larger wire size than the existing protocol, so to meet our message size requirement we designed the quantum-secure

rekeying to happen periodically rather than with every message. To determine whether a new post-quantum key is transmitted, PQ3 uses a rekeying condition that aims to balance the average size of messages on the wire, preserve the user experience in limited connectivity scenarios, and keep the global volume of messages within the capacity of our server infrastructure. Should the need arise, future software updates can increase the rekeying frequency in a way that's backward-compatible with all devices that support PQ3.

With PQ3, iMessage continues to rely on classical cryptographic algorithms to authenticate the sender and verify the Contact Key Verification account key, because these mechanisms can't be attacked retroactively with future quantum computers. To attempt to insert themselves in the middle of an iMessage conversation, an adversary would require a quantum computer capable of breaking one of the authentication keys before or at the time the communication takes place. In other words, these attacks cannot be performed in a *Harvest Now, Decrypt Later* scenario — they require the existence of a quantum computer capable of performing the attacks contemporaneously with the communication being attacked. We believe any such capability is still many years away, but as the threat of quantum computers evolves, we will continue to assess the need for post-quantum authentication to thwart such attacks.

A formally proven protocol

Our final requirement for iMessage PQ3 is formal verification — a mathematical proof of the intended security properties of the protocol. PQ3 received extensive review from Apple's own multi-disciplinary teams in Security Engineering and Architecture (SEAR) as well as from some of the world's foremost experts in cryptography. This includes a team led by Professor David Basin, head of the Information Security Group at ETH Zürich and one of the inventors of Tamarin — a leading security protocol verification tool that was also used to evaluate PQ3 — as well as Professor Douglas Stebila from the University of Waterloo, who has performed extensive research on post-quantum security for internet protocols. Each took a different but complementary approach, using different mathematical models to demonstrate that as long as the underlying cryptographic algorithms remain secure, so does PQ3. Finally, a leading third-party security consultancy supplemented our internal implementation review with an independent assessment of the PQ3 source code, which found no security issues.

In the first mathematical analysis, Security analysis of the iMessage PQ3 protocol, Professor Douglas Stebila focused on so-called game-based proofs. This technique, also known as reduction, defines a series of "games" or logical statements to show that the protocol is at least as strong as the algorithms that underpin it. Stebila's analysis shows that PQ3 provides confidentiality even in the presence of some key compromises against both classical and quantum adversaries, in both the initial key establishment and the ongoing rekeying phase of the protocol. The analysis decomposes the many layers of key derivations down to the message keys and proves that, for an attacker, they are indistinguishable from random noise. Through an extensive demonstration that considers different attack paths for classical and quantum attackers in the proofs, Stebila shows that the keys used for PQ3 are secure as long as either the Elliptic Curve Diffie-Hellman problem remains hard or the Kyber post-quantum KEM remains secure.

> *The iMessage PQ3 protocol is a well-designed cryptographic protocol for secure messaging that uses state-of-the-art techniques for end-to-end encrypted communication. In my analysis using the reductionist security methodology, I confirmed that the PQ3 protocol provides post-quantum confidentiality, which can give users confidence in the privacy of their communication even in the face of potential improvements in quantum computing technology. —Professor Douglas Stebila*

In the second evaluation, A Formal Analysis of the iMessage PQ3 Messaging Protocol, Prof. David Basin, Felix Linker, and Dr. Ralf Sasse at ETH Zürich use a method called symbolic evaluation. As highlighted in the paper's abstract, this analysis includes a detailed formal model of the iMessage PQ3 protocol, a precise specification of its fine-grained security properties, and machine-checked proofs using the state-of-the-art symbolic Tamarin prover. The evaluation yielded a fine-grained analysis of the secre-

cy properties of PQ3, proving that "in the absence of the sender or recipient being compromised, all keys and messages transmitted are secret" and that "compromises can be tolerated in a well-defined sense where the effect of the compromise on the secrecy of data is limited in time and effect," which confirms that PQ3 meets our goals.

> *We provide a mathematical model of PQ3 as well as prove its secrecy and authenticity properties using a verification tool for machine-checked security proofs. We prove the properties even when the protocol operates in the presence of very strong adversaries who can corrupt parties or possess quantum computers and therefore defeat classical cryptography. PQ3 goes beyond Signal with regards to post-quantum defenses. In PQ3, a post-quantum secure algorithm is part of the ratcheting and used repeatedly, rather than only once in the initialization as in Signal. Our verification provides a very high degree of assurance that the protocol as designed functions securely, even in the post-quantum world. —Professor David Basin*

Diving into the details

Because we know PQ3 will be of intense interest to security researchers and engineers as well as the cryptographic community, this blog post is really two posts in one. Up to now, we laid out our design goals, outlined how PQ3 meets them, and explained how we verified our confidence in the protocol with independent assessments. If you'd like to understand more detail about the cryptographic underpinnings, the remainder of the post is a deeper dive into how we constructed the PQ3 protocol.

Post-quantum key establishment

iMessage allows a user to register multiple devices on the same account. Each device generates its own set of encryption keys, and the private keys are never exported to any external system. The associated public keys are registered with Apple's Identity Directory Service (IDS) to enable users to message each other using a simple identifier: email address or phone number. When a user sends a message from one of their devices, all of their other devices and all of the recipient's devices receive the message. The messages are exchanged through pair-wise sessions established between the sending device and each receiving device. The same message is encrypted successively to each receiving device, with keys uniquely derived for each session. For the rest of this description, we will focus on a single device-to-device session.

Because the receiving device might not be online when the conversation is established, the first message in a session is encrypted using the public encryption keys registered with the IDS server.

Each device with PQ3 registers two public encryption keys and replaces them regularly with fresh ones:

1. A post-quantum **Kyber-1024** key encapsulation public key
2. A classical **P-256 Elliptic Curve** key agreement public key

These encryption keys are signed with ECDSA using a P-256 authentication key generated by the device's Secure Enclave, along with a timestamp used to limit their validity. The device authentication public key is itself signed by the Contact Key Verification account key, along with some attributes such as the supported cryptographic protocol version. This process allows the sender to verify that the recipient device's public encryption keys were uploaded by the intended recipient, and it guards against downgrade attacks.

When Alice's device instantiates a new session with Bob's device, her device queries the IDS server for the key bundle associated with Bob's device. The subset of the key bundle that contains the device's authentication key and versioning information is validated using Contact Key Verification. The device

then validates the signature covering the encryption keys and timestamps, which attests that the keys are valid and have not expired.

Alice's device can then use the two public encryption keys to share two symmetric keys with Bob. The first symmetric key is computed through an ECDH key exchange that combines an ephemeral encryption key from Alice with Bob's registered P-256 public key. The second symmetric key is obtained from a Kyber key encapsulation with Bob's post-quantum public key.

To combine these two symmetric keys, we first extract their entropy by invoking HKDF-SHA384-Extract twice — once for each of the keys. The resulting 48-byte secret is further combined with a domain separation string and session information — which includes the user's identifiers, the public keys used in the key exchange, and the encapsulated secret — by invoking HKDF-SHA384-Extract again to derive the session's initial keying state. This combination ensures that the initial session state cannot be derived without knowing both of the shared secrets, meaning an attacker would need to break both algorithms to recover the resulting secret, thus satisfying our hybrid security requirement.

Post-quantum rekeying

Ongoing rekeying of the cryptographic session is designed such that keys used to encrypt past and future messages cannot be recomputed even by a powerful hypothetical attacker who is able to extract the cryptographic state of the device at a given point in time. The protocol generates a new unique key for each message, which periodically includes new entropy that is not deterministically derived from the current state of the conversation, effectively providing self-healing properties to the protocol. Our rekeying approach is modeled after ratcheting, a technique that consists of deriving a new session key from other keys and ensuring the cryptographic state always moves forward in one direction. PQ3 combines three ratchets to achieve post-quantum encryption.

The first ratchet, called the symmetric ratchet, protects older messages in a conversation to achieve forward secrecy. For every message, we derive a per-message encryption key from the current session key. The current session key itself is then further derived into a new session key, ratcheting the state forward. Each message key is deleted as soon as a corresponding message is decrypted, which prevents older harvested ciphertexts from being decrypted by an adversary who is able to compromise the device at a later time, and provides protection against replayed messages. This process uses 256-bit keys and intermediate values, and HKDF-SHA384 as a derivation function, which provides protection against both classical and quantum computers.

The second ratchet, called the ECDH ratchet, protects future messages by updating the session with fresh entropy from an Elliptic Curve key agreement, ensuring that an adversary loses the ability to decrypt new messages even if they had compromised past session keys — a property called post-compromise security. The ECDH-based ratchet has a symmetrical flow: the private key of the outgoing ratchet public key from the sender is used with the last public key received from the recipient to establish a new shared secret between sender and receiver, which is then mixed into the session's key material. The new PQ3 protocol for iMessage uses NIST P-256 Elliptic Curve keys to perform this ratchet, which imposes only a small 32-byte overhead on each message.

Because the second ratchet uses classical cryptography, PQ3 also adds a conditionally executed Kyber KEM-based ratchet. This third ratchet complements the ECDH-based ratchet to provide post-compromise security against *Harvest Now, Decrypt Later* quantum attacks as well.

The use of a post-quantum ratchet can cause significant network overhead compared to an ECDH-based ratchet at the same security level. The post-quantum KEM requires sending both a public key and an encapsulated secret instead of a single outgoing public key. In addition, the underlying mathematical structure for quantum security requires significantly larger parameter sizes for public keys and encapsu-

lated keys compared to Elliptic Curves.

To limit the size overhead incurred by frequent rekeying while preserving a high level of security, the post-quantum KEM is instantiated with Kyber-768. Unlike the IDS-registered public keys used for the initial key establishment, ratcheting public keys are used only once to encapsulate a shared secret to the receiver, significantly limiting the impact of the compromise of a single key. However, while a 32-byte ECDH-based ratchet overhead is acceptable on every message, the post-quantum KEM ratchet increases the message size by more than 2 kilobytes. To avoid visible delays in message delivery when device connectivity is limited, this ratchet needs to be amortized over multiple messages.

We therefore implemented an adaptive post-quantum rekeying criterion that takes into account the number of outgoing messages, the time elapsed since last rekeying, and current connectivity conditions. At launch, this means the post-quantum ratchet is performed approximately every 50 messages, but the criterion is bounded such that rekeying is always guaranteed to occur at least once every 7 days. And as we mentioned earlier, as the threat of quantum computers and infrastructure capacity evolves over time, future software updates can increase the rekeying frequency while preserving full backward compatibility.

Completing the public key ratchets, whether based on ECDH or Kyber, requires sending and receiving a message. Although users may not immediately reply to a message, iMessage includes encrypted delivery receipts that allow devices to rapidly complete the ratchet even without a reply from the recipient, as long as the device is online. This technique avoids delays in the rekeying process and helps support strong post-compromise recovery.

Similar to the initial session key establishment, the secrets established through the three ratchets are all combined with an evolving session key using HKDF-SHA384 through sequential calls to the Extract function. At the end of this process, we obtain a final message key, which can now be used to encrypt the payload.

Padding and encryption

To avoid leaking information about the message size, PQ3 adds padding to the message before encryption. This padding is implemented with the Padmé heuristic, which specifically limits the information leakage of ciphertexts with maximum length M to a practical optimum of $O(\log \log M)$ bits. This is comparable to padding to a power of two but results in a lower overhead of at most 12 percent and even lower for larger payloads. This approach strikes an excellent balance between privacy and efficiency, and preserves the user experience in limited device connectivity scenarios.

The padded payload is encrypted with AES-CTR using a 256-bit encryption key and initialization vector, both derived from the message key. While public key algorithms require fundamental changes to achieve quantum security, symmetric cryptography algorithms like the AES block cipher only require doubling the key size to maintain their level of security against quantum computers.

Authentication

Each message is individually signed with ECDSA using the elliptic curve P-256 device authentication key protected by the Secure Enclave. The receiving device verifies the mapping between the sender's identifier (email address or phone number) and the public key used for signature verification. If both users have enabled Contact Key Verification and verified each other's account key, the device verifies that the device authentication keys are present in the Key Transparency log and that the corresponding account key matches the account key stored in the user's iCloud Keychain.

The device's authentication key is generated by the Secure Enclave and never exposed to the rest of the

device, which helps prevent extraction of the private key even if the Application Processor is completely compromised. If an attacker were to compromise the Application Processor, they might be able to use the Secure Enclave to sign arbitrary messages. But after the device recovers from the compromise through a reboot or a software update, they would no longer be able to impersonate the user. This approach offers stronger guarantees than other messaging protocols where the authentication key is sometimes shared between devices or where the authentication takes place only at the beginning of the session.

The message signature covers a wide range of fields, including the unique identifiers of the users and their push notification tokens, the encrypted payload, authenticated data, a ratchet-derived message key indicator that binds the signature to a unique location in the ratchet, and any public key information used in the protocol. The inclusion of these fields in the signature guarantees that the message can only be used in the context intended by the sender, and all the fields are exhaustively documented in the research papers from Stebila, Basin, and collaborators.

Conclusion

End-to-end encrypted messaging has seen a tremendous amount of innovation in recent years, including significant advances in post-quantum cryptography from Signal's PQXDH protocol and in key transparency from WhatsApp's Auditable Key Directory. Building on its pioneering legacy as the first widely available messaging app to provide end-to-end encryption by default, iMessage has continued to deliver advanced protections that surpass existing systems. iMessage Contact Key Verification is the most sophisticated key transparency system for messaging deployed at scale, and is the current global state of the art for automatic key verification. And the new PQ3 cryptographic protocol for iMessage combines post-quantum initial key establishment with three ongoing ratchets for self-healing against key compromise, defining the global state of the art for protecting messages against *Harvest Now, Decrypt Later* attacks and future quantum computers.

5.1 Apple Adds Post-Quantum Encryption to iMessage

by Roger Grimes
https://www.linkedin.com/pulse/apple-adds-post-quantum-encryption-imessage-roger-grimes-peh1e/

Apple announced they are adding end-to-end (E2E) post-quantum cryptography (PQC) encryption to iMessage.

Since 1999, the field of quantum computing has continued a steady, consistent, progression to a future world where sufficiently-capable quantum computers will be capable of quickly decrypting secrets protected by much of today's common cryptography (e.g., RSA, Diffie-Hellman, Elliptic Curve Cryptography, etc.). With this knowledge, starting in 2016, the National Institute of Standards and Technology (NIST) announced a multi-year public competition to create or select cryptography that appears to be resistant to quantum-based attacks.

NIST received many dozens of proposed "post-quantum cryptography" algorithms from teams around the world. These initial candidates were removed, combined, and selected to continue competing in additional competitive rounds. In July 2022, NIST selected the first four post-quantum cryptography (PQC) selections:

- CRYSTALS-Kyber (for encryption), and
- CRYSTALS-Dilithium, FALCON and SPHINCS+ (for digital signatures)

Note: NIST is holding additional rounds of PQC competition because three of the currently selected finalists rely upon the same type of mathematical protection (i.e., lattice problems). SPHINCS+ uses a different type of mathematical protection.

Geek Note: Kyber crystals are something invented in Star Wars. Dilithium crystals are something invented in Star Trek. For some unexplained reason, I just love this fact.

It will be another 1-2 years before these four NIST PQC finalists become the codified "official" NIST standards that everyone will need to deploy. But, yes, one day coming soon, EVERYONE will need to update all their software, hardware, and firmware from existing traditional encryption to post-quantum cryptography.

Apple is doing that now with iMessage. It's awesome. It's great.

Apple's iMessage is going to use CRYSTALS-Kyber encryption. You may see it written as Kyber by many writers because it distinguishes it from its similarly named, but different, Dilithium algorithm. Apple is implementing this using its newly named PQ3 post-quantum protocol, which smartly uses a hybrid of conventional cryptography (i.e., Elliptic Curve Cryptography) and CRYSTALS-Kyber.

This is smart because there is some concern that existing PQC may not turn out to be truly resistant to both future quantum and non-quantum attacks. During the NIST contest process, several very promising PQC candidates, two fairly close to being selected as finalists, were revealed not only NOT to be resistant to future quantum attacks, but able to be defeated on slow, old, traditional laptops used today. Some of these "late-breaking" successful encryption attacks have proven that the relatively "quick" review of the NIST PQC candidates may not be enough to ensure future resistance against future cryptography attacks.

So, many proponents of PQC, like Apple, are pairing PQC with traditional cryptography, in what is known as "hybrid" PQC. The theory is that if someone discovers how to break the newly selected PQC, the traditional cryptography will hold (at least until sufficiently-capable quantum computers are in use).

Per Apple: "Support for PQ3 will start to roll out with the public releases of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4, and is already in the corresponding developer preview and beta releases. iMessage conversations between devices that support PQ3 are automatically ramping up to the post-quantum encryption protocol. As we gain operational experience with PQ3 at the massive global scale of iMessage, it will fully replace the existing protocol within all supported conversations this year."

It's very smart that Apple is doing this and I applaud them for it. No one knows when your adversaries will get sufficiently-capable quantum computers that can crack today's cryptography. It could even already be done and being used by today's major quantum nation-states (e.g., the US and China) and we just don't know about. But most quantum observers think that the "quantum crack" will happen sometime between now and the next 10 years. It could happen any day now.

Even if we don't have any sufficiently-capable quantum computers, the world's adversaries are already collecting data that is currently protected by quantum-susceptible cryptography to have the capability to decipher it when they do get sufficiently-capable quantum computers. If you have secrets you need to protect going forward and suspect an adversary could be eavesdropping on your currently encrypted data, you should be thinking about PQC (and other protections).

This should serve as another wake-up call for everyone to start actively preparing for the post-quantum

world, where most traditional cryptography may need to be updated or replaced. If you are involved in organizational cybersecurity, you need to be creating a Post-Quantum project and start, NOW, preparing. You can read and use the guidance published in this guide from the Cloud Security Alliance, Practical Preparations in a Post-Quantum World, which I helped author.

If you're interested in more information about the post-quantum world, quantum, quantum computers, and post-quantum protections, I wrote a book on it: Cryptography Apocalypse: Preparing for the Day When Quantum Computing Breaks Today's Crypto.

Kudos to Apple for doing end-to-end, PQC, in their iMessage application. I'm sure they will be quickly extending it across their ecosystem. Other major vendors will be quickly following. And we all will be following and updating every device and software app we use within a few years. Don't let it be a surprise where you're having to come up to speed in the heat of the moment.

6.ETSI releases world's first Protection Profile for QKD

by IDQ
https://www.idquantique.com/etsi-releases-qkd-protection-profile/?utm_term=ETSI%20releases%20-World%20First%20Protection%20Profile%20for%20Quantum%20Key%20Distribution&utm_campaign=Quantum%20Era%20Security%20Times%3A%20February%202024&utm_content=email&utm_source=Act-On+Software&utm_medium=email&cm_mmc=Act-On%20Software-_-email-_-Quantum%20Era%20Security%20Times%3A%20February%202024-_-ETSI%20releases%20World%20First%20Protection%20Profile%20for%20Quantum%20Key%20Distribution

In September of 2023 we provided an update on ETSI's progress towards the development of standards for QKD systems. A few months on and we are delighted to say the ETSI Group Specification GS QKD 016 Protection Profile Standard has been published and validated.

This constitutes a major milestone on the path to the certification of QKD products. The Protection Profile was developed within the framework of the ETSI Industry Specification Group ISG-QKD, to which ID Quantique has contributed since its inception in 2008. The Protection Profile has subsequently been fully validated by the SGS evaluation lab in Graz, and the evaluation has been certified by the German certification body BSI.

Common Criteria and the GS QKD 016

Security evaluation and certification is globally recognised as a prerequisite for qualified deployment in real-world applications. It is the only objective way for customers with limited expertise to assess the security credentials of complex QKD solutions. However, effective evaluation becomes difficult if there isn't an agreed set of standards against which to benchmark security performance.

Common Criteria defines the procedures and elements required for standardisation, including:

- characterization of the optical components used
- protocols and algorithms
- implementation security against particular attacks

- generic security requirements

As the QKD market matures, government customers within Europe will require solutions evaluated to the established Common Criteria for Information Technology Security Evaluation (ISO/IEC/EN 15408). Specific use cases for dedicated industry applications may also require unique security requirements, against which QKD solutions will need to be evaluated.

The GS QKD 016 standard represents a significant milestone in this respect. There is still work to do, with quantum optical evaluation labs still in development – a final phase being managed by the EC project team "Nostradamus", led by Deutsche Telekom.

ID Quantique, in the meantime is ensuring that its own internal processes are "Common Criteria ready". This is further evidence of our commitment to standardisation and will help streamline product evaluation once final criteria will have been established.

Global efforts towards standardization

In addition to the ETSI group, several standardisation bodies are also working on QKD.

The CEN/CENELEC Focus Group on Quantum Technologies (FGQT) was established in 2020 and its goal was to prepare European standardisation of Quantum Technologies. In March 2023 its successor, the new joint technical committee JTC22 was founded in CEN/CENELEC, dedicated to the development of standards for European industry and research. The European Commission continues to publish rolling plans for ICT standardisation, including RP2023 for Quantum Technologies.

Elsewhere, the International Telecommunication Union (ITU) is undertaking its own standardisation efforts, with an active work programme: Framework of quantum key distribution protocols in QKD networks. Contributing members of the ITU work group include: The Centre for Quantum Technologies (CQT) in Singapore, the Infocomm Media Development Authority (IMDA), SK Telecom, ID Quantique, the National Institute of Information and Communication (NICT) and the National University of Singapore. With both ISO and IEC pursuing their own standardisation efforts, 2024 is likely to be a landmark year in the development of quantum technology standards.

In parallel, ID Quantique is in the middle of an evaluation process of its QKD products and related key management systems in countries such as South Korea, with the Korean National Security Research Institute (NSRI). It is currently undergoing intensive testing of its optic properties through the Korea Research Institute of Standards and Science (KRISS) to satisfy the preliminary conditions before the evaluation process. In 2022 in Korea, IDQ installed a QKD network connecting 48 government organizations with its partner SK Broadband.

7.Quantum computers can still be beaten by traditional PCs with new method

by Christopher McFadden
https://interestingengineering.com/innovation/classical-pcs-can-rival-quantum-ones

Researchers from New York University (NYU) have discovered that classical computers can, in some circumstances, keep up with, or even surpass, quantum computers. They found that by adopting a new innovative algorithmic method, classical computers can get a much-needed boost in speed and accura-

cy, which could mean that they still have a future should quantum computers ever take off.

Many experts believe that quantum computing represents a paradigm shift from classical computing. This is primarily because classical computers, as you are aware, process information using digital bits (0s and 1s), while quantum computers use quantum bits (qubits) to store information in values between 0 and 1.

This ability, so the story goes, enables quantum computers to process and store information in qubits and allows quantum algorithms to outperform classical counterparts. Additionally, quantum computers store information in values between 0 and 1, making it difficult for classical computers to imitate quantum ones perfectly.

However, as it turns out, quantum computers are delicate and prone to information loss. Furthermore, even if information is preserved, converting it to classical information necessary for practical computation isn't easy.

There is hope for classical computers yet

Classical computers, conversely, don't suffer from the problems of information loss and translation that quantum computers do. Additionally, classical algorithms can be designed to take advantage of these challenges and simulate a quantum computer with far fewer resources than previously believed, as explained in a recent research paper published in PRX Quantum.

The study's results indicate that classical computing can perform faster and more accurate calculations than state-of-the-art quantum computers. This breakthrough was achieved with an algorithm that keeps only part of the information stored in the quantum state—and just enough to compute the outcome accurately.

“This work shows that there are many potential routes to improving computations, encompassing both classical and quantum approaches,” explains Dries Sels, an assistant professor in New York University’s Department of Physics and one of the paper’s authors. “Moreover, our work highlights how difficult it is to achieve quantum advantage with an error-prone quantum computer," he added.

To this end, Sels and his colleagues focused on a tensor network, which is believed to represent the interactions between qubits accurately. These networks have been challenging to work with, but recent advancements in the field now allow these networks to be optimized using tools borrowed from statistical inference.

Tensor networks are an old PC's best friend

But, the new method focuses only on the most important pieces of information and ignores the rest, like when you compress a photo to make it smaller without losing the quality that matters to you. This method lets regular computers do some cool stuff quantum computers can do without all the fuss.

The researchers compare their method to compressing a photo into a JPEG file. Just like compressing a photo reduces its file size without making it incomprehensible. To this end, their technique simplifies the quantum computing problem so that a regular computer can handle it more efficiently.

“Choosing different structures for the tensor network corresponds to choosing different forms of compression, like different formats for your image,” says the Flatiron Institute’s Joseph Tindall, who led the project. “We are successfully developing tools for working with a wide range of different tensor networks. This work reflects that, and we are confident that we will soon be raising the bar for quantum computing even further.”

8.Quantum vs. Classical Computing: The Tug of War Continues

by Anthony Raphael
https://medriva.com/breaking-news/quantum-vs-classical-computing-the-tug-of-war-continues/

In the world of computational sciences, the dominance of quantum computing has been largely uncontested, primarily due to its touted speed and memory usage enhancements. Quantum computers, employing the principles of quantum mechanics such as superposition and entanglement, are known to outperform classical computers in certain tasks. However, recent research suggests that the reign of quantum computing might not be as secure as previously thought, as classical computing has managed to not only match but surpass the performance of state-of-the-art quantum machines.

Classical Computing Strikes Back

Recent findings have established that with a strategic approach and the right algorithm, classical computing can display superior performance to cutting-edge quantum machines. The secret to this breakthrough lies in an algorithm that selectively maintains quantum information, retaining just enough to accurately predict outcomes. This is somewhat akin to compressing an image into a JPEG file, where only essential information is kept.

The research team ventured into enhancing classical computing by focusing on tensor networks, which effectively represent qubit interactions. Advanced techniques adapted from statistical inference have been employed to optimize these networks, leading to a significant improvement in computational efficiency.

Quantum Computing: A Double-edged Sword

While quantum computing has the potential to revolutionize our information processing systems and solve complex problems, achieving a quantum advantage with an error-prone quantum computer is challenging. Quantum systems require qubits to be maintained in a coherent state to function efficiently, which is a considerable task. Moreover, scaling quantum systems is another hurdle that researchers across the globe are trying to overcome.

Despite these challenges, the field of quantum computing is rapidly advancing due to investments from major technology companies, research institutions, and governments worldwide. Quantum computing is anticipated to have a profound impact on various industries, enhancing our capabilities in areas such as cryptography, materials science, and artificial intelligence, among others.

Quantum Internet: A Step Closer to Reality

Parallel to the advancements in quantum computing, efforts are also being made to develop a quantum internet. A team of physicists at Stony Brook University made significant progress in building a quantum internet testbed by demonstrating a foundational quantum network measurement using room temperature quantum memories.

This achievement is a major leap towards developing a quantum internet, which is expected to enhance the internet system as we know it and provide certain services and securities that the current internet

does not have. The quantum hardware developed by the team operates at room temperature, significantly reducing the cost of operation and making the system much faster.

In conclusion, the race between classical and quantum computing continues to be an exhilarating one. With each making significant strides, it's a testament to the rapid pace of research and innovation in the field of computational sciences. Whether quantum will eventually take the reins, or classical will continue to surprise us with its resilience, the possibilities are indeed exciting.

9.The State of the Art in Quantum Computing

by Núria Costa
https://medium.com/edge-elections/the-state-of-the-art-in-quantum-computing-cffd654c363f

Quantum computing is a technology that exploits the laws of quantum mechanics to solve problems too complex for classical computers. The first significant contribution to the development of quantum computing occurred in 1982, when Richard Feynman postulated that to simulate the evolution of quantum systems in an efficient way, we would need to build quantum computers (computational machines that use quantum effects). Nevertheless, it was not until 1994 that the view on quantum computing changed. Peter Shor developed a polynomial time quantum algorithm allowing quantum computers to efficiently factorize large integers exponentially quicker than the best classical algorithm on traditional machines, turning a problem which is computationally intractable into one that can be solved in just a few hours by a large enough quantum computer. So, once practical quantum computers are a reality, it will be possible to crack cryptographic algorithms based on integer factorization, such as RSA, which are fundamental for the operation of internet protocols.

But what do we mean by "a large enough quantum computer"? How far are we from building it?

Large technology companies have been working for years with the objective of building a large-scale quantum device. As published by the Quantum Insider, the leading players in this field are Google, IBM, Microsoft and AWS (Amazon), although IBM has the longest computing history.

Apart from them, there are other promising companies which are also invested in fabricating quantum hardware and developing software. Some examples are D-Wave, Rigetti Computing, IonQ, PsiQuantum, Quantiuum or Oxford Ionics. It is worth noting that not all of them are working on the same type of quantum computers. Differences among these computers depend on the nature of qubits and how they can be controlled and manipulated. The main types of quantum computers are superconducting, photonic, neutral atoms-based, trapped ions, quantum dots and gate-based quantum computers, the first being the most mature and popular type.

IBM

In 2016, IBM put the first quantum computer on the cloud for anyone to run experiments (the IBM Quantum Experience). One year later, they introduced Qiskit, the open-source python-based toolkit for programming these quantum computers (the version 1.0 will be released this year). Then, in subsequent years, the company developed Falcon, a 27-qubit quantum computer (2018) and the 65-qubit Hummingbird (2020). Also, in 2020, IBM released their development roadmap, which had a major update in

2022 and provides a detailed plan to build an error-corrected quantum computer before the end of the decade. According to this roadmap, IBM was planning to build in 2021 the first quantum processor with more than 100 qubits, the 127 qubit Eagle; in 2022, the 433-qubit Osprey; and finally, in 2023, the 1121-qubit Condor processor. All objectives were successfully achieved. Nevertheless, as Jay Gambetta, VP of IBM Quantum, mentioned in his article, we must figure out how to **scale** up quantum processors since a quantum computer capable of reaching its full potential could require hundreds of thousands, maybe millions of high-quality qubits. For this reason, in the following years and with the ambition of solving the **scaling**[1] problem, the company is proposing three different approaches for "developing ways to link processors together into a modular system capable of scaling without physics limitations'".

Google

Another tech giant working on quantum computing is Google, which has the Quantum AI Campus. This company announced in 2018 a 72-qubit quantum processor called Bristlecone and in 2019 presented a 53-qubit quantum computer, Sycamore, and claimed **quantum supremacy**[2] for the first time, which generated a lot of debate in the community. Lastly, the Quantum AI researchers announced significant advances in quantum error correction by achieving for the first time the experimental milestone of scaling a logical qubit. Quantum error correction is essential for scaling up quantum computers and achieving error rates low enough for useful calculations.

Microsoft

Microsoft decided to focus on quantum computing in the late 1990s and currently is offering Azure Quantum, a cloud quantum computing service which provides an environment to develop quantum algorithms which can be run in simulators of quantum computers. Due to the company's approach of working with partners and academic institutions, Azure Quantum allows us to choose from different quantum hardware solutions created by industry leaders such as Quantinuum, Ionq, Quantum Circuits, Inc., Rigetti or Pasqal.

Microsoft is taking a different approach on the design of quantum computers — they are relying on a new type of qubit, a topological qubit. As they explicitly say, "Our approach to building a scaled quantum machine is the more challenging path in the near term, but it's the most promising one long term". In this regard, in 2022, Microsoft reported an important achievement on the development topological qubit hardware, and later that year they share more data from their experiments.

Amazon

Although Amazon has not announced that it is developing quantum hardware and/or software, they launched in 2019 Amazon Braket, a quantum computing service which makes it possible to build quantum algorithms, test them in a simulator, run them on different quantum computers and analyze the results. Customers can access hardware from leaders such as Rigetti, Ion-Q and D-Wave Systems, which means that they can experiment with systems based on three different qubit technologies.

In addition, Amazon also launched the Amazon Quantum Solutions Lab which helps companies to be ready for quantum computing by offering them the possibility "to work with leading experts in quantum computing, machine learning, optimization, and high-performance computing".

There are many companies working hard on building quantum hardware and software, each of them fol-

[1] **Scalability** refers to the ability to increase the number of qubits in a quantum system, allowing to solve more complex problems.

[2] **Quantum supremacy** describes the ability of a quantum computer for solving a problem that the most powerful conventional computer cannot process in a practical amount of time.

lowing their own roadmap and investing in the technology they consider to be most promising. Nevertheless, all of them have the same goal in mind: quantum computing at scale.

John Preskill, a theoretical physicist and expert on quantum computing and quantum error correction, in response to the question "How long do we have to wait? One year? 10 years? 100 years?", answered the following:

"Well, it depends on what you want. We're at a very early stage of the development of quantum computers, but even now, from a scientific perspective, the quantum computers we already have are empowering. They enable us to explore the behavior of complex quantum systems in ways that we've never been able to before, and that will fuel scientific discovery over the next five or 10 years. But for widespread practical impact, I think a reasonable estimate is decades, or more than 10 years."

And finally, what about prime factorization? Should we worry about sending an e-mail, making an online purchase, or authenticating ourselves in an online platform? Recent estimates by researchers at Google, the KTH Royal Institute of Technology and the Swedish NCSA, find that roughly 20 million 'reasonably good' physical qubits will be required to factor a 2048-bit number in 8 hours. We are not there yet, but it is clear that we should be prepared for the future threat.

10.A Look at D-Wave's Progress and Future Roadmap

by GQI
https://quantumcomputingreport.com/a-look-at-d-waves-progress-and-future-roadmap/

D-Wave Quantum Inc. was the first commercial company to enter the quantum computing market. The company was founded in 1999 and developed their first commercial product, a 128 qubit quantum annealing processor called the D-Wave One in 2011. The *Quantum Computing Report* published our first report about them in August 2015 with the announcement of the D-Wave 2X. Their forthcoming quantum processor, called Advantage2, will be D-Wave's sixth generation processor. They are also currently developing a gate-based fluxonium processor to provide a solution path for some applications that cannot use a quantum annealer. D-Wave is now a public company after completing a SPAC merger in August 2022. In this article we will take a look at their overall strategy, roadmap, and progress, both technically and commercially, to provide an update on the company.

Commercial Progress

We talk about Quantum Advantage often in these pages, but there is actual something even more important which I will call Quantum Production Revenue. After all, governments and venture capitalists are investing billions into quantum companies and they would certainly like to see a return on their investment in the form of commercial revenue. And what they want to see is something more than the occasional runs to demonstrate a Proof-of-Concept (POC) or to test out a new algorithm. They want to see end users using quantum in regular production usage for recurring revenue.

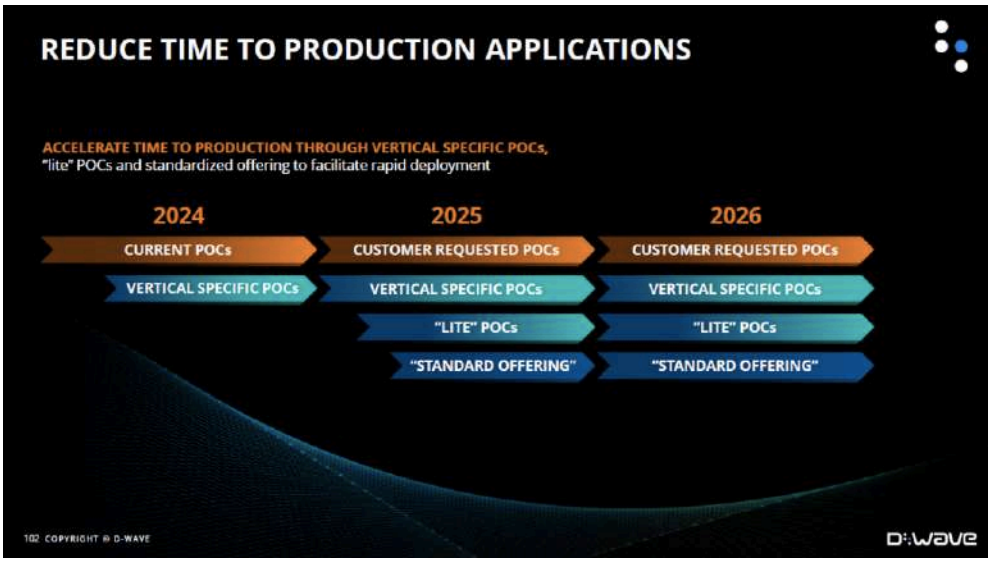
Some theorists will opine that a quantum annealing technology will not be able to surpass the best classical approaches. As expected, D-Wave does not quite agree and points to a recent paper published in *Nature* titled Quantum critical dynamics in a 5,000-qubit programmable spin glass as evidence that their quantum annealing processor can be significant faster that classical approaches for certain 3D spin glass optimization problems. But, more importantly, enterprise IT managers and corporate data analysts

may not always choose a solution on what is theoretically the best, but what solution is the easiest to implement. D-Wave has several pieces of software and services will do this which will give them an advantage over other quantum hardware providers who have yet to do this. Perhaps highly quantum savvy PhDs and Postdocs who can do it themselves won't need these tools. But for someone working within a commercial organization looking to achieve quick results, these tools can be very helpful.

In a recent presentation, D-Wave has disclosed that they have several dozen customer currently working with to explore using their annealers, 26 are developing proof-of-concepts, and two customers, the Pattison Food Group and Satispay, that have completed the proof-of-concepts and are now starting production. In addition, the company indicated that will have additional customers moving from POC to production in the next two quarters. D-Wave asserts that they are the only quantum company that has customers who have progressed to this level.

Software and Services

One important piece of technology that D-Wave has developed and enhanced over the years include their Solvers. This is software that allows a problem to be inputted at a high level as a quadratic model and the software will compile it to a hardware configuration that can run on the quantum annealer. Their original solver only allowed variables in the Binary Quadratic Model (BQM) to be specified as a 0 or 1. But over the years, the company has extended their solver to handle Discrete Quantum Models (DQM) and later a Constrained Quadratic Model (CQM) which can handle continuous variables as well as constraints. D-Wave has a next generation solver in development that will be released later this year that will provide even more improved performance for a growing set of use cases (see chart below). The company has also continued to improve its Ocean software which provides tools for software development in a hybrid quantum/classical environment. And their Leap Quantum Cloud Service provides real-time and secure cloud access to quantum computers and hybrid solvers



D-Wave positions themselves as a company that can provide practical quantum computing today and has a focus on landing new customers and moving them to production as quickly as possible. To that end, they previously established a Professional Services group that can provide assistance at a different levels to help customers from problem discovery, proof-of-concept, pilot production, and/or achieving full production. As part of D-Wave's thrust to accelerate customer's time to market, they are developing a series of POCs and standard offerings that customers may be able to start with and modify for their own use case. This would result in the customers getting into production much faster than having to

formulate a problem from scratch. D-Wave's roadmap for creating vertical specific POCs and standardized offerings is shown below:

One additional thing that is often overlooked when assessing quantum companies is that production users need real-time access to the quantum systems in order to get timely solutions to meet their schedules. It may be OK for a student to have a job wait in a queue for a few hours before their job can run, but that would be unacceptable for most production applications. D-Wave has put on focus on providing this as well as high levels of reliability and availability so that their production users can get their work done without delay.

Sales and Marketing

D-Wave's management has made some adjustments in their sales and marketing approach in order to increase the company's business development efforts. The first is to focus on the Manufacturing and Logistics verticals. Many of their current customers working on POCs come from these domains and use cases in these domains are a good fit with the inherent strength of their annealing technology to solve scheduling and optimization related problems. The company is also working to bring in more sales resources who are familiar with these industries and also recruit partners who can develop business for them and support additional enterprise customers.

Another area that will get increased focus from D-Wave is government sales. D-Wave currently has minimal sales to the government sector, but they were recently encouraged to see that the recent National Defense Authorization Act (NDAA) signed in December 2023 specifically calls out quantum annealing as a technology that should be evaluated for defense purposes. They will be pursuing more government sales and grants.

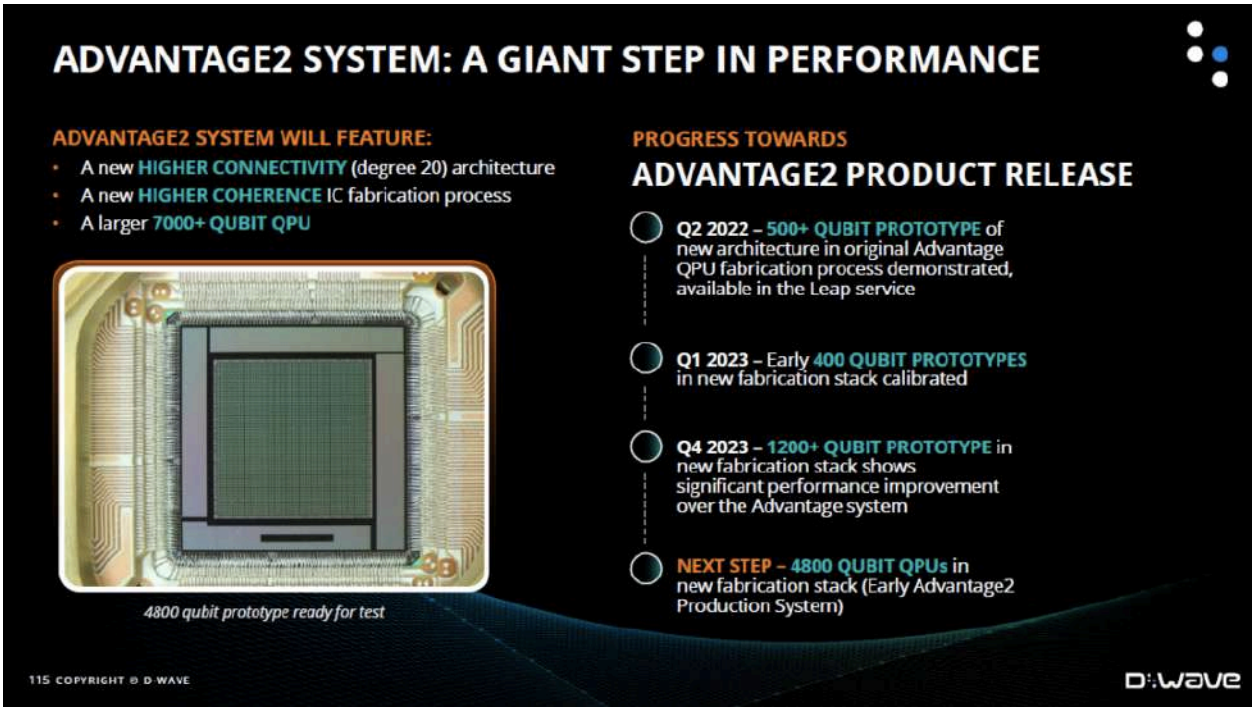
Hardware Technology

Last, but not least, D-Wave is continuing to advance both their annealing and gate-based hardware efforts. The company has been working on a successor to their current Advantage product that they are calling Advantage2. It will have over 7,000 qubits and have significant improvements in connectivity (from 15 to 20), coherence, and performance. They have been building prototype technology demonstrators of increasing size and have recently announced a 1200+ qubit version of Advantage2 that they will be making publicly available. They will also be using this demonstrator to test out some error mitigation technology they recently announced. The next version is a 4800+ qubit Advantage2 demonstrator that will be built in a new and improved production stack for further improvements. Finally, the full 7000 qubit version is expected to be released by 2025. Moving beyond the Advantage2, the company's roadmap shows an Advantage2 Performance Update annealer in 2026 and an Advantage3 annealer in 2028 that will incorporate additional features.

As we previously reported on these pages, D-Wave also has a development effort to create a gate-based processor. Once that is released, D-Wave would be the only company to provide both annealing and gate-based solutions which they feel will put them at an advantage. Their goal is to develop a superconducting based machine using fluxonium qubits that includes error correction. It is still several years away but the company is continuing to make progress. D-Wave released some encouraging results from a test chip last September. They recognize that a quantum annealer cannot cover all the potential quantum computing applications but adding a gate based machine will allow them to cover all of them. A key point the company has made is that there is a lot of common technology between quantum annealers and gate-based quantum processor. This includes superconducting qubits, fabrication, control electronics, cryogenics, and other things which will give them a head start in their development program.

D-Wave also has a very extensive patent portfolio that covers over 500 granted and pending patents worldwide covering hardware, software, applications, and other related areas. The company estimates

that about 60% of the portfolio is applicable to both annealing and gate-based processors.



Conclusion

D-Wave is advancing on several fronts including hardware, software, and customer engagement. The chart below provided by the company shows a summary of some of their efforts. The currently stand alone as the only commercial provider of annealing systems, but there are other groups researching this area. There are also other groups looking at other approaches for efficiently solving optimization problems. But D-Wave has been working on this for a long time and possess a great deal of technology and has engaged with a significant number of customers. Once many of the customers working on POCs finish them and move into production, D-Wave should be able enjoy increases in revenue that will start to make their many years of investments start to pay off.

11.The Linux Foundation and its partners are working on cryptography for the post-quantum world

by Steven Vaughan-Nichols
https://www.zdnet.com/article/cryptography-for-the-post-quantum-world/

We know the end of the line is in sight for classical cryptography. All the security encryption that protects our bank accounts, websites, and credit cards today will eventually be broken. That's not just a threat; that's the reality.

When Q-Day comes, which is the day quantum computers can break our existing encryption methods, we'll need a replacement for Advanced Encryption Standard (AES), RSA, and Blowfish. That's why the Linux Foundation and others have united behind the Post-Quantum Cryptography Alliance (PQCA).

It's also important to note that Bitcoin and other cryptocurrencies will be broken, too. As the Katten law firm's Daniel Davis and Alexander Kim recently observed: "Quantum computers have the potential to break the most advanced cryptographic protocols -- including those used for blockchain protocols -- in operation today."

PQCA is meant to galvanize the development and widespread adoption of post-quantum cryptography. These new crypto algorithms will be able to resist quantum computers' efforts to break them. PQCA is a collaborative platform, uniting the brightest minds from industry giants, academia, and the developer community to tackle the cryptographic challenges of the quantum age.

Leading the charge are founding members, such as tech behemoths Amazon Web Services (AWS), Cisco, Google, and IBM. Their collective expertise and resources are poised to propel the PQCA's mission to secure sensitive data and communication in the post-quantum world.

Jim Zemlin, the Linux Foundation's executive director, said: "By establishing an open and collaborative environment for innovation, the PQCA will help accelerate the development and adoption of post-quantum cryptography in open source and beyond."

Yet the great minds in PCQA aren't the only experts focused on this crucial area. The National Institute of Standards and Technology (NIST) is already working on four quantum-proof crypto algorithms:

- CRYSTALS-Kyber is designed for general encryption purposes, such as creating secure websites.
- CRYSTALS-Dilithium is designed to protect the digital signatures we use when signing documents remotely.
- SPHINCS+ is also designed for digital signatures.
- FALCON is another, less mature, algorithm for digital signatures.

The work from PQCA will be the central foundation for organizations and open-source projects seeking production-ready libraries and packages to support these quantum-proof algorithms and the U.S. National Security Agency's Cybersecurity Advisory concerning the Commercial National Security Algorithm Suite 2.0.

Part of PQCA's mission is its commitment to the practical application of post-quantum cryptography. The alliance will spearhead technical projects, such as developing software for evaluating, prototyping, and deploying new post-quantum algorithms. In other words, the alliance seeks to bridge the gap between theoretical cryptography and its real-world implementation.

One of PQCA's launch projects is the Open Quantum Safe project, which was founded at the University of Waterloo in 2014 and is one of the world's leading open-source software initiatives devoted to post-quantum cryptography.

PQCA will also host the new PQ Code Package Project, which will build high-assurance, production-ready software implementations of forthcoming post-quantum cryptography standards, starting with the ML-KEM algorithm.

All this effort matters because quantum computing is very much a mixed blessing. As Jon Felten, Cisco Systems' senior director of trustworthy technologies, said: "Quantum computing offers the potential to

solve previously unapproachable problems, while simultaneously threatening many digital protections we take for granted."

This "transition to Quantum-Resistant standards, algorithms, and protocols will undoubtedly be a challenging one," said Ted Shorter, CTO of Keyfactor. What's already clear is that we're entering a new era of computing. We won't know how effective our preparations will be until quantum computers have enough qubits to crack our existing encrypted data.

The level of progress is such that IBM recently released the first 1,000-qubit chip. That level of performance isn't enough to reach Q-Day. However, it's a moment that isn't too far from being realized.

12.IBM: Enabling a quantum-safe environment

by Marlet Salazar
https://backendnews.net/ibm-enabling-a-quantum-safe-environment/

During a media briefing addressing the challenges of the quantum era hosted by technology giant IBM, subject matter experts (SMEs) in quantum computing highlighted strategies for addressing concerns about its impact on encryption.

Quantum computing is making great strides faster than expected. In fact, the optimism surrounding its use cases and how it could help solve real-world problems can be quite infectious.

"Many customers and users out there have been asking whether quantum computing, which has been steadily developing, comes with risks," said Ray Harishankar, IBM Fellow, IBM Quantum Safe. "As quantum computing progresses, one area of concern is prime number factorization, which poses a risk to today's encryption methods."

Harishankar explained how prime factorization, while extremely helpful in quantum computing, could be potentially a risk to data security. The ability of quantum computers to find factors of massive numbers is crucial for many encryption methods used today to keep information safe.

Regular (or classic) computers struggle with prime factorization because it is incredibly complex. But quantum computers, with their special abilities, can solve this problem much faster. Shor's algorithm can do that when run on a quantum computer and can crack these codes.

Harishankar further explained that security protocols most organizations rely on today, also rely upon the idea that prime factorization is too hard for computers to solve quickly.

"Q-day"

"But if quantum computers become powerful enough to crack these codes, it could potentially put our sensitive information at risk," he said.

The Reuters special report titled "U.S. and China race to shield secrets from quantum computers" explored concerns surrounding "Q-Day," the hypothetical day when quantum computers decode encryption, rendering it ineffective.

“Securing today’s data against the future risks posed by quantum computing needs to begin now,” Harishankar said.

He also emphasized the importance of initiating education for both customers and researchers without delay.

IBM Quantum Safe

In 2016, the NIST assessed 69 cryptographic schemes for potential standardization and chose four finalists: for public key encryption and for digital signatures. After a rigorous selection process of algorithms submitted, the US National Institute of Standards and Technology (NIST) has chosen cryptographic tools that can possibly block quantum computers in 2022. These cryptographic tools — Dilithium, Crystals, Falcon, and Kyber — are available on the IBM z16 mainframe.

IBM has developed the IBM Quantum Safe technology, which is a comprehensive set of tools, capabilities, and approaches for securing enterprises in preparation for the quantum future and ensuring data security.

In its experience with working with clients, IBM recognized the critical need to address cryptography-related issues, with discovery being the initial step. Uncovering such issues can be daunting, even for large enterprises. Once this hurdle is overcome, the subsequent steps become more manageable.

“We believe that the time to start is now,” emphasized Harishankar. “Enterprises need to begin to understand and create an inventory of their cryptography usage across the organization.”

With a comprehensive understanding, securing these assets can be achieved incrementally and systematically. Prioritizing the protection of the most valuable, vulnerable, or critical systems is key.

13.Introducing Adiantum: Encryption for the Next Billion Users

by Paul Crowley and Eric Biggers
https://security.googleblog.com/2019/02/introducing-adiantum-encryption-for.html

Storage encryption protects your data if your phone falls into someone else's hands. Adiantum is an innovation in cryptography designed to make storage encryption more efficient for devices without cryptographic acceleration, to ensure that *all* devices can be encrypted.

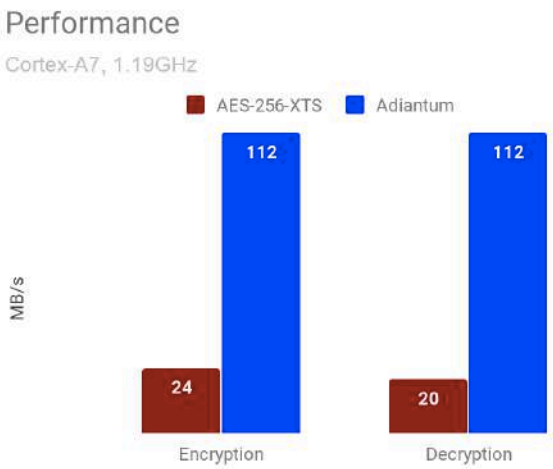
Today, Android offers storage encryption using the Advanced Encryption Standard (AES). Most new Android devices have hardware support for AES via the ARMv8 Cryptography Extensions. However, Android runs on a wide range of devices. This includes not just the latest flagship and mid-range phones, but also entry-level Android Go phones sold primarily in developing countries, along with smart watches and TVs. In order to offer low cost options, device manufacturers sometimes use low-end processors such as the ARM Cortex-A7, which does not have hardware support for AES. On these devices, AES is so slow that it would result in a poor user experience; apps would take much longer to launch, and the device would generally feel much slower. So while storage encryption has been required for most devices since Android 6.0 in 2015, devices with poor AES performance (50 MiB/s and below) are exempt. We've been working to change this because we believe that encryption is for everyone.

In HTTPS encryption, this is a solved problem. The ChaCha20 stream cipher is much faster than AES when hardware acceleration is unavailable, while also being extremely secure. It is fast because it exclusively relies on operations that all CPUs natively support: additions, rotations, and XORs. For this reason, in 2014 Google selected ChaCha20 along with the Poly1305 authenticator, which is also fast in software, for a new TLS cipher suite to secure HTTPS internet connections. ChaCha20-Poly1305 has been standardized as RFC7539, and it greatly improves HTTPS performance on devices that lack AES instructions.

However, disk and file encryption present a special challenge. Data on storage devices is organized into "sectors" which today are typically 4096 bytes. When the filesystem makes a request to the device to read or write a sector, the encryption layer intercepts that request and converts between plaintext and ciphertext. This means that we must convert between a 4096-byte plaintext and a 4096-byte ciphertext. But to use RFC7539, the ciphertext must be slightly larger than the plaintext; a little space is needed for the cryptographic nonce and message integrity information. There are software techniques for finding places to store this extra information, but they reduce efficiency and can impose significant complexity on filesystem design.

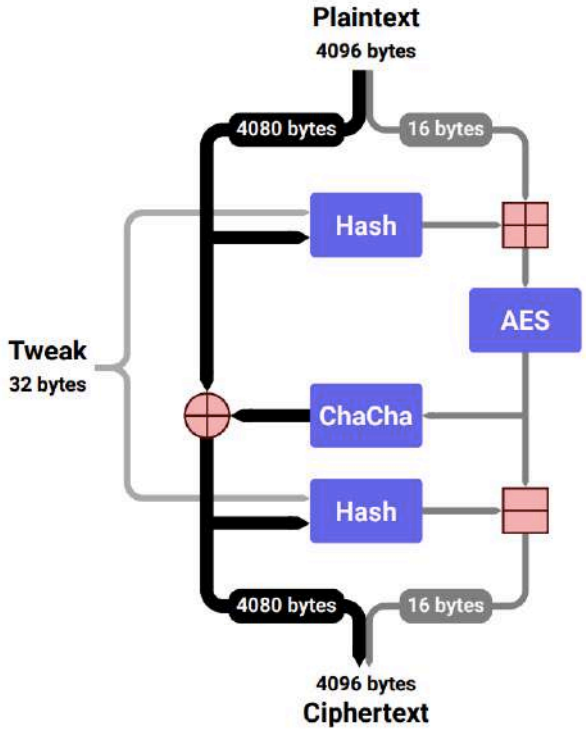
Where AES is used, the conventional solution for disk encryption is to use the XTS or CBC-ESSIV modes of operation, which are length-preserving. Currently Android supports AES-128-CBC-ESSIV for full-disk encryption and AES-256-XTS for file-based encryption. However, when AES performance is insufficient there is no widely accepted alternative that has sufficient performance on lower-end ARM processors.

To solve this problem, we have designed a new encryption mode called Adiantum. Adiantum allows us to use the ChaCha stream cipher in a length-preserving mode, by adapting ideas from AES-based proposals for length-preserving encryption such as HCTR and HCH. On ARM Cortex-A7, Adiantum encryption and decryption on 4096-byte sectors is about 10.6 cycles per byte, around 5x faster than AES-256-XTS.



Unlike modes such as XTS or CBC-ESSIV, Adiantum is a true wide-block mode: changing any bit anywhere in the plaintext will unrecognizably change all of the ciphertext, and vice versa. It works by first hashing almost the entire plaintext using a keyed hash based on Poly1305 and another very fast keyed hashing function called NH. We also hash a value called the "tweak" which is used to ensure that different sectors are encrypted differently. This hash is then used to generate a nonce for the ChaCha encryption. After encryption, we hash again, so that we have the same strength in the decryption direction as the encryption direction. This is arranged in a configuration known as a Feistel network, so that we can decrypt what we've encrypted. A single AES-256 invocation on a 16-byte block is also required, but for

4096-byte inputs this part is not performance-critical.



Cryptographic primitives like ChaCha are organized in "rounds", with each round increasing our confidence in security at a cost in speed. To make disk encryption fast enough on the widest range of devices, we've opted to use the 12-round variant of ChaCha rather than the more widely used 20-round variant. Each round vastly increases the difficulty of attack; the 7-round variant was broken in 2008, and though many papers have improved on this attack, no attack on 8 rounds is known today. This ratio of rounds used to rounds broken today is actually better for ChaCha12 than it is for AES-256.

Even though Adiantum is very new, we are in a position to have high confidence in its security. In our paper, we prove that it has good security properties, under the assumption that ChaCha12 and AES-256 are secure. This is standard practice in cryptography; from "primitives" like ChaCha and AES, we build "constructions" like XTS, GCM, or Adiantum. Very often we can offer strong arguments but not a proof that the primitives are secure, while we can prove that if the primitives are secure, the constructions we build from them are too. We don't have to make assumptions about NH or the Poly1305 hash function; these are proven to have the cryptographic property ("ε-almost-Δ-universality") we rely on.

Adiantum is named after the genus of the maidenhair fern, which in the Victorian language of flowers (floriography) represents sincerity and discretion.

Additional resources

The full details of our design, and the proof of security, are in our paper *Adiantum: length-preserving encryption for entry-level processors* in IACR Transactions on Symmetric Cryptology; this will be presented at the Fast Software Encryption conference (FSE 2019) in March.

Generic and ARM-optimized implementations of Adiantum are available in the Android common kernels v4.9 and higher, and in the mainline Linux kernel v5.0 and higher. Reference code, test vectors, and a benchmarking suite are available at https://github.com/google/adiantum.

Android device manufacturers can enable Adiantum for either full-disk or file-based encryption on devices with AES performance <= 50 MiB/sec and launching with Android Pie. Where hardware support for AES exists, AES is faster than Adiantum; AES must still be used where its performance is above 50 MiB/s. In Android Q, Adiantum will be part of the Android platform, and we intend to update the Android Compatibility Definition Document (CDD) to require that all new Android devices be encrypted using one of the allowed encryption algorithms.

14.Three ways to achieve crypto agility in a post-quantum world

by Gregory Webb
https://www.helpnetsecurity.com/2024/02/06/crypto-agility-strategies/

Crypto agility is the foundation for digital trust. As more enterprises speed up app development and build networks connecting many functions (often in the cloud), they rely on encryption keys and digital certificates to secure communications channels between users, applications and other assets.

Both public trust certificates (TLS/SSL), which are issued by trusted Certificate Authorities (CAs), and private certificates issued by an internal CA within a company, enable an identity-first approach to security that protects all connected applications, services, including all the machine identities that do the automated grunt work of digital functions.

The impact of Google's 90 day proposal on crypto agility

Transport layer security (TLS) certificates (and previously secure socket layer (SSL) certificates) were, until recently, almost an afterthought: keeping them updated was a bit of digital housekeeping that came around every few years.

Over the last decade, browser vendors and the certificate authorities (CAs) who comprise the CA/Browser Forum have increased the pressure by shortening the lifespan of public trust certificates to intentionally reduce their attack surface. In 2020, Apple reduced the lifespan certificates to a year, pushing others to match them, and in March 2023, Google announced a proposal to reduce TLS certificate validity to 90 days.

This shift poses a significant challenge to admins responsible for **certificate lifecycle management (CLM)**. Even small-to-midsize organizations can have thousands or tens of thousands of certificates quietly operating in the background, and the number keeps growing as more apps, cloud-based services, IoT devices and others are adopted. Many of them depend on machine identities that themselves require certificates.

Crypto agility is no longer a luxury

Keeping up with certificates is not really a choice left up to admins; failing to effectively manage certificate expirations and upscaling encryption not only leaves the enterprise vulnerable to breaches but also to downtime caused by an expired certificate. This has recently plagued even major organizations with deep wells of tech support, such as Starlink and Microsoft.

With quantum computing threatening to break current encryption standards – including RSA and ECC –

post-quantum cryptography (PQC) offers a quantum-resistant alternative, ensuring long-term security.

Integrating PQC into crypto agility strategies is crucial for organizations to safeguard against future attacks. This involves understanding the emerging standards, like those developed by NIST, and preparing for the seamless adoption of PQC algorithms.

Crypto agility best practices

To achieve crypto agility, consider these three strategies:

- **Embrace CLM:** Establish a uniform PKI policy to take control of the certificate process, starting with improving visibility into the certificates in the network. Centralizing and automating management can help improve visibility into the expiration and encryption infrastructure of different certificates—a big challenge in CLM—and establish standards.

  Many organizations have established a crypto center of excellence to streamline the management process and reduce human error. They have also deployed automation to handle provisioning of certificates and manage their lifecycle, to refresh those in use and revoke unused certificates that could become security blind spots. Establishing guidelines and procedures for effective certificate usage and management eliminates inconsistencies, minimizes security risks, and ensures compliance with industry regulations.

- **Liberate the certificate:** Encryption standards are the foundation of CLM, ensuring the data is protected. But encryption standards vary by vendor and certificate authority (CA), so a holistic approach that does not rely on CA tools is key. A uniform PKI policy should establish cross-CA certificate discovery and renewal processes and standardize certificate formats.

  CA-provided tools can reduce manual effort and improve efficiency by making it easier to discover and manage certificates issued by that specific CA. But these provider-specific tools leave out other public and private CAs and certificates deployed across multiple endpoints, such as servers, mobile devices and laptops that also must access the network.

  These proprietary automation methods miss the last-mile certificate installation and end-point binding, and often can't manage certificates across clouds and containers, which creates gaps in automation and leaves the staff provisioning certificates manually. A CLM practice that is CA-agnostic can avoid putting PKI and InfoSec teams in silos that force them to work with fragmented visibility and resorting to manual processes.

- **Get proactive:** The looming threat of quantum decryption threatens to upend popular algorithms such as RSA and ECC, and the sheer volume of certificates—and their shortened life spans—makes keeping up with certificate expirations a growing challenge. These imperatives make proactive monitoring and rapid response to changing crypto requirements and emerging threats a must.

  A CLM-forward organization must stay informed about industry trends, collaborate with experts in detection and remediation, and implement vulnerability management processes. Sharing information about looming threats and communicating about expired certificates found in commonly used services can help speed remediation and reduce the blast radius any certificate compromise may cause.

The bottom line

The CLM challenge is escalating. Now is the time for organizations to develop the management

processes and approaches that will make effective CLM work for their infrastructure in a post-quantum world.

15.Tech Giants Form Post-Quantum Cryptography Alliance

by Ionut Arghire
https://www.securityweek.com/tech-giants-form-post-quantum-cryptography-alliance/

The Linux Foundation today announced the launch of the **Post-Quantum Cryptography Alliance (PQCA)**, an initiative to advance and drive the adoption of post-quantum cryptography.

Founded by AWS, Cisco, IBM, IntellectEU, Nvidia, QuSecure, SandboxAQ, and the University of Waterloo, the PQCA will focus on addressing the security challenges posed by quantum computing.

With quantum computing expected to allow threat actors to break existing security keys fast, securing data and communications in the post-quantum era becomes imperative, and the PQCA is set to help address this issue.

The alliance will engage in the development of both standardized and post-quantum algorithms, aiming to help organizations and open source projects looking for libraries and packages to support their alignment with the Commercial National Security Algorithm Suite 2.0.

To facilitate the adoption of post-quantum cryptography, the PQCA will engage in various technical projects, including the development of software for evaluating, prototyping, and deploying post-quantum algorithms.

PQCA founding members have long been active in the standardization of post-quantum cryptography, co-authoring the first four algorithms selected in the NIST Post-Quantum Cryptography Standardization Project, and the work of PQCA builds on this foundation.

PQCA's launch projects include the Open Quantum Safe project, which was founded at the University of Waterloo in 2014, and the new PQ Code Package project, aimed at the development of high-assurance production-ready software implementations of post-quantum cryptography standards. Both are listed on PQCA's GitHub page.

"Quantum computing offers the potential to solve previously unapproachable problems while simultaneously threatening many digital protections we take for granted. Cryptography is foundational for securing data, users, devices, and services. The necessary conversion to post-quantum cryptography represents one of the largest and most complex technology migrations in the digital era," Cisco director Jon Felten said.

The launch of PQCA comes roughly one year after IBM published a roadmap to help federal agencies and businesses with the migration to post-quantum computing. Also last year, UK and US government agencies published guidance to help organizations with the transition.

16.Improved differential-neural crypt-analysis for round-reduced Simeck32/64

by Rong Xie
https://www.eurekalert.org/news-releases/1033515

Deep learning has led to great improvements recently on a number of difficult tasks.

In CRYPTO 2019, Gohr innovatively integrated deep learning with differential cryptanalysis, specifically applied to Speck32/64, resulting in developing a neural distinguisher that outperforms the DDT-based distinguisher. Applying differential neural cryptanalysis methods to more cryptographic algorithms is an issue worth studying.

To solve the problems, a research team led by Liu ZHANG published their new research on 15 Dec 2023 in *Frontiers of Computer Science* co-published by Higher Education Press and Springer Nature.

The team used multiple convolutional layers with different kernel sizes based on the round function of Simeck32/64 to capture the characteristics of the ciphertext in multiple dimensions. Compared with existing research results, the accuracy and number of rounds of the differential-neural distinguisher for Simeck32/64 are improved.

In the research, they improve the Inception neural network according to the round function of Simeck32/64. To capture the connections between ciphertext pairs, they use multiple ciphertext pairs to form a sample as input to the neural network. These approaches enabled us to improve the accuracy of (9-12)-round differential-neural distinguisher (*ND*).

To establish solid baselines for *ND*, they compute the full distribution of differences induced by the input difference (0x0000, 0x0040) up to 13 rounds for Simeck32/64. To make a fair comparison with *ND*, they investigate the accuracy of DDT-distinguishers (*DD*) with multiple ciphertext pairs under independent assumptions. The comparison shows that the 9-, 10-round *NDs* achieve higher accuracy than the *DD*. This demonstrates that the *ND* contains more information than the *DD*.

Firstly, they found some (simultaneous-) neutral bit-sets for a 3-round differential. After comprehensive improvements in many aspects, they finally improve the 15-round and launch the first practical 16 and 17-round key recovery attacks for Simeck32/64 based on *ND*.

