Crypto News

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

August 01, 2024

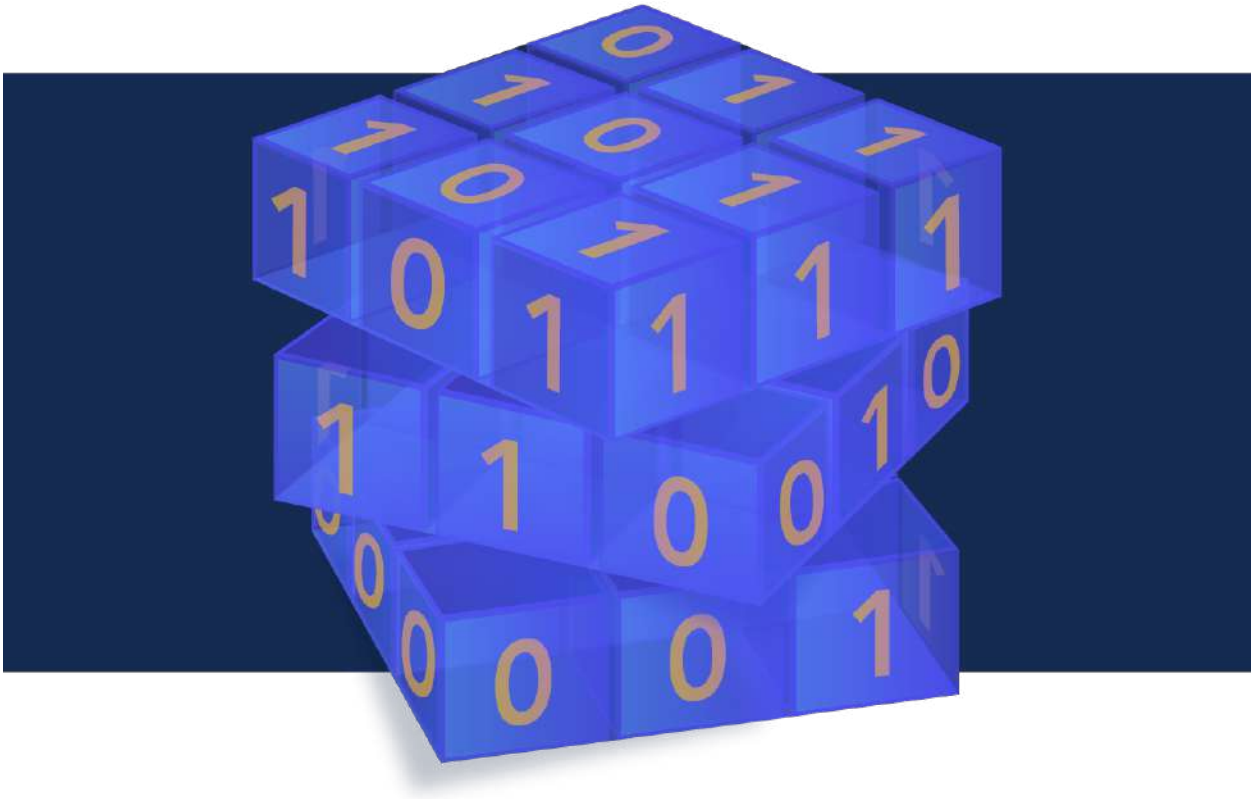


TABLE OF CONTENTS

Editorial

Happy August Readers! As summer moves along and we're all soaking up the sun and relaxing by the pool, take a few minutes to catch up on everything Quantum Safe with this issue of Crypto News!

Let's dive in (pun intended) with this bold statement; "Quantum is unimportant to post-quantum". The author of article 29 makes this potentially divisive statement but one that I can get behind. A compelling case is presented indicating that even if cryptographically significant computers never materialize, quantum safe cryptography should still be the goal and gold-standard of any organization. By walking us through the history of cryptography and how it's evolved over the past several decades, the author makes a solid case for implementing post-quantum algorithms regardless of whether cryptographically significant quantum computers will be a reality or not.

For those of us (including myself) who are confident that cryptographically significant quantum computers are inevitable, navigate to article 11 to get more information for yourself as well as your leadership that will help build your case to get the CFO to loosen those purse strings to fund your post-quantum project. My advice is that if your organization does any business with the United States Government (USG), know that they are allocating billions of dollars for post-quantum readiness. If you are a vendor or supplier to the USG in any way, you'll need to be ready when they inevitably request that you share your "post-quantum plan" to continue supporting them. Similar to the Cybersecurity Maturity Model Certification (CMMC) requirements, organizations who don't plan now for their post-quantum future will be too late when regulation and legislation solidify requiring post-quantum algorithms be used to secure data within their network to continue supporting the USG.

To keep the topic of quantum readiness going, article 28 provides guidance for your organization to reach crypto resilience in a post-quantum world. It's another great article highlighting the importance of starting your organization's quantum journey sooner rather than later to ensure you aren't late to the proverbial party. The guidance is high level and non-technical personnel friendly which can aid in ensuring you're able to get the leadership support required to push post-quantum projects forward. As always, the rest of the newsletter is full of interesting and informational articles that are not to be missed. Happy reading!

The Crypto News editorial is authored by the co-Chair of the Quantum-Safe Security-Working Group (QSS WG) of the Cloud Security Alliance (CSA), Mehak Kalsi, MS, CISSP, CISA, CMMC-CCP and it is compiled by Dhananjoy Dey.

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

1.Accenture and SandboxAQ Expand Partnership to Help Organizations Strengthen Data Encryption Today and Protect Against Future Threats

by Alison Geib, Denise Berard, and Tila Pacheco
https://newsroom.accenture.com/news/2024/accenture-and-sandboxaq-expand-partnership-to-help-organizations-strengthen-data-encryption-today-and-protect-against-future-threats

Accenture and SandboxAQ are expanding their partnership to address the critical need for enterprise data encryption that can defend against current data breaches, as well as future AI and quantum threats. Together, Accenture and SandboxAQ are helping organizations secure sensitive data and strengthen encryption across their technology portfolios. The joint offering will also provide observability across environments to help increase enterprise resilience and lower impact from third party risks.

More than half (52%) of CEOs consider the accelerated pace of technology innovation a top risk for cyberattacks, with 86% rating cyber trust and resilience in emerging technologies like generative AI and quantum computing as highly relevant for their organizations, according to research from Accenture.

The research serves as a reminder that strong cryptography management, requiring the latest algorithms to protect systems, processes and data is a foundational pillar to defending against evolving cyber threats. As part of an ongoing commitment to cryptographic excellence, Accenture is introducing a new Encryption Risk Assessment service, integrated with SandboxAQ's AQtive Guard. The service provides clients with deep visibility into risks caused by weak cryptography before these risks have a chance to impact critical data across networks, file systems, and cloud applications.

"The prevalence of generative AI, as well as expected new global post-quantum encryption standards, makes data protection absolutely critical to safeguarding confidential business information and data used to train AI foundational models or used in AI applications," said Paolo Dal Cin, global lead of Accenture Security. "The reality is that malicious actors are stealing sensitive data now, with the intention of decrypting it later using quantum computers that can break many current encryption methods. Our assessment service enables clients to see potential risks to their data and upgrade encryption to increase protection against ransomware, data theft and manipulation campaigns, and to prepare for future risks from quantum computing. Companies that assess their data encryption level now will be more protected against current attacks and better prepared to mitigate future risks."

The service can identify risks across important areas including the existence of cryptographic assets such as digital certificates or cryptographic keys, and usage of cryptographic algorithms, both symmetric and public key, as well as any other cryptographic constructions such as hash functions, for a comprehensive view of cryptography use throughout the enterprise. When combined with data security and privacy policies along with governance, risk and compliance guidelines, the assessment delivers prioritized recommendations for remediation action, enabling businesses to act with urgency and agility to protect their overall infrastructure against the most advanced and sophisticated threats, and in their transition to post-quantum technology.

"Our continued collaboration with Accenture will help our largest global 1000 clients defend themselves against advanced AI-driven cybersecurity attacks, protecting their most sensitive data today and tomorrow," said Jack Hidary, CEO of SandboxAQ. "As we help clients discover data that's vulnerable to current and future attacks, there are many benefits from enhancing their cryptography defenses. The recent global outage from just one software update highlights the need to increase observability across the enterprise."

2.Financial services not ready for TLS changes and post-quantum crypto

by Editorial Team
https://www.bobsguide.com/financial-services-not-ready-for-tls-changes-and-post-quantum-crypto/

Venafi, the leader in machine identity security, today released a new research report, Organisations Largely Unprepared for the Advent of 90-Day TLS Certificates. The report examines organisations' current state of preparedness to transition to new machine identity standards, including shorter certificate lifecycles and post-quantum cryptography.

The survey of 800 security decision-makers across the U.S., UK, Germany and France, included 117 respondents working in financial services (FS). It revealed that 70% of FS security leaders (72% cross sector) recognise the pressing need to move to shorter certificate lifespans to improve security. However, many feel unprepared to take action, with 74% (77% cross sector) saying the shift to 90-day certificates will mean more outages are inevitable.

Additional highlights from the survey findings include:

- **90-Day Certificate Challenges –** 79% of financial services security leaders (81% cross sector) believe Google's proposed plans to shorten TLS certificate lifespans from 398 days to 90 days will amplify existing challenges they have around managing certificates. An overwhelming 93% of FS survey respondents (94% cross sector) are concerned about the impact of the changes, with 68% (73% cross sector) saying it could cause "chaos" and a further 68% (75% cross sector) saying it could even make them less secure.

- **Volatile CA Landscape –** The recent decree that certificates issued by Certificate Authority (CA) Entrust can no longer be trusted is just the latest example of disruption in the CA market. In fact, 86% of FS security leaders (88% cross sector) report their organisation has been impacted by CA revocations. Of these, 54% (45% cross sector) had to deploy extra resources to find, revoke and replace certificates; 38% (38% cross sector) suffered a security incident; and 26% (31% cross sector) had a certificate-related outage.

- **Quantum Denial –** With momentum gathering around the need to migrate to new quantum-resistant encryption algorithms, 61% of FS security leaders (64% cross sector) say they "dread the day" the board asks about their migration plans. 81% (78% cross sector) say if a quantum computer capable of breaking encryption is built, they will "deal with it then," with 58% (60% cross sector) believing that quantum computing doesn't present a risk to their business today *or in the future.* Moreover, 62% (67% cross sector) dismiss the issue, stating it has become a "hype-pocalypse."

"We recently lived through the world's greatest IT outage which severely impacted banks and financial

institutions worldwide – the CrowdStrike update outage was an error and unexpected. Security teams know they will be hit with major risks when new outages occur from what they love to hate: more expiring certificates," said Kevin Bocek, chief innovation officer at Venafi. "Shifting to shorter certificate lifecycles significantly reduces these risks and is a necessary move. However, this can also bring more chaos for security teams – and it's a double whammy with Entrust being distrusted in Chrome. There aren't just canaries in the coal mine; there are groundhogs in every cloud, virtual machine and Kubernetes cluster. It's not just one software update vendor; it's the entire Internet as we know it."

The introduction of 90-day certificates means FS organisations will need to renew their certificates five times more often than they do now – quintupling the effort needed. The survey reveals this will be a major challenge for FS organisations for two reasons:

- **Delayed Deployment –** Only 8% of financial services security leaders (8% cross sector) fully automate all aspects of TLS certificate management across their entire enterprise, with 33% (29% cross sector) still relying on their own software and spreadsheets to manage the problem. As a result, it takes an average of 2-3 working days (an average of 22.03 hours for FS compared to 21.75 hours cross sector) to deploy a certificate.

- **TLS Transformation –** The volume of TLS certificates in use at organisations has been steadily rising, due to the growth in technology adoption in recent years. 97% of FS security leaders (95% cross sector) say digital transformation initiatives have increased their organisation's use of SSL/TLS in the past year by an average of 38% (36% cross sector). As a result, the average FS organisation now manages 4934 TLS certificates (3,730 cross sector) – a number that is expected to increase by 42% (39% cross sector) by 2026, taking the figure up to over 7,000 (5,000 cross sector).

Similar challenges exist with quantum. 69% of FS survey respondents (67% cross sector) believe shifting to post-quantum cryptography will be a nightmare, as they don't know where all their keys and certificates are. Looking at the specific challenges these shifts present, the potential speed of the migration, lack of internal skills and knowledge, as well as fears that adversaries will use quantum computing to attack before businesses have a chance to migrate, were cited as the top three concerns for FS organisations. However, 85% (86% cross sector) say taking control of the management of keys and certificates is the best way to prepare for future quantum risks.

"There's great news: from 90-day certificates to replacing distrusted CAs to making the transition to post-quantum, FS security teams today have machine identity security capabilities they didn't have available just a few years ago. Security teams can get certificate lifecycle management (CLM), PKI-as-a-service and workload identity issuers all on one control plane now," Bocek concludes. "The business case is simple for making sure 90-day certificate lifetimes don't wreak havoc. We know the problem is coming, unlike the last major IT outage, and the automation we put in place with machine identity security gets us ready for the post-quantum future, the next CA distrust and running in whatever cloud our developers choose. At Venafi, we are built for these times."

3.Businesses Brace for NIST Post-Quantum Cryptography Algorithms

Q&A with Keyfactor's Chris Hickman

https://www.iotworldtoday.com/quantum/businesses-brace-for-nist-post-quantum-cryptography-algorithms

The U.S. National Institute of Standards and Technology (NIST) is due to release its four finalized post-quantum cryptography (PQC) algorithms. At one point they were expected to arrive in July, but while that looks unlikely it is almost certain they will drop by the end of the year.

While cryptographically relevant quantum computers are years away, U.S. businesses will need to begin migrating to using the new standards and they will become a model for much of the rest of the world to follow.

In this Q&A, Keyfactor chief security officer Chris Hickman details how businesses can best determine which processes to prioritize as they begin their PQC transition and the first steps they must take once these PQC standards are live.

Enter Quantum: NIST is releasing the algorithms later than expected. As they have been anticipated for a long time, what will happen when they do?

Chris Hickman: There are two ways the market is looking at that. Some people think it's a finish line, but I personally think the announcement will finally give us a starting line to know what the track looks like, to use a car analogy. We're going to finally know how to start bringing to market the final set of standards.

We've been encouraging our customers to plan at this stage and trying to get people behind the idea that this is not just a post-quantum problem per se, this is an evolution of cryptography. People need to look at it in the light of this inevitable change and embrace it rather than entering the philosophical debate around whether post-quantum is real and when it will happen.

PQC will force organizations into a spot of saying, OK, what is my cryptographic landscape? By and large, crypto has been handled very poorly in most organizations. It's become a checkbox on a request for proposal, "Do you support RSA and ECC?" Nobody has done a good job of maintaining crypto as a critical asset in the organization.

We don't know what vulnerabilities these new algorithms could have in the future. They're going to be as close to perfect as they can be, but they're never going to be perfect. Organizations need to take an approach that says, okay, we're going to start managing crypto with some level of agility as a critical asset. We're going to maintain that inventory and we'll be able to respond to those changes.

What will the challenge be for organizations?

We publish a report every year and found only 23% of organizations had started some work around PQC, which is concerningly low. Over the course of the year, that has probably increased because it's getting on the radar of boards and the risk associated with it is during a higher level of attention.

Trying to find crypto in the organization is immensely difficult. The only way that I can explain it when a customer asks how do I get started is that we know asymmetric cryptography and PKI are going to be among the first things to fall. Symmetric cryptography seems to be fairly robust against post-quantum computers. So let's start looking for things like certificates in your organization.

Around 73% of respondents and the research we did don't even know how many keys they have in their organization. It's a massive landscape for people to go after just in trying to figure out what they have in the way of certificates in my organization.

Where NIST leads, the world is expected to follow. How will we see PQC roll out globally?

NIST has set the standards here and the world has agreed to follow their lead. I've had the pleasure of speaking with some of the folks at NIST who are running this program, and it's been a conscientious decision to, rather than create conflict amongst standards organizations, rally around one and for the world to participate in the development of the standards.

There are obviously going to be some regional variances around data sovereignty type issues and in some cases, countries would rather use domestically developed crypto algorithms based on this set of standards. But the world is gonna have to move quickly and the entire ecosystem is coming together to work to solve the problem.

IoT devices are historically under-resourced for large cryptographic keys. How should organizations that use them prepare for PQC?

IoT is an interesting space because a lot of IoT devices are based on restrained chipsets and they don't have a lot of addressable memory. There are some emerging technologies that may show up in the next round of standards that will deal with smaller key sizes, specifically targeted at IoT and constrained devices.

There are ways to protect them at the perimeter that might work as stopgap measures depending on where they fit with release cycles. But the real problem is that organizations are going to have to find ways to move the identity of devices in the interim and use an identity gateway to broker between post-quantum and classical algorithms, with the classical algorithms being on device and post-quantum being at the edge somewhere.

How soon will organizations need to act when NIST finally releases its PQC algorithms?

Unfortunately, the answer is, it depends. We're seeing some organizations embracing PQC standards ahead of the game, especially financial institutions and healthcare technology companies in North America. They have probably already identified pools of data that need to be very quickly migrated and have spent the time to figure out what's in the supply chain o for that data.

A big piece of this is figuring out is, if that data resides in multiple places and one place isn't ready to go to post-quantum, you're gonna leave your data at risk. Organizations need to take the approach of what data do I have and what's the risk to the organization.

They then need to look at what their supply chain is like, not only in physical hardware and software but also in that data flow chain and then start assessing the priority of that against other priorities in the business. I don't think people will be able to do meaningful things for a few months but they need to be ready to go very quickly.

The thing that organizations need to be doing today, beyond assessing their data, is being ready for different size post-quantum keys which will impact on basics like network bandwidth. If you're using massive keys, there's going to be an implication to bandwidth so there are things that can be done today to mitigate that risk, both in your data and also in understanding how this impacts your infrastructure.

4.Quantum Error Mitigation May Face Hard Limits

by Matt Swayne
https://thequantuminsider.com/2024/07/26/quantum-error-mitigation-may-face-hard-limits/

Quantum error mitigation is a promising technique to reduce noise in quantum computing without the significant resource demands of fault-tolerant schemes, but a team of researchers say the technique faces fundamental constraints.

The researchers recently published a study in Nature that offers a glimpse into these limitations, ones that pose challenges for how effective error mitigation can be in larger quantum systems.

According to the researchers, quantum computers hold the potential to solve complex problems beyond the capabilities of classical supercomputers. However, slight interactions with the environment can lead lead to decoherence. And that can threaten the reliability of quantum computations. While quantum error correction can theoretically address these issues, it demands significant resources, making it impractical for near-term quantum devices.

As a practical alternative, quantum error mitigation has emerged. Error mitigation in quantum computing is a method used to correct mistakes caused by noise in the system using classical computing techniques, without needing extra quantum hardware. This means that developers can avoid the need for mid-circuit measurements and adaptive gates.

Error Mitigation Faces a Statistical Challenge

The study frames error mitigation as a statistical inference problem, demonstrating that estimating accurate results from a quantum system becomes much harder as the system gets bigger. Even with quantum computations involving only a few steps, known as shallow circuit depths, the researchers report that an extremely large number of measurements of the quantum system's output, or samples, is required in the worst case. This, essentially, makes effective noise mitigation infeasible for larger circuits, according to the researchers.

They write: "We identify striking obstacles to error mitigation. Even to mitigate noisy circuits slightly beyond constant depth requires a superpolynomial number of uses of those circuits in the worst case. These obstacles are seen when we turn the lens of statistical learning theory onto the problem of error mitigation."

The researchers show that noise can scramble quantum information at exponentially smaller depths than previously thought. One way to think of it, if the analogy holds, is trying to tune in a radio so the signal is clear but you lose it to static almost immediately.

This scrambling has the potential to affect various near-term quantum applications, including quantum machine learning and variational quantum algorithms, limiting their performance and ruling out exponential speed-ups in the presence of noise.

Current Error Mitigation Techniques

The study rigorously reviews many error-mitigation schemes in use today, such as zero-noise extrapola-

tion and probabilistic error cancellation. These techniques, while effective in certain cases, face severe resource penalties. In one example, the team details that zero-noise extrapolation requires an exponentially increasing number of samples as the number of gates in the light cone of the observable grows, depending on the noise levels.

Similarly, probabilistic error cancellation under a sparse noise model also exhibits exponential scaling, they write. These findings contribute to a theoretical understanding of when and why these penalties occur, challenging the practicality of current error mitigation approaches.

Theoretical Framework and Findings

The researchers use statistical methods to explain error mitigation, describing it as comparing an ideal, noise-free quantum circuit with the actual, noisy results to correct errors. They distinguish between weak error mitigation, which estimates expectation values, and strong error mitigation, which aims to produce samples from the clean output state.

Their framework encompasses various practical error-mitigation protocols, including virtual distillation, Clifford data regression, zero-noise extrapolation, and probabilistic error cancellation. Despite ongoing development and high expectations, the study builds on prior work to highlight the inherent limitations of these techniques.

Implications for Quantum Computing

The implications are significant for the development of quantum computing. Error mitigation, while a promising short-term solution, faces intrinsic limitations that must be addressed to realize the full potential of quantum devices. As noise affects the distinguishability of quantum states, effective error mitigation must act as a robust — to coin a name — denoiser, distinguishing states even when accessed only through their noisy versions.

The study also offers insights that could help establish the fundamental limits on a wide range of error-mitigation protocols. This doesn't mean that error-mitigation is useless, however, rather the researchers say future work needs to address the creation of innovative approaches to overcome these challenges.

Limitations And Future Work

The researchers did mention some limitations with their study. They acknowledged that their theoretical framework, while comprehensive, might not account for all practical nuances in real-world quantum computing environments. Specifically, they noted that their results are based on worst-case scenarios, which might not reflect typical experimental conditions. It's also possible that assumptions made about noise models and statistical methods might not fully capture the complexity of actual quantum noise behavior. These factors suggest that while their findings highlight significant challenges, further work will be needed to assess the practical applicability of their conclusions.

The team suggested exploring new error mitigation techniques that could potentially overcome the identified scalability issues. The study also highlighted the importance of developing more accurate noise models and statistical methods that closely mirror real-world quantum computing environments. These future directions aim to enhance the reliability and scalability of quantum error mitigation, ultimately bringing practical quantum computing closer to reality.

The research team included: Yihui Quek, associated with both Freie Universität Berlin in Germany and Harvard University, who led the research; Daniel Stilck França, the University of Copenhagen in Denmark and Univ Lyon in France; Sumeet Khatri and Johannes Jakob Meyer, both affiliated with Freie Universität Berlin; Jens Eisert, of both Freie Universität Berlin and Helmholtz-Zentrum Berlin für Materialien und En-

ergie in Germany.

The study is highly technical and this overview might miss some of the nuance. It's always recommended to read the paper for a deeper dive.

5.Secure Boot is completely broken on 200+ models from 5 big device makers

by Dan Goodin
https://arstechnica.com/security/2024/07/secure-boot-is-completely-compromised-on-200-models-from-5-big-device-makers/

In 2012, an industry-wide coalition of hardware and software makers adopted Secure Boot to protect against a long-looming security threat. The threat was the specter of malware that could infect the BIOS, the firmware that loaded the operating system each time a computer booted up. From there, it could remain immune to detection and removal and could load even before the OS and security apps did.

The threat of such BIOS-dwelling malware was largely theoretical and fueled in large part by the creation of ICLord Bioskit by a Chinese researcher in 2007. ICLord was a rootkit, a class of malware that gains and maintains stealthy root access by subverting key protections built into the operating system. The proof of concept demonstrated that such BIOS rootkits weren't only feasible; they were also powerful. In 2011, the threat became a reality with the discovery of Mebromi, the first-known BIOS rootkit to be used in the wild.

Keenly aware of Mebromi and its potential for a devastating new class of attack, the Secure Boot architects hashed out a complex new way to shore up security in the pre-boot environment. Built into UEFI—the Unified Extensible Firmware Interface that would become the successor to BIOS—Secure Boot used public-key cryptography to block the loading of any code that wasn't signed with a pre-approved digital signature. To this day, key players in security — among them Microsoft and the US National Security Agency — regard Secure Boot as an important, if not essential, foundation of trust in securing devices in some of the most critical environments, including in industrial control and enterprise networks.

An unlimited Secure Boot bypass

On Thursday, researchers from security firm Binarly revealed that Secure Boot is completely compromised on more than 200 device models sold by Acer, Dell, Gigabyte, Intel, and Supermicro. The cause: a cryptographic key underpinning Secure Boot on those models that was compromised in 2022. In a public GitHub repository committed in December of that year, someone working for multiple US-based device manufacturers published what's known as a platform key, the cryptographic key that forms the root-of-trust anchor between the hardware device and the firmware that runs on it. The repository was located at https://github.com/raywu-aaeon/Ryzen2000_4000.git, and it's not clear when it was taken down.

The repository included the private portion of the platform key in encrypted form. The encrypted file, however, was protected by a four-character password, a decision that made it trivial for Binarly, and anyone else with even a passing curiosity, to crack the passcode and retrieve the corresponding plain text. The disclosure of the key went largely unnoticed until January 2023, when Binarly researchers found it while investigating a supply-chain incident. Now that the leak has come to light, security experts say it effectively torpedoes the security assurances offered by Secure Boot.

"It's a big problem," said Martin Smolár, a malware analyst specializing in rootkits who reviewed the Binarly research and spoke to me about it. "It's basically an unlimited Secure Boot bypass for these devices that use this platform key. So until device manufacturers or OEMs provide firmware updates, anyone can basically… execute any malware or untrusted code during system boot. Of course, privileged access is required, but that's not a problem in many cases."

Binarly researchers said their scans of firmware images uncovered 215 devices that use the compromised key, which can be identified by the certificate serial number 55:fb:ef:87:81:23:00:84:47:17:0b:b3:cd:87:3a:f4. A table appearing at the end of this article lists each one.

The researchers soon discovered that the compromise of the key was just the beginning of a much bigger supply-chain breakdown that raises serious doubts about the integrity of Secure Boot on more than 300 additional device models from virtually all major device manufacturers. As is the case with the platform key compromised in the 2022 GitHub leak, an additional 21 platform keys contain the strings "DO NOT SHIP" or "DO NOT TRUST."

Not ready for prime time

These keys were created by AMI, one of the three main providers of software developer kits that device makers use to customize their UEFI firmware so it will run on their specific hardware configurations. As the strings suggest, the keys were never intended to be used in production systems. Instead, AMI provided them to customers or prospective customers for testing. For reasons that aren't clear, the test keys made their way into devices from a nearly inexhaustive roster of makers. In addition to the five makers mentioned earlier, they include Aopen, Foremelife, Fujitsu, HP, Lenovo, and Supermicro.

Cryptographic key management best practices call for credentials such as production platform keys to be unique for every product line or, at a minimum, to be unique to a given device manufacturer. Best practices also dictate that keys should be rotated periodically. The test keys discovered by Binarly, by contrast, were shared for more than a decade among more than a dozen independent device makers. The result is that the keys can no longer be trusted because the private portion of them is an open industry secret.

In an interview, Binarly founder and CEO Alex Matrosov wrote:

> *"Imagine all the people in an apartment building have the same front door lock and key. If anyone loses the key, it could be a problem for the entire building. But what if things are even worse and other buildings have the same lock and the keys?"*

Matrosov said his team found identical test platform keys on both client and server-related products. Team members also determined that at least one test key was used in devices sold by three distinct manufacturers.

"If the key will be leaked, it's impacting the ecosystem," he explained. "It's not impacting a single device."

Binarly has named its discovery PKfail in recognition of the massive supply-chain snafu resulting from the industry-wide failure to properly manage platform keys. The report is available here. Proof-of-concept videos are here and here. Binarly has provided a scanning tool here.

Secure Boot in a nutshell

The four key resources to make Secure Boot work are:

1. **The Platform Key, or PK:** This provides the root-of-trust anchor in the form of a cryptographic key embedded into the system firmware. It establishes the trust between the platform hardware and all firmware that runs on it.

2. **The Key Exchange Key, or KEK:** This is the key that establishes trust between the operating system and the platform firmware.

3. **The Signature Database, or DB:** A database containing trusted signatures and certificates for third-party UEFI components and boot loaders approved by the hardware manufacturer.

4. **The Forbidden Signature Database or DBX:** A database of signatures and certificates used for revoking previously trusted boot components so they can no longer run during bootup.

Updates to both the DB and DBX must be signed by a KEK in the Secure Boot KEK database.

The following three images—provided by Binarly, Microsoft, and the NSA respectively—give a visual overview of these four main resources.

.
.
.

6.Encryption is on the Cusp of a Paradigm Shift with FHE

by Guy Zyskind
https://www.thestreet.com/crypto/innovation/encryption-is-on-the-cusp-of-a-paradigm-shift-with-fhe-

The problem with most forms of encryption being used today is that once data is encrypted, it becomes frozen or fixed in place—meaning it can't be operated on or "processed" without first decrypting it. This has huge implications for the safety and security of sensitive data. Fhenix's Guy Zyskind explains how a new type of encryption called Fully Homomorphic Encryption (FHE) is going to fundamentally alter the way data is encrypted and used.

Whether or not they're aware of it, encryption is a crucial technology for anyone who uses the internet. So important that they are utilizing it in some form or another many times throughout their day. Whether it's sending a text message or email to a friend, checking their bank account balance, or doing any number of the different things people do online, encryption is the technology that ensures only trusted parties are able to view this information. The thing is, for something as important and ubiquitous as data privacy and security, there is currently a huge problem with the way this data is being safeguarded.

To understand this problem, it's helpful to first understand what encryption is and how it functions at a basic level. Put simply, encryption is the process of converting data into a format that is unreadable to anyone who does not have the necessary key to decrypt it. Robust encryption is absolutely critical to a safe and usable internet.

The problem with most forms of encryption currently being used today is that once data is encrypted, it becomes frozen or fixed in place—meaning it can't be operated on or "processed" without first decrypting it. This has huge implications for the safety and security of sensitive data. See, data that cannot be operated on is limited in its utility. In order for it to be useful, it needs to be processed or manipulated—

something current widespread forms of encryption do not support. The standard workaround for this is to decrypt the encrypted data, process it, then re-encrypt it. As an example, imagine you're an accountant working on a spreadsheet of your company's financials. The data is sensitive, which is why the document is encrypted and password-protected. In order to view and work on it, you need to decrypt it. Once you've finished your work, you save the document, effectively re-encrypting it. This is a simplified example of how most encryption currently works. While it's certainly one way to do it, the approach is less than ideal as it breaks the circle of encryption, creating an opportunity for unencrypted plaintext data to be leaked. Not great.

Luckily, there's an advanced form of encryption that enables operations to be performed on encrypted data without ever having to decrypt it. That type of encryption is called Fully Homomorphic Encryption (FHE), and it's going to fundamentally alter the way data is encrypted and used.

Craig Gentry, one of the foremost pioneers of Fully Homomorphic Encryption and the first to prove that it's possible, uses a glove-box analogy to explain what FHE does. Gentry likens FHE to a glove box where encrypted data is stored. Someone can reach inside that glove box and manipulate the data it contains without ever actually revealing the data itself. This is called "blind data processing," and it's incredibly useful, especially when we're dealing with inputs from multiple parties—a common scenario in computing referred to as secure multiparty computation.

FHE is Rapidly Evolving

So if FHE is a much more flexible and secure form of encryption, why isn't it the standard? Well, because it turns out that creating a solution that provides computation of encrypted data is really hard. Like, really hard. So hard that it's a problem many smart people have dedicated their entire lives and careers to solving. But, if there's one thing that's true of technological progress (and human beings in general), it's that we keep making incremental progress on seemingly impossible problems until eventually they're solved.

Significant advances in FHE have been made over the past few decades, bringing us close to a tipping point where the technology may soon be feasible for widespread use. These advancements span various areas, including algorithmic research, hardware acceleration, and the development of FHE libraries and toolkits.

While technological breakthroughs may seem to arrive all of a sudden, springing forth fully-formed like Athena from the head of Zeus, the reality is that they are often the result of incremental progress made in many different fields, which eventually leads to a defining piece of technology. The use of the steam engine for locomotives and steamships in the nineteenth century, for example, was made possible by advances in air pressure, vacuums, rotary motion, and thermodynamics made in the centuries and decades preceding. Similarly, FHE is the beneficiary of numerous advancements being made in cryptography and computing.

Much progress has been made in FHE algorithmic research since the first viable FHE scheme was presented by Gentry in his 2009 PhD dissertation. From the introduction of the first practical FHE scheme (BGV) in 2011 and its implementation in 2012, to the introduction of faster and more flexible schemes like TFHE and CKKS in 2016. Notable creations of FHE libraries and toolkits have also been made, including Microsoft's Simple Encrypted Arithmetic Library (SEAL), OpenFHE, and Zama's TFHE-rs. On the hardware front, progress is also being made to mitigate FHE's high computational overhead, one of its greatest bottlenecks to growth. In 2021, DARPA began the Data Protection in Virtual Environments (DPRIVE) project with the goal of reducing computational run time overhead, accelerating FHE calculations to within one or two orders of magnitude of current performance on unencrypted data.

Slowly, Then All at Once

Given the considerable progress in FHE, why isn't it more widely discussed or recognized for the significant benefits it offers humanity? It's hard to say exactly why, but it could have something to do with how humans are notoriously poor at forecasting exponential growth curves. Take Zero Knowledge Proofs (ZKPs) for example, a technology with comparable mathematical complexity, which has nevertheless made huge strides over the last decade, resulting in numerous practical applications. From being completely theoretical just over a decade ago, to taking several minutes to prove no double-spend (zCash) a decade ago, ZKPs are now being used to prove arbitrary computations, including inference over medium-sized machine-learning models.

Given the continued progress of FHE, there's no reason to assume it isn't on a similar growth trajectory. As Lenin famously quipped, "There are decades where nothing happens; and there are weeks where decades happen."

To summarize, I believe FHE's commercial adoption is fast approaching reality. When it does, its application will extend to various industries, establishing a new paradigm in data privacy and security. This shift will greatly benefit us all at a time when our world is becoming increasingly digitized, placing an ever-increasing premium on data sovereignty. In such a landscape, the holistic encryption provided by FHE will be crucial for safeguarding our sensitive and valuable data.

7.Systems Designed Today Must Support Post-Quantum Cryptography Tomorrow

https://www.design-reuse.com/news/56568/post-quantum-cryptography.html

Post-Quantum Cryptography (PQC) will answer to the imminent threat created by advances in quantum computing. Xiphera will present and demonstrate hardware-based IP cores for PQC algorithms in Japan in September 2024.

The landscape of cryptography and cybersecurity is inevitably shifting: the rapid development of quantum computers will solve many computational problems, but at the same time, it creates novel threats to securing data and information. Powerful enough quantum computers will eventually be able to break the traditional public-key cryptographic algorithms such as RSA and elliptic curve cryptography that we use in our everyday lives.

Post-quantum cryptography (PQC) answers to the imminent quantum threat. PQC algorithms are implemented on traditional computational platforms, but they withstand both traditional and quantum attacks. Implementing PQC already today is crucial for everyone, but its importance is emphasised especially in long lifecycle applications e.g. in industrial and automotive industries.

Xiphera's xQlave® family of Post-Quantum Cryptography consists of fully hardware-based PQC IP cores, designed to withstand quantum attacks and implemented without any software components. The xQlave® family includes IP cores for ML-KEM (previously CRYSTALS-Kyber) Key Encapsulation Mechanism and ML-DSA (previously CRYSTALS-Dilithium) Digital Signature algorithms. The IP cores comply with the standardisation of PQC algorithms by the American National Institute of Standards and Technology (NIST).

8.Researchers Develop Method for High-Capacity, Secure Quantum Communication Using Qudits

by James Dargan
https://thequantuminsider.com/2024/07/23/researchers-develop-method-for-high-capacity-secure-quantum-communication-using-qudits/

Scientists at the Chinese Academy of Sciences have developed a new method for high-capacity, secure quantum communication using qudits, promising a powerful quantum internet. Unlike traditional qubits, which encode information in a state of 0, 1, or both, qudits operate in higher dimensions, enabling greater data transmission.

The technique utilizes spatial mode and polarization properties of light to create four-dimensional qudits on a specialized chip, resulting in faster data transfer and enhanced error resistance. This method is particularly advantageous for satellite-based quantum communication due to its ability to maintain quantum properties over long distances.

The process involves generating an entangled state with two photons, where one photon is manipulated to form a 4D qudit, while the other acts as a remote control. This allows scientists to control and encode information onto the qudit.

This breakthrough could revolutionize quantum communication, paving the way for a high-speed, secure quantum internet. It also has the potential to develop unbreakable encryption protocols and contribute to advanced quantum computers. Researchers are now focusing on improving qudit accuracy and scaling up the technology for even higher dimensions.

9.Release of Post-Quantum Cryptographic Standards Is Imminent

by Robert Huntley
https://www.eetimes.eu/release-of-post-quantum-cryptographic-standards-is-imminent/

As the quantum computing industry advances and the possibility of large-scale fault-tolerant quantum computing becomes ever nearer, post-quantum cryptography (PQC) is paramount. Cybersecurity professionals eagerly await the publication of the selected algorithm standards by the U.S. National Institute of Standards and Technology (NIST), which are in the final stages of industry consultations and ratification. Starting in 2016, NIST has been instrumental in leading global efforts to define cryptographic algorithms capable of resisting brute-force attempts by quantum computers to compromise them.

EE Times Europe caught up with Joppe Bos, a cryptographic researcher at NXP Semiconductors and co-author of one of the selected algorithms, to learn the current status of the standardization process.

EE Times Europe: We've heard very little about the PQC standards recently. How long before they are published?

Joppe Bos: NIST has announced the four winning algorithms. Three of the four — Crystals Kyber, Crystals Dilithium and Sphincs+ — are ready for release. The fourth, Falcon, will need more time. NIST has said that they signed off on the three and that the final step before publishing sits with the legal department of the U.S. government. No one knows if this process will take a long time or be quick. NIST hasn't communicated this in a particularly concrete way, but I think we'll have an answer this summer.

EE Times Europe: Getting the standards is one thing, but what about when PQC-ready ICs will appear?

Bos: The good thing is we have had the draft standards for a while. NIST has been relatively open concerning where they would make minor technical amends, allowing companies to prepare. Many companies, including NXP, are ready internally to support the new standards. Our crypto libraries are fully prepared. Of course, some companies have it much easier. If you look at the big cloud providers and cybersecurity companies, they just need functional implementation. Achieving high-assurance implementations hardened against fault attacks requires much more work, something we have been working on for the last couple of years. For the much smaller devices — for instance, those used in industrial IoT — we need to resort to our bag of tricks to get these implementations working on devices that don't have the massive amounts of memory the public, open-source implementations need.

EE Times Europe: Will we see some device-level segmentation in the market regarding security functionality?

Bos: Yes, and the partitioning will be on multiple levels. One is on the security level, such as those products requiring certifications like finance credit cards and smart cards for building access. Then higher levels require implementations to protect against side-channel attacks. When I talk about the migration toward post-quantum cryptography, people always think the biggest challenge is performance, and it is a big challenge, but it's not the biggest one. The biggest challenge is the memory requirements. For PQC, the keys are much bigger, and signatures are much bigger, like 4 or 5 kB. If you need to operate on these items, you need a lot of memory. With elliptic-curve cryptography [ECC], you only need a handful of bytes of memory. Much of our research has been spent producing small implementations for the embedded world. We've been working on this challenge for some time now to ensure small devices can run post-quantum cryptography implementations once the standards come out.

EE Times Europe: What key deadlines should embedded developers be working against?

Bos: The summer of 2024 is the first important date since three of the NIST standards will be released in this period. Then the big kickoff for the migration toward post-quantum crypto begins. Also, we'll see governments that have already communicated post-quantum migration guidance—that is, the U.S., the BSI [Federal Office for Information Security] in Germany, and France—lay down their timelines and plans. The dates they give may differ slightly, but the message is the same. From 2025 onward, you should start migrating until 2030–2033. By 2033, the migration should be complete. In this transition period, they often recommend using a hybrid approach, running classical crypto in combination with post-quantum crypto. However, in 2030 or 2033, depending on which document you read, you should switch and only run post-quantum crypto since using RSA and ECC is prohibited.

EE Times Europe: What advice do you give embedded developers about embarking on the post-quantum journey?

Bos: First, get your priorities straight. What should you migrate first? That's quite interesting, because if you read articles about the migration toward post-quantum crypto, the No. 1 example people always use is the "harvest now, decrypt later," also known as "store now, decrypt later," attacks. That is highly rele-

vant but not necessarily for embedded devices because of the use cases. When people say this, they're talking about transport layer security. This is because they assume that you can break the initial key exchange step with a quantum computer, allowing you to decrypt all the information. However, while this priority applies to many companies, focusing on the key exchange first is not the priority for many embedded use cases. Instead, attention should be paid to migrating the digital signatures first.

There are two use cases to consider. The first is a secure boot used in automotive, industrial and consumer IoT devices. When you switch them on, they have a secure boot process so that you know you can trust the software used to boot the device. The secure boot uses a signature verification to confirm that the software booted is genuine.

The second use case is secure updates, either over the air or not. That also uses signature verification. You need to verify that the software coming in has not been tampered with and comes from an authority that can push these updates. It is much more important to ensure that your signature verification is post-quantum-secure, because if you can deploy devices that have a post-quantum-secure boot and update process now, then later on, you can push and migrate the other parts on your system. For NXP and our embedded customers, the priority is to focus on migrating these two parts first.

10.CrowdStrike CEO summoned to explain epic fail to US Homeland Security committee

by Richard Speed
https://www.theregister.com/2024/07/23/crowdstrike_ceo_to_testify/?utm_source=daily&utm_medium=newsletter&utm_content=top-article

The US House Committee on Homeland Security has requested public testimony from CrowdStrike CEO George Kurtz in the wake of the chaos caused by a faulty update.

Mark E Green, Chairman of the Committee on Homeland Security, and Andrew R Garbarino, Chairman of the Subcommittee on Cybersecurity and Infrastructure Protection, signed the letter.

Kurtz has been asked to show up before 1700 ET on July 24 for a hearing. We hope he's not flying Delta to Washington DC, as the US airline has canceled more than 5,000 flights since Friday as a result of CrowdStrike's update file crashing Windows systems.

The committee letter reads: "We cannot ignore the magnitude of this incident, which some have claimed is the largest IT outage in history. In less than one day, we have seen major impacts to key functions of the global economy, including aviation, healthcare, banking, media, and emergency services."

The full impact of the outage has yet to be determined and may never be. Green and Garbarino listed the thousands of commercial flights cancelled in the US alone, disruptions to emergency call centers, and surgery cancellations as among the consequences of the broken update.

While expressing relief that the chaos was not the result of a cyberattack, the chairmen noted: "This incident must serve as a broader warning about the national security risks associated with network dependency. Malicious cyber actors backed by nation-states, such as China and Russia, are watching our

response to this incident closely."

"Recognizing that Americans will undoubtedly feel the lasting, real-world consequences of this incident, they deserve to know in detail how this incident happened and the mitigation steps CrowdStrike is taking."

While the letter is a request for Kurtz to show up for questions, he could also be subpoenaed to provide testimony. *The Register* asked CrowdStrike if its CEO planned to put in an appearance.

Kevin Benacci, Senior Director, Corporate Communications, CrowdStrike, told us: "CrowdStrike is actively in contact with relevant Congressional Committees. Briefings and other engagement timelines may be disclosed at Members' discretion."

Kurtz said on Twitter X on July 19: "As this incident is resolved, you have my commitment to provide full transparency on how this occurred and the steps we're taking to prevent anything like this from happening again."

The incident was caused by a malware signature update issued by CrowdStrike, which resulted in its Falcon software crashing on Windows.

The software runs at a low level within the Windows kernel, resulting in Windows crashing with a Blue Screen of Death every time it boots.

According to figures from Gartner, CrowdStrike had an Endpoint Protection Platform market share of 14.7 percent in 2023, second only to Microsoft's 40.2 percent. As such, the update was able to wreak havoc around the globe on millions of Windows devices.

11.The Long-Term Forecast for Quantum Computing Still Looks Bright

by Jean-François Bobier, Matt Langione, Cassia Naudet-Baulieu, Zheng Cui, and Eitoku Watanabe
https://www.bcg.com/publications/2024/long-term-forecast-for-quantum-computing-still-looks-bright

A lot has happened since 2021, when we published our forecast for the quantum computing market. Both the new technology and its classical computing alternative have advanced in unforeseen ways, changing the trajectory, if not the overall direction, of the developing market. It's time to update our analysis.

Where Quantum Computing Stands Versus Its Potential and the Competition

The key question is whether quantum computing is finally nearing a point where it can fulfill its transformative potential. The answer, right now, is mixed.

Challenges persist. Quantum computing today provides no tangible advantage over classical computing in either commercial or scientific applications. Though experts agree that there are clear scientific and commercial problems for which quantum solutions will one day far surpass the classical alternative, the newer technology has yet to demonstrate this advantage at scale. Fidelity—the accuracy of quantum operations—is still not up to par and hinders broader adoption. Meanwhile, classical computing continues to raise the bar thanks to the big strides it has taken in hardware (such as GPUs), algorithms, and ar-

tificial intelligence (AI) libraries and frameworks.

At the same time, quantum is showing undeniable momentum. The number of physical qubits on a quantum circuit—a key indicator of computing capability—has been doubling every one to two years since 2018, reflecting significant technological progress. This trend is expected to continue for at least the next three to five years.

Despite a 50% drop in overall tech investments, quantum computing attracted $1.2 billion from venture capitalists in 2023, underscoring continued investor confidence in its future.

Governments around the world are active in this area, too. Led by the US and China, they have been making big investments in the technology, envisioning a future in which quantum computing plays a central role in national security and economic growth. Public sector support is likely to exceed $10 billion over the next three to five years, giving the technology enough runway to scale.

This article navigates these contrasting narratives, examining how the persistent hurdles and burgeoning advances could coalesce to unleash quantum computing's potential.

The Challenges of Value Creation in the NISQ Era

Three years ago, we expected the market to mature in three phases, and this is still the case: noisy intermediate-scale quantum (NISQ), until 2030; broad quantum advantage, 2030–2040; and full-scale fault tolerance, after 2040. (See Exhibit 1.)

Exhibit 1 - Value Creation and Market Phases Forecast (2021 Report)

	NISQ (before 2030)	Broad quantum advantage (2030–2040)	Full-scale fault tolerance (after 2040)
Total annual value creation for end users (in operating income)	$5 billion–$10 billion	$80 billion–$170 billion	$450 billion–$850 billion
Total annual value for providers (in revenue, ~20% of value creation)	$1 billion–$2 billion	$15 billion–$30 billion	$90 billion–$170 billion

Source: BCG analysis.
Note: NISQ = noisy intermediate-scale quantum.

We also remain confident about our projection that quantum computing will create $450 billion to $850 billion of economic value, sustaining a market in the range of $90 billion to $170 billion for hardware and software providers by 2040. (This projection is consistent with the projected market for high-powered computer providers, which is expected to reach $125 billion by 2040 according to Statista.)

Our assumptions for near-term value creation in the NISQ era have proved optimistic, however, and require revision. Accordingly, some companies in some industries will need to rethink how they approach quantum technology.

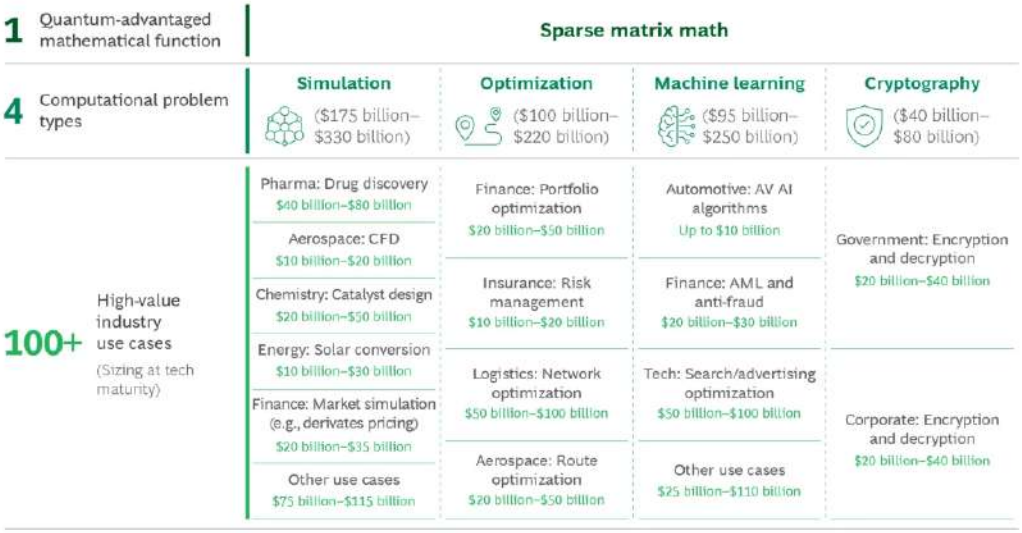
We based our initial projections on two key criteria that we assessed would lead hardware and software advances to converge at a point where they could then surpass the performance of classical computing:

- **Hardware Performance.** We expected quantum volume (as measured by the number of qubits and their fidelity) to double every one to two years.
- **Software Performance.** We anticipated that new quantum algorithms would be developed to

harness quantum hardware better and accelerate benefits (such as by increasing speed, improving the efficiency of energy usage, and unlocking new uses) over classical computing in affected use cases.

For our 2021 forecast, we assessed more than 100 use cases stemming from four types of computational problems where quantum could have a technological advantage: simulation, optimization, machine learning, and cryptography. (See Exhibit 2.)

Exhibit 2 - BCG's 2021 Forecast by Use Case Category



Sources: Industry interviews; BCG analysis.

Note: AML = anti-money laundering; AV AI = audiovisual artificial intelligence; CFD = computational fluid dynamics.

In our assessment, we assumed that developers and users would pursue three types of use cases: optimal, intractable, and brand new.

Optimal. For many complex optimization, simulation, and machine-learning problems, classical computers employ heuristic approaches to find solutions that typically fall within a 5% to 20% margin of error of the optimal answer. Many experts expected near-term quantum solutions to narrow that margin with better accuracy and to deliver their solutions more quickly.

Unfortunately, NISQ algorithms (such as the quantum approximate optimization algorithm and the variational quantum eigensolver) also rely on heuristic methods, with greater inherent uncertainty than classical solvers, which benefit from years and even decades of experience and hardware improvements. Classical solvers and AI algorithms are likely to outperform quantum computing on most intractable problems until error correction can decisively demonstrate advantage.

Intractable. Quantum computers can solve some problems that are beyond the capabilities of classical computers. As the size of these "intractable" problems increases, the time and computational resources required to solve them exactly (as opposed to approximately) grow exponentially, making them unmanageable for classical machines. Examples include computing the color emitted by a dye, the conductivity of a material, and the properties of a molecule in a drug. For practical systems, exact calculations require more transistors than there are atoms in the universe—which is why Richard Feynman proposed quantum computing in 1981.

The word *exact* (with regard to both accuracy and precision) is important. AI has made inroads into prob-

lems considered intractable at the time of our 2021 publication, and this has led to speculation that quantum computing may have a lesser role to play in tackling these problems because AI solutions could offer a “good enough” alternative. The reality is more nuanced. AI relies on learning solutions from data (such as in the case of large language models, which learn from semantic relationships in existing language and data). The availability and quality of training data sets impose inherent limitations on the accuracy and precision of AI answers. Quantum computing does not suffer from such constraints and thus offers superior capabilities.

By design, AI faces two major limitations: the results contain a certain degree of error, and they lose accuracy as they venture further from the training data set. In the large-molecule universe, including proteins, which is thought to be in the 10^{50} range, we can assume there will never be enough training data to represent the possibilities faithfully. Quantum computing will likely remain the best solution for today’s intractable problems, notably by simulating nature as Feynman envisioned.

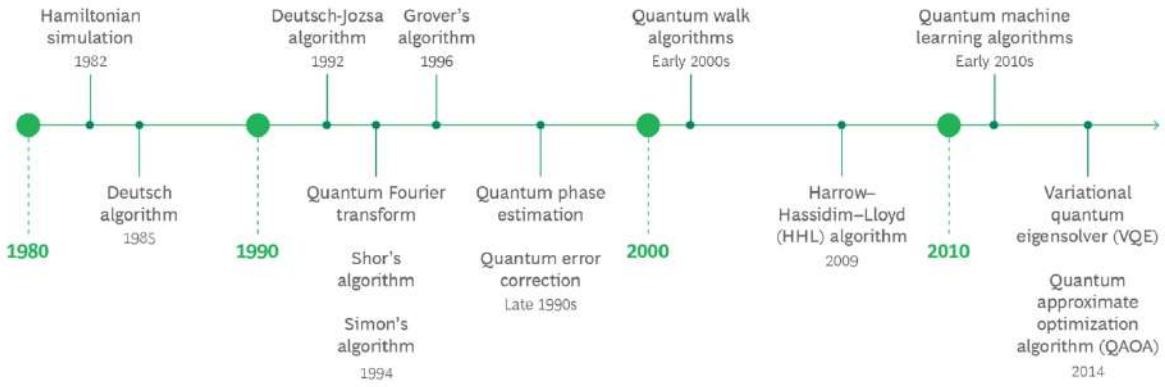
Brand New. These are use cases that we don’t know we will need yet, in the same way that ridesharing became obvious and all but indispensable once smartphones made it possible. Our 2021 and current market forecasts estimate that brand new use cases will generate 20% to 30% of future value, based on prior introductions of new technology.

Hardware and Software Fall Short

The NISQ era has not lived up to our expectations for two reasons. First, technical hurdles in hardware development are proving tough to overcome. Qubit numbers have been increasing fast, but fidelity remains a big issue. Analysis by the community-driven platform Metriq, which tracks quantum technology benchmarks, suggests that with existing software, most valuable use cases require both 10,000 to 20,000 qubit-gate operations and close to 100% gate fidelity. But circuits of more than 30 qubits have so far achieved at best a 99.5% fidelity rate (a barrier that was only partially broken in April 2024 when collaborative efforts by Microsoft and Quantinuum on their H1 systems reached a "three nines" rate for 2-qubit gates). Because errors accumulate exponentially, even the best hardware fails after about 1,000 to 10,000 qubit-gate operations. Useful algorithms need millions of gate operations (even billions in the case of Shor’s algorithm), so quantum machines still need to improve by many orders of magnitude.

Development of new algorithms has lagged, too. In fact, most significant algorithm advances were formalized between the 1980s and the 2010s. Little progress has occurred in the past ten years. (See Exhibit 3.)

Exhibit 3 - A Timeline of Key Algorithm Development



Source: BCG research.

Second, competition from classical computing has been fiercer than we anticipated. In particular, AI has exceeded expectations in scientific fields, offering viable alternatives for previously intractable problems. In the long run, quantum computing will bring definitive advantages to handling highly complex problems—such as many-body physics and NP-hard optimization—over classical solvers, which rely on imperfect heuristic and approximate algorithms. NISQ limitations force current quantum algorithms to depend on heuristic approaches too, and this reliance makes advantage impossible to prove consistently, if there is any.

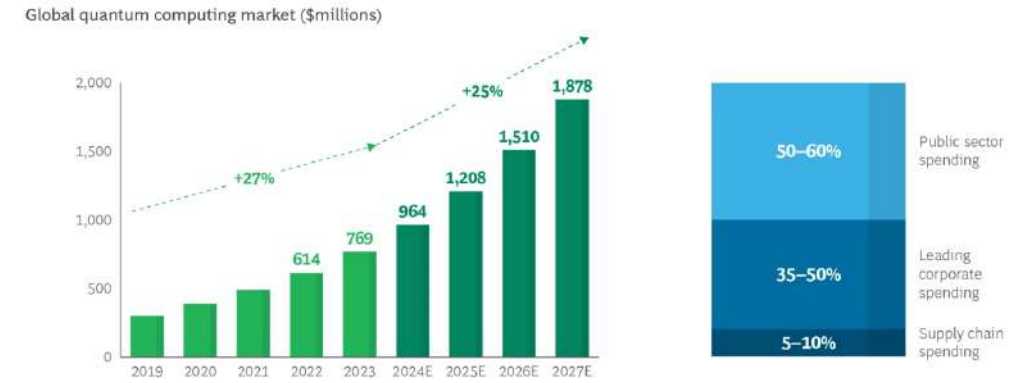
Together, these factors have prevented quantum computing from realizing a definitive advantage over classical systems in both hardware and software capabilities, at least through the approach based on digital gates. There are alternatives. Companies such as D-Wave, Pasqal, Kipu Quantum, and Qilimanjaro have chosen to pursue analog and hybrid (analog combined with few gates) quantum computing. These approaches could unlock commercial use cases in the short term without needing too many gate operations.

Recent advances confirm that quantum computing continues to achieve significant progress. Innovative prototypes have demonstrated substantial improvements in solving complex problems, showcasing the potential for optimization, quantum simulations, and material simulations. The development of application-specific quantum chips and the expansion of cloud-based quantum computing services highlight the movement toward delivering practical and scalable quantum solutions.

The Impact on Providers

By leveraging analog methodologies, quantum machines can still deliver tangible near-term value, especially in materials and chemicals simulations, ranging from $100 million to $500 million a year during the NISQ era. Although this forecast is significantly lower than our previous projection, we do not expect it to have a major impact on the market for hardware and software providers. We continue to foresee a provider market in the range of $1 billion to $2 billion by 2030, in line with projections by others.

Exhibit 4 - Public Sector Spending Will Continue to Support the Growth of the Quantum Computing Market



Source: Hyperion Research.

Three factors are in play here. First, as it has done in the past with technologies such as semiconductors, the internet, and GPS, the public sector is providing substantial support through orders and grants. For example, the UK Ministry of Defence has purchased quantum computers from ORCA Computing even though these machines do not yet the break the 40-qubit threshold that a classical high-powered computer can simulate. We estimate that public orders of quantum computers already support more

than half of the market. Given existing program announcements and the geopolitical importance of quantum technologies, this level of demand should persist over the next three to five years. (See Exhibit 4.)

Second, leading corporations are investing in enterprise-grade quantum capabilities. In a 2023 publication on quantum adoption, we tracked more than 100 active proof-of-concept projects among Fortune 500 companies, representing a total investment of about $300 million. These companies have ambitions to become first movers—for example, by filing patents for promising materials discovered with quantum computers or by devising hedging strategies that more rapidly exploit market imperfections. Despite AI advances and NISQ setbacks, we expect more companies to pursue long-term programs in the coming years, thanks to the tangible prospects for technological advances, notably in error correction, and to use of AI as a source of training data with little overlap in use cases.

Third, providers can generate revenues by forming supply chains that involve such equipment as controls, dilution fridges, lasers, vacuums, and software. We estimate that supply chain spending will account for 5% to 10% of quantum computing hardware and software revenues this year.

Error Correction Will Accelerate Progress

The prospects for qubit error correction were theoretical and uncertain in 2021. Most experts predicted achievement of this milestone sometime after 2030; some said that it would never materialize. But the past three years have seen substantial practical advances. A collaboration among Harvard, QuEra, MIT, and NIST/UMD demonstrated error correction with 48 logical qubits on the neutral atoms platform. Superconducting qubit leader IBM created another innovative error-correcting code—one that is ten times more efficient than prior methods. Recently, Microsoft and Quantinuum demonstrated an 800-times error reduction with trapped ions. Other clever innovations such as stronger hardware encoding (by the quantum design firm Alice & Bob) have also come into play since 2021, fostering growing optimism about the practicality of error correction.

In our 2021 forecast, we noted that 90% of the total calculated value was contingent on improvement in error correction. Public roadmaps from IBM, QuEra, and Alice & Bob, among others, promise to achieve full error correction by 2029 at the latest. Its sooner-than-expected arrival will accelerate time-to-value for end users in the medium term.

Enterprise Impact

The bottom line is that while quantum computing remains an exciting prospect in some sectors, the technology remains in its infancy and offers limited immediate value for most enterprises. Not all industries will want to embark on the quantum journey. Investment is most clearly justifiable for companies that can capitalize on significant gains as soon as error correction improves (through transformative advances in molecular development, for example) or that seek a first-mover advantage (such as quantum computing services provided by tech giants or cybersecurity enhancement through new decryption methods).

Five industries (followed by the public sector) top the list of those positioned to benefit from error-corrected quantum computing. The technology provides each with its own set of benefits:

- **Technology companies** need to stay ahead in tech race, and being first (or early) to provide quantum computing and hybrid tech services will put tech providers in a strong competitive position, potentially for decades to come.

- **Chemicals and agricultural companies** will find quantum computing a powerful tool to enhance their molecular modeling and simulation capabilities, leading to breakthroughs in material science

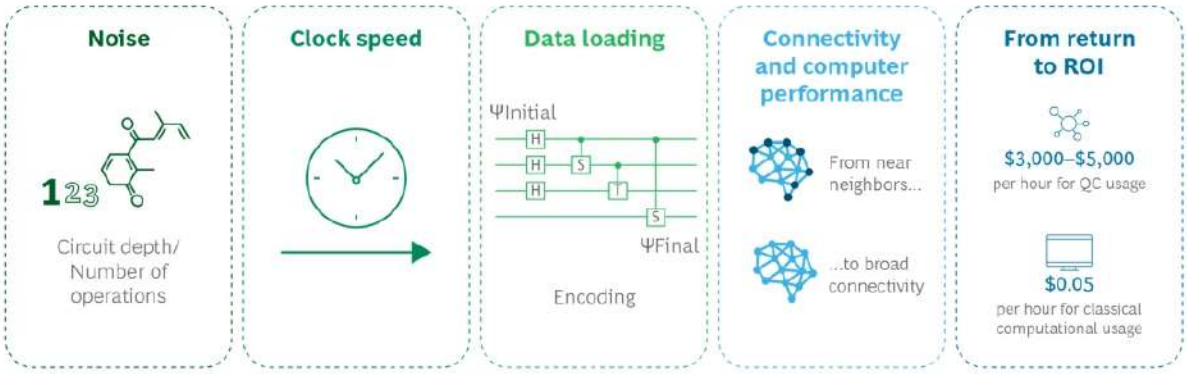
and crop protection.

- **Pharmaceuticals companies** will be able to model complex molecular interactions at unprecedented speeds, accelerating drug discovery and reducing time-to-market for new medications.
- **The defense and space industry** will achieve significant advances in secure communications, complex system simulations, and other technologies critical for national security and advanced aerospace projects.
- **Financial institutions** will gain the ability to process vast amounts of data for risk assessment and portfolio optimization, providing a competitive edge in a fast-paced market.

Shifting Focus

There is a strong focus today on enabling manufacturers to increase the number of qubits in a quantum processor. This is undeniably key in the quantum race. Still, we expect the focus of development to broaden to encompass additional criteria as users seek to fully harness emerging value. (See Exhibit 5).

Exhibit 5 - Developers' Focus Will Broaden to Include Factors in Addition to Qubit Count



Source: BCG analysis.
Note: QC = qubit count.

Noise. As mentioned earlier, low fidelity rates prevent NISQ-era algorithms from providing real ROI in the near term. At least in the case of digital computing, it will be necessary to implement error correction code to drastically reduce noise and permit increased circuit depth.

Clock Speed. Speed is another variable that may need to improve, since quantum computers today are slow compared with their classical counterparts. There is a big difference even among the different quantum computing modalities. For example, the current state-of-the-art performance level for cold atom systems is thought to be in the kHz range, but we expect superconducting qubits to reach clock speeds in the MHz range. Slower operational speeds impose severe limitations on practical applications. According to a 2006 study on the architecture-dependent execution time of Shor's algorithm, factoring a 576-bit number within a month requires a clock rate of 4 kHz, while a clock rate of 1 MHz could complete the task in about three hours. As algorithms emerge that provide exponential advantage over classical methods, quantum computing's clock speed limitations will diminish.

Data Loading. The ability to load data into a quantum computer is a key bottleneck today. Solving a computational problem typically starts with encoding the information into the bits of the computer. The problem is that qubits are scarce. Smart algorithms can map the data in the computer with a minimum of requirements, but quantum machines are far from competing with the terabytes of processing power available in classical computers. An alternative approach that avoids loading classical data would be to compute directly from a native quantum state—for instance, with data coming from a previous computation or from quantum sensors.

Connectivity and Computer Performance. Defined as the ability to apply gates between distant qubits, connectivity is crucial for maximizing the speed and efficiency of quantum algorithms. Therefore, it will play a significant role in a quantum architecture's ability to implement efficient error correction code. Some quantum technologies, such as trapped ions and neutral atoms, already benefit from high intrinsic connectivity, but alternative technologies, such as superconducting and silicon qubits, are usually limited to near-neighbor connectivity (linking only with adjacent qubits) and so experience computational overhead (by moving qubits around the circuit at every step).

From Return to ROI. The focus of financial assessments will shift over time from expectations for long-term return to near-term ROI. Quantum computing is currently 100,000 times more expensive per hour than classical computing ($1,000 to $5,000 per hour for quantum machines compared with $0.05 per hour for classical computing), but we expect this gap to shrink with increasing scale over time. While this comparison does not account for qualitative differences in outcomes, it does highlight that not all use cases will derive sufficient value from quantum computing to justify the cost. Moreover, corporate buyers typically aim for a one-year break-even point—although a three- to five-year break-even target may be acceptable in certain cases. In this scenario, the most favored use cases for quantum technologies will be those that promise a rapid ROI.

The More Things Change…

A lot has indeed changed since 2021. Perhaps the most remarkable thing, though, is the stability of the overall picture. Impediments to quantum computing in the near term, such as circuit depth and fidelity rates, do not threaten the long-term development of the technology or the market. The challenges of 2021 are still the challenges today, and they are closer to resolution. Quantum computing is still on track to create enormous value in sectors where it can solve business problems faster or better. End users need to build out their partnerships with providers and develop their own skill sets because today as in 2021 quantum computing remains a winner-take-most technology.

12.QuSecure Collaborates with NVIDIA to Support cuPQC, Post-Quantum Cryptography Library

by Ariana Lynn
https://www.thefastmode.com/technology-solutions/36395-qusecure-collaborates-with-nvidia-to-support-cupqc-post-quantum-cryptography-library

QuSecure last Friday (12 July) announced it has joined NVIDIA and a select group of technology leaders in supporting NVIDIA's cuPQC, a recently launched pioneering library set to redefine cryptography in the quantum era. NVIDIA's cuPQC leverages the unmatched parallelism of NVIDIA GPUs to meet the rigor-

ous demands of next-generation security algorithms, marking a monumental leap in bringing PQC to environments that stand to benefit most from their protection, including telecommunications, insurance, banking and finance, critical infrastructure, and the public sector, all of which QuSecure currently and actively supports.

According to the company, the threats from quantum computing pose unprecedented challenges to current cryptographic standards, with the potential to compromise the public keys safeguarding today's communications, including the global internet. Recognizing this urgency, governmental and industry efforts are intensifying to devise robust PQC solutions, with cryptographers working on advanced algorithms to replace today's public keys. QuSecure, at the forefront of cryptographic innovation, is supporting and collaborating with NVIDIA to promote the availability of potent computational resources to foster the development and validation of advanced algorithms destined to replace existing public keys.

In groundbreaking benchmarks, cuPQC has already demonstrated remarkable acceleration of Kyber, a leading candidate for securing quantum-resistant keys, achieving speeds multiple times faster on an NVIDIA H100 Tensor Core GPU than on traditional CPU benchmarks. The forthcoming NVIDIA Blackwell architecture GPUs are optimized for the intricate integer mathematics pivotal in cryptography and aim to amplify this acceleration.

13.Raman Research Institute Achieve Breakthrough in Quantum Cybersecurity

by BL Chennai Bureau
https://www.thehindubusinessline.com/news/science/raman-research-institute-achieve-breakthrough-in-quantum-cybersecurity/article68405699.ece

Scientists at the Quantum Information and Computing (QuIC) lab of the Raman Research Institute, Bengaluru, have reported "a major breakthrough" in cybersecurity.

They've created a new way to generate truly unpredictable random numbers, crucial for stronger quantum communications encryption. "This could revolutionize how we protect sensitive data in the future," says a press release from the Department of Science and Technology, Government of India.

The security of quantum communications relies on inherent randomness. The QuIC scientists performed "a photonic experiment" to demonstrate a violation of the Leggett Garg Inequalities (LGI), a litmus test for "quantumness" in a system.

Taking this further, over the last few years, the group carried out extensive research in collaboration with researchers from the Indian Institute of Science (IISc), Bengaluru, IISER-Thiruvananthapuram and the Bose Institute, Kolkata, to use such LGI violations in a completely unexplored domain-- truly unpredictable random number generation, secure against device tampering and imperfections. These numbers are crucial in applications like cryptographic key generation, secure password creation and digital signatures, among others.

In today's digital world, where we rely heavily on technology, strong passwords are vital for everyone's safety. This new method offers the enhanced protection we all need daily. Researchers noted that it uses truly random numbers to generate keys that will be used to encrypt the passwords.

"It is resilient against attacks on the initial state, which is typically the most vulnerable point in this

scheme. The certified random numbers are important because any predictability of these numbers can compromise the entire security system, making it vulnerable to attacks. These numbers ensure the robustness of encryption, authentication and data integrity processes and maintain trust and security in digital interactions," says Urbasi Sinha, faculty at RRI.

There are several advantages to generating certified random numbers using this method.

"These include the creation of strongly protected passwords, enhanced account security by resisting brute-force attacks, ensuring uniqueness, integrity thereby preventing forgery and token generation with multi-factor authentication, adding a crucial security layer in this vulnerable cyber world," said Debashis Saha, IISER Thiruvananthapuram faculty and co-author of the study.

The experiment generated over 9,00,000 random bits rapidly, nearly 4,000 bits/second. This high random number generation can help use these numbers towards applications that require rapid randomness.

With further engineering interventions and innovations, devices adopting this method could find powerful applications not only in cybersecurity and data encryption but also in the context of varied types of randomness-based simulations and randomized control trial statistical studies in diverse important areas.

"These include economic surveys, drug designing/testing, as well as for any futuristic technology that would rely on provable unpredictability as a critical resource", said Bose Institute's Professor Dipankar Home, another co-author of the study.

14.How Post-Quantum Cryptography Can Ensure Resilience

by Nils Gerhardt
https://technative.io/how-post-quantum-cryptography-can-ensure-resilience/

For several years, quantum computing has been a question of when, not if – but it's accelerating fast, and organizations must start preparing now for its impact.

Quantum computing brings new security implications: because its compute power is significantly higher than that of conventional computers, it could decrypt the encryption that lies at the heart of digital security.

The National Security Agency (NSA) released an updated *Commercial National Security Algorithm* (CSNA) paper with recommendations and guidance on implementing post-quantum cryptography (PQC). The NSA is recommending that all organizations become post-quantum secure by 2030.

It's an aggressive timeline that underscores the severity of the problem. And it highlights the reality that current encryption methodologies won't suffice.

Quantum computing has changed the game

While quantum computers aren't being developed with the goal of cracking existing cryptography, their potential computing powers mustn't be underestimated. And as with any emerging technology, there will likely be bad actors who use this tech for malicious purposes.

Quantum computing represents a major threat to data security, as it can make attacks against cryptography much more efficient. There are two ways bad actors could use this technology. One is the "Store now, decrypt later" method, in which cybercriminals steal sensitive data and wait until quantum computers have the ability to break its encryption. This is particularly important for you to know if your organization retains data with a long confidentiality span.

The other method is to break the data's digital signatures. A bad actor could "compute" credentials based on publicly available information, then impersonate someone with the authority to sign documents or approve requests. As with the above message, criminals can do this retroactively if older signatures are not updated.

Today's encryption methods cannot stand against the capabilities of tomorrow's quantum computers. When large-scale quantum computers are built, they will have the computing ability to decrypt many of the current public key cryptography systems. As mentioned earlier, this would have far-reaching consequences for the integrity and privacy of digital communications.

Current algorithms (like RSA or ECC) are designed to require thousands of years to decrypt using classical computing; quantum computers could do this work in a matter of hours. This significant difference is the core threat that quantum computing represents and the reason that the cybersecurity industry must address it.

Leveling up your cryptography for the quantum decryption age

According to NIST guidance, RSA-2048 – a widely used encryption system – is only considered secure until 2030. While quantum computing is still a few years away, the time to start planning is now. There are always people who doubt the timeline of quantum computer readiness, but the point isn't whether or not quantum computers will exist with 100% certainty in 2030 to break today's crypto.

Imagine you will have a Y2K scenario with potentially devastating effects to the whole of society in terms of finances, safety, revealed secrets and more. You don't know when this "Q-Day" will be, but you do know that the likelihood of this day being in 2030 is NOT zero. What would you do? Almost everyone will agree that you have to start preparing now to avoid such catastrophic outcomes, whether anything will happen in 2030 or whether it happens later.

NIST notes that the goal of post-quantum cryptography is to develop cryptographic systems that are secure against both quantum and classical computers. Planning your post-quantum cryptography migration now is essential to ensure the long-term security of your data and applications. Quantum computers may be rolled out earlier than the current expectation of 2030, and cryptography discovery and migration will take time. In addition, legacy code and libraries will be around for a long time. Doing everything possible now is the key to ensuring data security.

Understanding PQC in practice: Two use cases

It's useful to examine real-world use cases to drive home both the serious nature of the threat and the efficacy of the solution. The first example is using quantum-proof digital signatures and encryption for long-term secure satellite communication.

The CCSDS Space Data Link Security Protocol requires cryptographic algorithms for authentication, encryption and authenticated encryption. The algorithms and methods used were XMSS, including state handling (signatures), CRYSTALS-Kyber (the key encapsulation mechanism) and key injection for long-term secure firmware updates.

The second example is securing firmware updates for chips using post-quantum cryptography. The organization used the CRYSTALS-Dilithium (signatures) and CRYSTALS-Kyber (encryption) algorithms and the following methods:

- Generation of CRYSTALS-Dilithium key pair in the hardware security module (HSM)
- Cryptographic key injection (Public Dilithium key) during chip manufacturing
- Signature verification in the field
- Confidentiality achieved by encrypting with CRYSTALS-Kyber

This protocol solved the challenges of memory space on the chips and protection against side channel attacks.

Preparation is power

The cybersecurity sector has permanent job security because as long as there is new technology, there will be bad actors exploiting it for their evil purposes. Quantum computing is just the next technology that security professionals need to stay on top of. 2030 may seem like a faraway date, but some feel that it's hardly enough time to make the transition to PQC. It's important to begin that transition process now so that you can meet Q-Day with confidence, whenever it arrives.

15.Forrester: Security leaders stall on post-quantum migration despite high-level concerns

by Nancy Liu
https://www.sdxcentral.com/articles/analysis/forrester-security-leaders-stall-on-post-quantum-migration-despite-high-level-concerns/2024/07/

Despite high-level awareness and mounting concerns over the impending quantum threat, security leaders are "taking baby steps" on implementing post-quantum encryption (PQE), awaiting further developments, standards, vendor, and open-source product announcements, according to Forrester's latest 2024 State of Quantum Security report.

The report underscores the urgency for organizations to prepare for Q-Day – the day when quantum computers will have the capability to break traditional asymmetric cryptography and algorithms.

"Q-Day, when quantum computers can break traditional, asymmetrical encryption may be in the future, but preparation is in full swing," stated Forrester VP and principal analyst Andras Cser.

However, the analyst firm noted industry progress on PQE implementation has been slow. While 71% of surveyed security leaders feel knowledgeable about quantum computing as an emerging technology, only 21% of the respondents rank it among the technologies causing the most concern. This highlights a significant gap between awareness and actionable progress.

"Some organizations hear that post-quantum is 15 years out, and it's hard to get that tension," Steve Stevens, the executive director of financial industry standards body X9, stated in the Forrester report.

Mixed messages for post-quantum migration

Forrester noted when planning for the post-quantum migration, security and research leaders often have to contend with some mixed messages, including:

- **NIST's repeated competitions risk slowing algorithm adoption.** The National Institute of Standards and Technology (NIST) in 2022 revealed the first group of winners from its post-quantum cryptography competition, which was initiated in 2016. Many security leaders are still waiting for NIST's post-quantum cryptography (PQC) standards, which are expected to be released this year.

- **Government agencies are waiting on NIST but want the private sector to start planning.** Despite closely following NIST, government agencies globally offer broader and more aggressive recommendations. For example, the Germany's BSI information security office strongly encourages post-quantum migration, emphasizing hybrid implementation with classical schemes, while starting work on an open-source library with some of the post-quantum algorithms.

- **Industry organizations and consultancies push inventory but then hit a wall.** Security industry associations and consulting firms currently focus on advising their members and customers on how to discover and inventory encrypted data and the algorithms used to encrypt it. Another common theme among organizations is to ask third parties for their migration plans.

"While NIST has been working on standardizing PQE algorithms, post-quantum algorithms have not yet been vetted," Cser explained. "However, we expect that data discovery, prioritization, and value assessments will be critical; commercial solutions will be available for discovering and replacing/augmenting current vulnerable encryption algorithms; and existing cloud and [on-premises] key management solutions will continue to play an important part in post-quantum key management."

Tech giants start implementing post-quantum security measures

Forrester pointed out that some leading tech companies and organizations like Google and Cloudflare have begun implementing post-quantum algorithms, and Apple's recent announcement of PQ3 for iMessage is another notable push.

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

Palo Alto Networks, a major player in the traditional cybersecurity industry, is also leaning into quantum security. The vendor has started implementing quantum-resistant capabilities across its technologies while partnering with federal agencies and other industry peers for PQC migration.

In February, the Linux Foundation announced the launch of the Post-Quantum Cryptography Alliance (PQCA). The founding members of this initiative include Amazon Web Services (AWS), Cisco, IBM, IntellectEU, NVIDIA, QuSecure, SandboxAQ, and the University of Waterloo.

16.Announcing AES-GEM (AES with Galois Extended Mode)

by Scott Arciszewski
https://blog.trailofbits.com/2024/07/12/announcing-aes-gem-aes-with-galois-extended-mode/

Today, AES-GCM is one of two cipher modes used by TLS 1.3 (the other being ChaCha20-Poly1305) and the preferred method for encrypting data in FIPS-validated modules. But despite its overwhelming success, AES-GCM has been the root cause of some catastrophic failures: for example, Hanno Böck and Sean Devlin exploited nonce misuse to inject their Black Hat USA slide deck into the MI5 website.

Security researchers have been sounding the alarm about AES-GCM's weaknesses for years. Nineteen years ago, Niels Ferguson submitted a paper to a NIST project on block cipher modes outlining authentication weaknesses in AES-GCM (although NIST would ultimately standardize it). And earlier this year, Amazon published a paper that detailed practical challenges with AES-GCM and posited that AES' 128-bit block size is no longer sufficient, preferring a 256-bit block cipher (i.e., Rijndael-256).

To address these issues, I propose a new block cipher mode called Galois Extended Mode (GEM for short), which I presented last month at the NIST workshop on the requirements for an accordion mode cipher. AES-GEM improves the security of GCM in every dimension with minimal performance overhead.

Important: The current design for AES-GEM is not ready for production use, as some details will likely change in the future. To understand the current design, let's start by understanding where AES-GCM falls short, and then discuss how we can do better with GEM.

How AES works

Before we dive in, it may be helpful for some readers to explain some of the terms and concepts used throughout this blog post.

AES (Advanced Encryption Standard) is a block cipher widely used to encrypt information. It supports multiple key sizes (128-, 192-, and 256-bit keys) but always operates on 128-bit blocks. AES is the standardized form of the Rijndael family of block ciphers. Rijndael supports other block sizes than 128-bit, but only the 128-bit blocks were standardized by NIST. Modern processors provide dedicated hardware instructions for accelerating AES operations, but the AES key schedule can still negatively impact performance.

ECB (Electronic Code Book) mode is the absence of a block cipher mode of operation. It involves computing the block cipher directly on a block of data. ECB mode is not semantically secure, as many cryptographers have demonstrated. For improved security, block ciphers like AES are typically used with a mode of operation. (If not, they almost certainly should be. Get in touch with our cryptography team if you think you're using ECB to encrypt sensitive data.)

CTR (Counter Mode) is a mode of operation for block ciphers wherein an increasing sequence of values is encrypted with the block cipher to produce a pseudorandom keystream. To encrypt data, simply calculate the XOR of each plaintext byte with each corresponding keystream byte.

GCM (Galois/Counter Mode) is a block cipher mode of operation that provides authenticated encryption. It is what cryptographers call an AEAD mode: Authenticated Encryption with Additional Data. GCM can provide confidentiality for sensitive data and integrity for both sensitive and public data.

AEAD modes are important for designing cryptosystems that are resilient to attackers who attempt to mutate encrypted data in order to study the system's behavior in hopes of learning something useful for cryptanalysis.

GCM is a composite of Counter Mode (CTR) for encrypting the plaintext and a Galois field Message Au-

thentication Code (GMAC), which authenticates the ciphertext (and, if provided, additional associated data). GMAC is defined with a function called **GHASH**, which is a polynomial evaluated over the authenticated data. The output of GHASH is XORed with an encrypted block to produce the final authentication tag. The authentication key, called H, is calculated by encrypting a sequence of 128 zeroed bits.

POLYVAL is an alternative to GHASH that is used in AES-GCM-SIV. The irreducible polynomial used by POLYVAL is the reverse of GHASH's irreducible polynomial.

Many cipher modes (including GCM and CTR) require a number that is used only once for each message. This public number that should never be repeated is called a **nonce**.

Finally, the **birthday bound** is a concept from probability theory that indicates the likelihood of collisions in a set of random values. In cryptography, it implies that if nonces are selected randomly, the probability of two nonces colliding increases significantly as more nonces are used. For AES-GCM with 96-bit nonces, after about 2^{32} messages, there's a 1 in 2^{32} chance of a nonce collision, which can lead to security vulnerabilities such as the ability to forge messages.

Practical challenges with AES-GCM today

The biggest challenge with AES-GCM, as others have pointed out, is that AES only has a 128-bit block size. This has two primary consequences:

The size of the public nonce and internal counter is constrained to a total of 128 bits. In practice, the nonce size is usually 96 bits, and the counter is 32 bits. If a larger nonce is selected, it is hashed down to an appropriate size, which has little improvement on security. If you ever reuse a nonce, you leak the authentication subkey and can, therefore, forge messages indefinitely.

Above a certain number of blocks encrypted under the same key, an attacker can distinguish between ciphertext and random bytes with significant probability.

When you understand that we're dealing with powers of two, 96 bits of nonce space may sound like a lot, but if you're selecting nonces randomly, you can encrypt only 2^{32} messages before you have a 2^{-32} probability of a collision. Using a cipher with a larger block size would alleviate this pain point, but it's not the only way to fix it.

The AES block size is not the only problem with AES-GCM in practice. As Niels Ferguson pointed out in 2005, a successful forgery against short tags reveals the authentication subkey.

Further, we also learned that AES-GCM has an unexpected property where multiple keys can decrypt the same ciphertext + authentication tag. Its discoverers referred to this problem as Invisible Salamanders because it allowed them to hide a picture of a salamander from an abuse-reporting tool in an encrypted messaging application. Mitigating against Invisible Salamanders in a protocol that uses AES-GCM requires some one-way commitment of the key used.

Finally, the maximum plaintext length for a single message in AES-GCM is relatively small: just below 64 GiB. In order to cope with this maximum length, software often decomposes larger messages into shorter frames that fit within this length constraint. This leads to the limited nonce space before the birthday bound being used up much more quickly than if longer messages were tolerable.

Introducing AES-GEM

Our proposal, Galois Extended Mode, is a modification of GCM (Galois/Counter Mode) that currently addresses most of these weaknesses. However, there is still an open question about which tactic we

want to employ to mitigate the last pain point, which I will explain momentarily.

At a high level, we propose two variants: AES-128-GEM and AES-256-GEM. We also specify two AEAD constructions using the standard AEAD

AES-128-GEM

- **Key length:** 128 bits
- **Subkey length:** 128 bits
- **Nonce length:** 192 bits
- **Maximum plaintext length:** $2^{61} - 1$bytes
- **Maximum AAD length:** $2^{61} - 1$bytes
- **Tag length:** 48 bytes (AEAD) or 16 bytes (without commitment)

AES-256-GEM

- **Key length:** 256 bits
- **Subkey length:** 256 bits
- **Nonce length:** 256 bits
- **Maximum plaintext length:** $2^{61} - 1$bytes
- **Maximum AAD length:** $2^{61} - 1$bytes
- **Tag length:** 48 bytes (AEAD) or 16 bytes (without commitment)

The road from GCM to GEM

If you start with the existing design for AES-GCM and make the following changes, you will arrive at the current draft for GEM.

Nonce extension

First, we need a longer nonce, which we will use for subkey derivation in the next step.

For 256-bit keys, a 256-bit nonce is a nice round number. For 128-bit keys, we end up needing 192 bits.

In either case, the rightmost 64 bits will be reserved for the actual underlying encryption. The remaining bits (192 bits for AES-256, 128 bits for AES-128) are to be used for subkey derivation.

This allows us to amortize the cost of the key derivation and set up an AES key schedule across multiple messages, provided the first $(n - 64)$ bits of the nonce and key are the same.

Subkey derivation

There are multiple strategies for using AES for key derivation. At Real World Cryptography 2024, Shay Gueron presented DNDK-GCM, which uses an interesting construction to achieve subkey derivation.

We want to keep things simple and well-understood. Consequently, we based our key derivation strategy on CBC-MAC since CMAC is already an FIPS-approved MAC (i.e., for AES-CCM).

In the case of AES-256, we use two CBC-MAC outputs to derive a 256-bit subkey. However, this approach has one subtly annoying property: The two halves will never produce the same output, so there are, strictly speaking, fewer than 2^{256} possible outputs.

In both variants of GEM, we borrow a trick from Salsa20's design: XOR the output with the input key to ensure the subkey is indistinguishable from uniformly random to any attacker who doesn't know the input key. If you don't know this key, the output is indistinguishable from a random key of the appropriate length.

Support for longer messages

The reason we needed 64 bits of leftover nonce, rather than 96 as would be typical for GCM, is that our internal counter size is not 32 bits long. It is, instead, 64 bits long.

Otherwise, as currently written, GEM behaves identically to what you'd expect from GCM: It uses counter mode for bulk data encryption. Let's put a pin in that and revisit it in a moment.

Improved authentication security

Our incumbent design, AES-GCM, is constructed in the following way:

1. Derive an authentication subkey, H, by encrypting an all-cleared block with the key.
2. Calculate GHASH() of the ciphertext, associated data, and a block containing the lengths of both segments (in bits).
3. XOR the output of step 2 with the AES-CTR encryption of a counter block.

Our design is mostly the same, but with an important tweak:

1. Derive an authentication subkey, H, by encrypting an all-set block with the subkey.
2. Calculate GHASH() of the ciphertext, associated data, and a block containing the lengths of both segments (in bits).
3. Encrypt the output of step 2 with AES-ECB, using the input key.
4. XOR the output of step 3 with the AES-CTR encryption of a counter block.

Step 3 directly addresses the weaknesses that Niels Ferguson identified with AES-GCM in 2005. The other changes are implementation details.

This tweak offers better security for short tags since the AES encryption of the raw GHASH output bits is a nonlinear transformation that is not invertible without the key. We use the input key rather than the subkey since the only other place the input key is used to encrypt data (i.e., subkey derivation) is never directly revealed.

Key commitment

Before we tackle GEM's protection against Invisible Salamander-style attacks, we need to analyze some other subtleties of the design.

The component lengths in the final block for both GCM and GEM are both expressed in terms of bits, not bytes, and are restricted to 2^{64} each. This means that, even though GEM could theoretically allow up to 2^{64} blocks (or 2^{68} bytes) of plaintext per message due to its internal counter, we would have to tweak the final GHASH step to accommodate this extra overhead.

Instead of doing that, the unreachable values for the internal counter are reserved for the cipher's internal use. Specifically, the internal counter values that end in $0x0200000000000000$ through $0xFFFFFFFFFFFFFFFF$ cannot be reached while respecting this $(2^{61} - 1)$ byte limit on the plaintext.

The all-set block($0xFFFFFFFF\ FFFFFFFF\ FFFFFFFF\ FFFFFFFF$) is already used in GEM for the authentication subkey, while the 64-bit trailing nonce + $0XFFFFFFFF\ 0xFFFFFFFF$ is used for the counter block, for the final authentication tag calculation.

To provide key commitment, the next two blocks down, the nonce + $0xFFFFFFFF\ 0xFFFFFFFC$ and $0xFFFFFFFF\ 0XFFFFFFFD$ will serve as a commitment value for the key and nonce.

We specify two blocks because using one AES block here is not sufficient. Consider the case of AES-256, which has 256-bit keys and 128-bit blocks: by the pigeonhole principle, we expect there to be 2^{128} different keys that will map a given fixed plaintext value into a fixed ciphertext value. Therefore, a single block is not sufficient for commitment. However, no such pigeonhole consideration is necessary for two successive blocks, assuming the block cipher is secure.

In this way, we can quickly generate a commitment value for a given key and nonce.

In the AEAD interface, the commitment is appended to the authentication tag. Both must be compared to their recomputed values, in constant-time, when decrypting messages.

AES-GEM's performance characteristics

Although we've addressed most of GCM's pain points, the actual performance impact of GEM is minimal.

AES-256-GEM:

- **Key derivation:** four additional blocks of AES encryption, some XORs, one additional key schedule
- **Authentication:** one additional block of AES encryption
- **Key commitment:** two additional blocks of AES encryption

AES-128-GEM:

- **Key derivation:** two additional blocks of AES encryption, some XORs, one additional key schedule
- **Authentication:** one additional block of AES encryption
- **Key commitment:** two additional blocks of AES encryption

Since AES is very fast these days due to hardware acceleration, this performance impact should be mostly unnoticeable in all but the most performance-sensitive of applications. In those cases, the key derivation performance cost can be amortized across up to 2^{32} different messages if the derived subkey is cached.

Polishing AES-GEM

There is one final issue that the current draft of GEM does not sufficiently address, but we hope to discuss this issue at the NIST workshop and will certainly address it in the final design.

Although our draft GEM construction allows for longer messages than GCM, the AES block size makes it risky to use as-is. The primary concern is that encrypting a very long message would give an attacker a

significant advantage in distinguishing AES-GEM ciphertexts from sequences of random bytes. (This is one of the concerns raised in Amazon's 2024 paper.)

There are a few ways we can polish GEM to address this weakness, which have different performance characteristics and trade-offs.

.
.
.

17.Oxford Ionics breaks global quantum performance records

https://www.oxionics.com/news/oxford-ionics-breaks-global-quantum-performance-records?utm_source=substack&utm_medium=email

Oxford Ionics has demonstrated the highest performing quantum chip in the world, which can be produced at scale in a standard semiconductor fabrication plant.

Building stable, high-performance quantum computers is hugely challenging. It demands the creation of high-performance qubits and a way to control those qubits in a scalable way. Only one technology - trapped ions - has demonstrated the performance needed to build a useful quantum computer. However, until now, trapped ions have been difficult to scale as they are typically controlled by lasers.

Oxford Ionics has eliminated the need to use lasers to control qubits through the development of a patented Electronic Qubit Control system. This unique, embedded approach takes the highest performing qubit technology - trapped ions - and integrates everything needed to control them into a silicon chip that can be mass-produced using standard semiconductor manufacturing facilities and processes.

Oxford Ionics has set industry records in both two-qubit gate and single-qubit gate performance (fidelity). Previous world records have been achieved with the use of error correction to reduce errors in hardware[1]. Oxford Ionics chips provide **over twice the performance, without needing error correction, using 10x fewer qubits**:

- Proven implementation of two-qubit gates with fidelities at the 99.97% level
- Proven implementation of single-qubit operations with 99.9992% fidelity

Building a useful quantum computer requires high performing single and two-qubit gate operations. Oxford Ionics' significantly increased qubit performance means that powerful quantum computers can be built with far fewer qubits and that valuable commercial applications can be deployed before needing to implement complex and costly error correction techniques.

Together with the scalability of Oxford Ionics' approach, these results indicate the dawn of useful quantum computing is far closer than previously thought. With proven engineering, Oxford Ionics will now build a scalable 256 qubit chip that can be manufactured on existing semiconductor production lines.

---

[1] Quantum computers are extremely susceptible to noise, leading to errors in computations. Error correction can be used to identify and fix errors, at the cost of needing many more qubits for any given computation. Oxford Ionics' quantum chips are performing better today than any error corrected qubits.

Dr Michael Cuthbert, Director of the UK's National Quantum Computing Centre, said: "The new results mark a pivotal step forwards in ion trap quantum computing and validates the scalability of the technology. The reported one and two qubit gate results outperform other players' achievements to date, meaning error correction becomes achievable with minimal overheads. This performance underpins the proprietary architecture Oxford Ionics will deliver to the National Quantum Computing Centre as part of our Quantum Computing Testbed procurement and we are really excited to see both how this will be deployed, and how we will be able to use these ultra-high performance qubits for the development of algorithms and new applications."

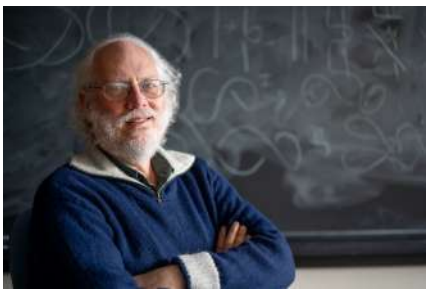
Dr Chris Ballance, co-founder and CEO of Oxford Ionics, said: "The industry's biggest players have taken different paths towards the goal of making quantum computing a reality. From the outset, we have taken a 'rocket ship' approach - focusing on building robust technology by solving the really difficult challenges first. This has meant using novel physics and smart engineering to develop scalable, high performance qubit chips that do not need error correction to get to useful applications, and can be controlled on a classic semiconductor chip. Since we started in 2019, we have hit every target on our roadmap on time and today's results validate our confidence in our approach. We are now able to focus on the commercialisation of our technology and delivering useful quantum computing at scale."

Dr Tom Harty, co-founder and CTO at Oxford Ionics, said: "When you build a quantum computer, performance is as important as size - increasing the number of qubits means nothing if they do not produce accurate results. We have now proven that our approach has delivered the highest level of performance in quantum computing to date, and is now at the level required to start unlocking the commercial impact of quantum computing. This is an incredibly exciting moment for our team, and for the positive impact that quantum computing will have on society at large."

18.Shannon Award for 2025

by Samir M. Perlaza
https://www.itsoc.org/news/shannon-award-2025

The IEEE Information Theory Society is pleased to announce that Prof. Peter Shor (MIT) is the recipient of the 2025 Claude E. Shannon Award for consistent and profound contributions to the field of information theory. He will deliver his Shannon Lecture at ISIT 2025 in Ann Arbor, Michigan, USA.



Peter Shor is the Morss Professor of Applied Mathematics at the Massachusetts Institute of Technology. Prof. Shor is well known for his quantum factoring and discrete-log algorithms. Following the 1994 publications of those algorithms Prof. Shor made a number of fundamental information-theoretic contributions that set firm engineering foundations for the field. To address the concern that errors and noise would be an insurmountable problem to implementation of the factoring algorithm, Shor proposed the first quantum error-correcting codes. Next, while classic error-correction presumes reliable encoding and ecoding, quantum algorithms cannot make the same assumption. Shor developed a theory of, and methods for, fault-tolerating quantum computing. Third, Shor worked with co-workers to devleop a systematic theory of quantum error-correction that allowed classic code constructions to be imported into quantum ECC. Fourth, Shor contributed to a number of questions of channel capacity for quantum channels. Beyond the above Peter Shor has contributed to a wide range of other problems, say in quantum cryptography and other fields. Peter Shor also served as the first AE in "Quantum Information Theory" for the IEEE Trans. on Inf. Theory from 2000-2002.

19.Quantum Randomness Unlocks New Frontiers in Computing & Cryptography

by James Dargan
https://thequantuminsider.com/2024/07/11/quantum-randomness-unlocks-new-frontiers-in-computing-cryptography/

Professor Thomas Vidick's novel research in quantum computing is helping us with our understanding of randomness and its applications in cryptography and secure communication. A researcher at the Weizmann Institute of Science, at the heart of his work lies the exploration of quantum mechanics' inherent randomness, a feature that sets it apart from classical physics.

"Classical Newtonian mechanics is a completely deterministic theory," Vidick recently explained at the 2024 Blavatnik Awards Science Symposium. "In principle, if you know the initial conditions, you can predict what is going to happen." However, quantum mechanics introduces a fundamental shift in this paradigm. "Quantum mechanics is different. It's inherently random," Vidick noted, illustrating this concept with the famous Schrödinger's cat thought experiment.

This quantum randomness, once a point of contention among physicists like Einstein, is now a well-accepted fact and a powerful resource in computation. Vidick stressed its importance: "We as computer scientists are used to thinking of randomness as a resource. It's a bit like time or space. You also have randomness. Randomness is a critical resource for algorithms. It's critical for secret communication."

The practical applications of quantum randomness are already emerging in the form of quantum random number generators. However, Vidick's research goes beyond mere generation to tackle the critical issue of verification.

"Assuming that you bought this box that generates random numbers, are you going to use the box or not?" said Vidick, posing a crucial question.

To address this challenge, Vidick introduced the concept of entanglement, a quantum phenomenon that allows for the certification of true randomness. He described an experiment involving entangled particles: "I'm going to take these two particles or photons, put them very far apart and put each of them in the box. Each of these boxes represent some physical apparatus that can make observations on the photons."

Through this experiment, Vidick demonstrated how entanglement can be used to verify the randomness of quantum processes.

"However this experiment is performed, in order to generate bits that satisfy all the constraints that I described to you, you must do it randomly," he concluded.

This breakthrough in certifying quantum randomness has far-reaching implications. It not only ensures the integrity of quantum-generated random numbers but also paves the way for more complex verification tasks in quantum computing and communication networks.

Vidick's work represents a significant step towards realizing the full potential of quantum computing. As the field rapidly advances, his research provides crucial tools for verifying and trusting quantum processes, essential for the development of future quantum technologies.

The impact of Vidick's research extends beyond theoretical physics and computer science. It builds a way for ultra-secure communication systems, unbreakable encryption methods and computational capabilities that far surpass classical computers. As quantum computing continues to evolve, Vidick's contributions in certifying quantum randomness will undoubtedly play a pivotal role in shaping the future of digital security and computation.

20.New Blast-RADIUS attack breaks 30-year-old protocol used in networks everywhere

by Dan Goodin
https://arstechnica.com/security/2024/07/new-blast-radius-attack-breaks-30-year-old-protocol-used-in-networks-everywhere/

One of the most widely used network protocols is vulnerable to a newly discovered attack that can allow adversaries to gain control over a range of environments, including industrial controllers, telecommunications services, ISPs, and all manner of enterprise networks.

Short for **Remote Authentication Dial-In User Service**, RADIUS harkens back to the days of dial-in Internet and network access through public switched telephone networks. It has remained the de facto standard for lightweight authentication ever since and is supported in virtually all switches, routers, access points, and VPN concentrators shipped in the past two decades. Despite its early origins, RADIUS remains an essential staple for managing client-server interactions for:

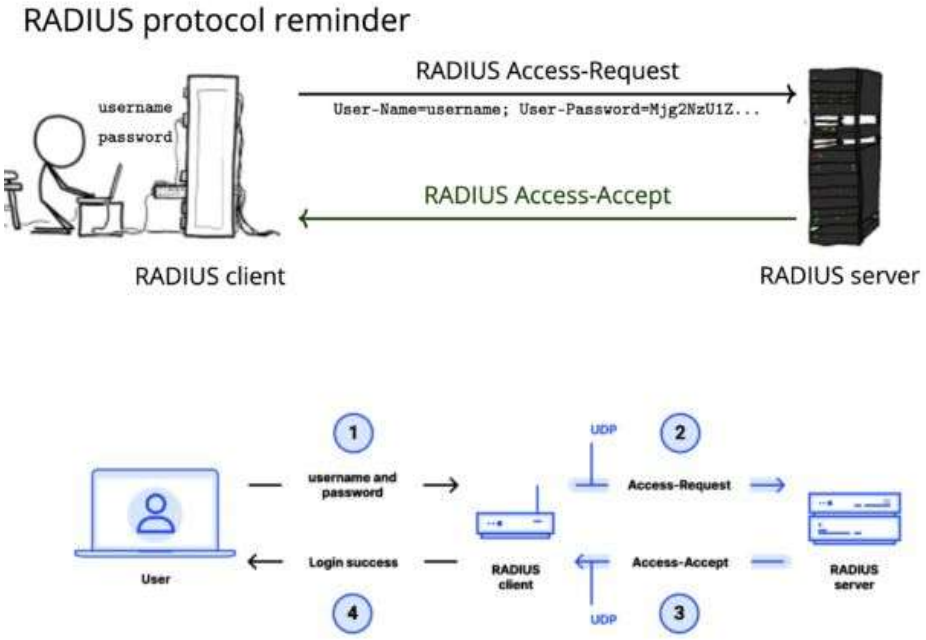
- VPN access
- DSL and Fiber to the Home connections offered by ISPs,
- Wi-Fi and 802.1X authentication
- 2G and 3G cellular roaming
- 5G Data Network Name authentication
- Mobile data offloading
- Authentication over private APNs for connecting mobile devices to enterprise networks
- Authentication to critical infrastructure management devices
- Eduroam and OpenRoaming Wi-Fi

RADIUS provides seamless interaction between clients—typically routers, switches, or other appliances providing network access—and a central RADIUS server, which acts as the gatekeeper for user authentication and access policies. The purpose of RADIUS is to provide centralized authentication, authorization, and accounting management for remote logins.

The protocol was developed in 1991 by a company known as Livingston Enterprises. In 1997 the Internet Engineering Task Force made it an official standard, which was updated three years later. Although there is a draft proposal for sending RADIUS traffic inside of a TLS-encrypted session that's supported by some vendors, many devices using the protocol only send packets in clear text through UDP (User Datagram Protocol).

Roll-your-own authentication with MD5? For real?

Since 1994, RADIUS has relied on an improvised, home-grown use of the MD5 hash function. First created in 1991 and adopted by the IETF in 1992, MD5 was at the time a popular hash function for creating what are known as "message digests" that map an arbitrary input like a number, text, or binary file to a fixed-length 16-byte output.



For a cryptographic hash function, it should be computationally impossible for an attacker to find two inputs that map to the same output. Unfortunately, MD5 proved to be based on a weak design: Within a few years, there were signs that the function might be more susceptible than originally thought to attacker-induced collisions, a fatal flaw that allows the attacker to generate two distinct inputs that produce identical outputs. These suspicions were formally verified in a paper published in 2004 by researchers Xiaoyun Wang and Hongbo Yu and further refined in a research paper published three years later.

The latter paper—published in 2007 by researchers Marc Stevens, Arjen Lenstra, and Benne de Weger—described what's known as a chosen-prefix collision, a type of collision that results from two messages chosen by an attacker that, when combined with two additional messages, create the same hash. That is, the adversary freely chooses two distinct input prefixes P and P' of arbitrary content that, when combined with carefully corresponding suffixes S and S' that resemble random gibberish, generate the same hash. In mathematical notation, such a chosen-prefix collision would be written as $H(P\|S)=H(P'\|S')$. This type of collision attack is much more powerful because it allows the attacker the freedom to create highly customized forgeries.

To illustrate the practicality and devastating consequences of the attack, Stevens, Lenstra, and de Weger used it to create two cryptographic X.509 certificates that generated the same MD5 signature but different public keys and different Distinguished Name fields. Such a collision could induce a certificate authority intending to sign a certificate for one domain to unknowingly sign a certificate for an entirely different, malicious domain.

In 2008, a team of researchers that included Stevens, Lenstra, and de Weger demonstrated how a chosen prefix attack on MD5 allowed them to create a rogue certificate authority that could generate TLS certificates that would be trusted by all major browsers. A key ingredient for the attack is software named hashclash, developed by the researchers. Hashclash has since been made publicly available.

Despite the undisputed demise of MD5, the function remained in widespread use for years. Deprecation of MD5 didn't start in earnest until 2012 after malware known as Flame, reportedly created jointly by the governments of Israel and the US, was found to have used a chosen prefix attack to spoof MD5-based code signing by Microsoft's Windows update mechanism. Flame used the collision-enabled spoofing to hijack the update mechanism so the malware could spread from device to device inside an infected network.

More than 12 years after Flame's devastating damage was discovered and two decades after collision susceptibility was confirmed, MD5 has felled yet another widely deployed technology that has resisted common wisdom to move away from the hashing scheme—the RADIUS protocol, which is supported in hardware or software provided by at least 86 distinct vendors. The result is "Blast RADIUS," a complex attack that allows an attacker with an active adversary-in-the-middle position to gain administrator access to devices that use RADIUS to authenticate themselves to a server.

"Surprisingly, in the two decades since Wang et al. demonstrated an MD5 hash collision in 2004, RADIUS has not been updated to remove MD5," the research team behind Blast RADIUS wrote in a paper published Tuesday and titled *RADIUS/UDP Considered Harmful*. "In fact, RADIUS appears to have received notably little security analysis given its ubiquity in modern networks."

The paper's publication is being coordinated with security bulletins from at least 90 vendors whose wares are vulnerable. Many of the bulletins are accompanied by patches implementing short-term fixes, while a working group of engineers across the industry drafts longer-term solutions. Anyone who uses hardware or software that incorporates RADIUS should read the technical details provided later in this post and check with the manufacturer for security guidance.

21.AI for Quantum and Quantum for AI: How the AI Boom May Reverberate Across Future Technologies

by Matt Swayne
https://thequantuminsider.com/2024/07/10/ai-for-quantum-and-quantum-for-ai-how-the-ai-boom-may-reverberate-across-future-technologies/

One of the hotly debated buzzwords in the quantum industry is "quantum AI" — using quantum computing to power artificial intelligence (AI). A pioneering quantum technologies venture firm suggests that quantum AI might may be more than just a marketing attempt to hang two hip-sounding technologies together to take advantage of the current AI boom. Quantum for AI — and AI for quantum — may be the key to overcoming critical technological challenges and creating practical solutions to big societal and scientific problems.

In an online white paper based on a recent presentation by Quantonation, the venture capital firm said

that there's a symbiotic relationship between AI and quantum technology and that these fields are driving each other forward and reshaping the landscape of computational power.

The team also suggests that the intersection of AI and quantum may be more than a happy scientific exploration, but an inevitable partnership being shaped by today's economic forces and tomorrow's technological barriers.

It's Crunch Time

The rapid advance of AI has led to an unprecedented demand for computational resources — an AI compute crunch. Quantonation pointed out that the computational requirements for training frontier AI models have skyrocketed, requiring 1000 times more compute power than four years ago. This surge has also led to a 100-fold increase in the cost of training these models. NVIDIA, with its dominant market position, has seen rapid growth, achieving a market cap exceeding $3.1 trillion.

This rapidly inflating demand for computational power would be enough to present technological and economic incentives to explore alternatives to traditional CPUs and GPUs, Quantonation points out. They identified several promising areas in research and development, including Field Programmable Gate Arrays (FPGAs), Machine Learning Application-Specific Integrated Circuits (ML ASICs), superconducting, thermodynamic, reversible, optical, analog and biological computing.

Among these, quantum computing stands out as one of the most disruptive, offering new algorithms and problem-solving approaches that are unattainable with other hardware.

The team writes: "Critically, quantum computing doesn't just offer a constant factor speedup – it unlocks entirely new algorithms and approaches to problem-solving. If you are going to unseat NVIDIA and other well funded incumbents, then you need more than just great execution. You need a fundamentally disruptive approach."

The Virtuous Cycle: AI and Quantum

Quantonation emphasized the mutually beneficial relationship between AI and quantum technologies, highlighting several key areas where they intersect:

Quantum for AI

1. **Faster Training and Inference**: Quantum machine learning is an active research area, exploring heuristic approaches on near-term quantum devices and long-term research on complexity speedups for future quantum computers.

2. **Quantum-Inspired Classical Algorithms**: Techniques like tensor networks, developed for quantum physics, are being applied to large linear algebra problems on classical computers.

3. **Better Training Data**: Quantum computers can provide more accurate simulations of the physical world, while quantum sensors offer better measurements. This improved data can enhance classical machine learning models.

4. **Enhanced Privacy and Security**: Quantum computing supports blind quantum computing, ensuring the privacy of data during computations.

AI for Quantum

1. **Quantum Processor Design Optimization**: Machine learning can assist in the design and simu-

lation of quantum processors.

2. **Improved Calibration and Control**: Better machine learning can enhance the calibration and programming of quantum systems, reducing errors.

3. **Optimization in Variational Quantum Algorithms**: Hybrid algorithms, which combine classical and quantum computing, can benefit from improved machine learning techniques.

4. **Automated Translation of Classical Code to Quantum Algorithms**: AI systems could facilitate the porting of classical code to quantum algorithms, aiding in the adoption of quantum computing.

Practical Examples

Although quantum AI may sound long-future futuristic, the initial waves of transformation are hitting the shore now. Researchers and entrepreneurs are exploring paths to quantum AI now and building products that could take advantage of merging these two powerful technologies. Quantonation provided a few real-world examples from companies in their portfolio that demonstrate the practical applications of the AI-quantum synergy:

1. **Qubit Pharmaceuticals**: Quantum-accelerated simulations could help train better machine learning models for drug discovery, creating a virtuous cycle of improved data and models.

2. **Multiverse Computing**: Developed CompactifAI, a quantum-inspired approach that significantly accelerates the training of Large Language Models (LLMs).

3. **Pasqal**: Leveraging analog quantum programming with neutral atom computers to implement graph neural networks, addressing problems in logistics, social network analysis, and biological processes.

The State of Quantum Machine Learning

The field of quantum machine learning (QML) is in its early stages but is growing rapidly. In 2023, over 4,000 publications on QML marked a significant increase from a decade earlier, the team writes. Despite this growth, QML still represents a small fraction of all machine learning research, indicating that much work remains.

And there are challenges — a lot of them — that scientists will need to overcome before QML becomes practical, Quantonation notes.

They write that theoretical quantum speedups in machine learning will face the need for significant quantum memory and the difficulty of comparing performance at scale. The team also emphasized the importance of empirical results, which are currently limited by the subscale size of existing quantum computers.

Looking Ahead

Quantonation anticipates that the ongoing AI boom will drive increased interest and investment in quantum technologies. Quantum-inspired classical algorithms are already making an impact, and future generations of quantum computers are expected to bring practical quantum machine learning techniques to fruition.

However, realizing the long-term potential of these technologies will require focused, sustained investment and effort. Quantonation writes that they remain committed to supporting the convergence of AI

and quantum tech, backing startups and technologies that are poised to shape the future of computing.

22.Quantum Xchange Enables Enterprises to Track Progress Toward Post-Quantum Standardization with Dynamic Dashboards

by April Burghardt
https://www.businesswire.com/news/home/20240710717768/en/Quantum-Xchange-Enables-Enterprises-to-Track-Progress-Toward-Post-Quantum-Standardization-with-Dynamic-Dashboards

Quantum Xchange delivering the future of encryption with crypto agility, visibility, and management solutions, today announced the latest release of CipherInsights, the company's network monitoring, crypto-discovery and risk assessment tool. Version 11.0 includes several new features to pinpoint any weaknesses in enterprise cryptography and ease an organization's inevitable migration to quantum-safe cryptography, replacing their legacy encryption with Post Quantum Cryptography (PQC) standards to be announced by the U.S. Department of Commerce's National Institute for Standards and Technology (NIST) summer 2024.

Deployed as a passive listener on the network, CipherInsights continuously monitors dozens of cryptographic risk factors in near real time, including quantum-vulnerable cryptography and where encryption is deficient or outright lacking. The sensor-based tool and on-the-wire analysis differs from network visibility and vulnerability scanners in that it scans and analyzes all traffic – even outbound traffic destined for an external host. For its functionality and practicality, CipherInsights is a discovery tool accepted by NIST's National Cybersecurity Center of Excellence, Migration to PQC Project.

NIST highly recommends organizations begin their migration planning with a systems audit and inventory of all quantum-vulnerable cryptography in use throughout the enterprise. From there, risk analysis, prioritization, and remediation efforts can take place. Quantum Xchange has responded, adding advanced dashboards to CipherInsights that capture an organization's progress towards quantum-safety, prioritized by risk and exposure. On a single screen an organization can quickly determine what encryption is quantum-safe, what is not yet quantum-safe, and what cryptography is currently breakable by hackers using conventional systems.

Further efficiencies found in CipherInsights version 11.0 include new Application Programming Interfaces (APIs) to ensure seamless integration with established infrastructure and cybersecurity tools, such as Configuration Management Database (CMDB), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR) systems. This version update also adds the ability to produce Cryptographic Bill of Materials (CBOM), which is quickly becoming the industry standard for reporting on cryptography used in an organization.

Even more prophetic are the additions of several new data fields to the already robust intelligence gathering and continuous network monitoring capabilities of CipherInsights. Now users can obtain upfront knowledge into which systems will respond well to the new PQCs and what connectivity and functionality will break when PQC standards are introduced to the network. This advanced troubleshooting and risk mitigation feature is certain to save organizations considerable time, resources, and budget on their path to quantum safety.

"We're extremely proud of the CipherInsights product and its ability to provide in-depth visibility in the cryptographic deficiencies at large government agencies and commercial enterprises," said Dr. Vincent Berk, Chief Strategist at Quantum Xchange. "The global migration to quantum-safe cryptography will be a major undertaking fraught with uncertainties and unforeseen risks. We're providing the technologies and real-time insights to navigate these unchartered waters easily and affordably with solutions that meet organizations wherever they are in their cryptographic journey – assess quantum readiness with CipherInsights and deploy quantum remediation with Phio TX."

23.Will banks be ready for post-quantum chaos if they're too focused on a pre-quantum world?

by Suneet Muru
https://www.retailbankerinternational.com/analyst-comment/will-banks-be-ready-for-post-quantum-chaos/?utm_source=substack&utm_medium=email&cf-view&cf-view

The fear of fintech disruption has forced banks to actively discuss and explore a plethora of transformative technologies like artificial intelligence, cryptocurrency, and the Internet of Things. However, quantum computing, potentially the most disruptive (or even destructive) of them all, receives a relatively small amount of boardroom airtime.

Quantum computers, which use the properties of quantum physics to store data and perform computations, can reach estimated speeds of up to 10 million times that of a classical computer. They therefore have the potential to massively bolster the efficiency and capabilities of banks. However, they are also far more powerful, giving rise to both financial and reputational damage on unprecedented scales. Do banks understand the potential risks and opportunities associated with quantum computers?

What is quantum computing?

Quantum computing uses the unique behavior of sub-atomic particles to create incredibly powerful computers. Unlike classical computers, which use bits, quantum computers use qubits. Like classical bits, qubits eventually have to transmit the information as a one or a zero. However, they are special because they can simultaneously represent both a one and a zero, a condition known as superposition. Entanglement is another key property of quantum mechanics, where entangled qubits cannot be individually described, and their properties depend on each other. This allows for exponential increases in computing power as more qubits are added.

These differences mean that quantum computers have the potential to perform complex simulations and calculations at a speed that surpasses classical supercomputers, but maintaining qubit stability remains a challenge. Quantum computers are also systems that are designed to carry out specific tasks, as opposed to classical computers which are more general-purpose systems.

Quantum opportunities in banking

Financial markets today are complex and chaotic global systems in which fund managers must balance the ever-changing risks and returns of portfolios. Monte Carlo simulations have been used for years to create models but face limitations on classical computers. Quantum computers are believed to be able

to revolutionize financial modeling, portfolio optimisation, fraud detection, and customer targeting. JP Morgan and Goldman Sachs are leading the way in exploring quantum computing for finance, focusing on algorithms and applications rather than hardware. JP Morgan has collaborated with Quantinuum on research papers covering topics like option pricing and portfolio optimisation using quantum computers.

In general, quantum computers have the potential to exponentially increase the speed of almost everything banks do from a technological standpoint. For example, they can process digital payments much faster than classical computers, paving the way for near-frictionless capital flow. Risk quantification is a key challenge facing banks, especially concerning cyber risks, which are many and varied. Having a computer that can take unstructured data across multiple risk types and very quickly understand the relationship between different factors could be a game changer for banks in both predicting and understanding the impact of financial market turmoil.

Quantum risks in banking

It is believed that quantum computers, should they achieve sufficient size and power, could break the encryption methods currently used by banks to secure financial data and transactions, such as Advanced Encryption Standard, Rivest-Shamir-Adleman, and Diffie-Helman. This makes banks susceptible to a form of cyber-attack known as “Harvest Now, Decrypt Later” whereby adversaries store encrypted data over extended periods until they can decrypt it in the future using quantum computers. Banks hold large amounts of sensitive data and are subsequently exploring solutions to protect against quantum threats.

In July 2023, HSBC became the first bank to commercially trial the Quantum Secure Metro Network (QSMN), a project led by BT and Toshiba that uses quantum key distribution (QKD) to secure data transmission between customer sites in London. QKD is a method of encryption that uses the properties of quantum particles to create a key for encrypting and decrypting messages. The key is transferred using entangled qubits. Furthermore, BBVA is a founding member of the Quantum Safe Financial Forum (QSFF), an initiative that aims to share best practices and coordinate actions to address a safe transition to post-quantum cryptography.

Those banks that take proactive measures to incorporate quantum use cases while aiming to protect against quantum threats stand to become leaders in quantum computing. While the potential of quantum may seem like a distant dream, being unprepared for its transformative potential will be far more damaging in the long run than the short-term spending loss of funds from dedicating spending towards the theme.

24.Researchers Crack DoNex Ransomware Encryption with Flaw in Cryptographic Schema

by Alan J
https://thecyberexpress.com/donex-ransomware-encryption-decryption/

Researchers have discovered a critical flaw in the cryptographic schema of the DoNex ransomware and all of its variants and predecessors. Since then, they have collaborated with law enforcement agencies to discreetly provide a decryptor to affected DoNex victims since March 2024.

The cryptographic vulnerability was publicly discussed at Recon 2024, prompting the researchers to officially disclose details of the flaw and its implications.

DoNex Ransomware Operations

Avast researchers noted that the DoNex ransomware has undergone several rebrandings after initially identifying as Muse in April 2022. Subsequent iterations of DoNex included a rebrand to a purported Fake LockBit 3.0 in November 2022, then to DarkRace in May 2023, and finally to DoNex in March 2024. Since April 2024, the researchers noted that no newer samples were detected, and that the ransomware group's official TOR address remained inactive, suggesting that DoNex may have ceased its evolution and rebranding attempts.

DoNex ransomware employs a complex encryption process. During its execution, an encryption key is generated using the *CryptGenRandom* function. This key initializes a *ChaCha20* symmetric key, which is then used to encrypt files.

After encryption, the symmetric key is encrypted with RSA-4096 and appended to the affected file. For files up to 1 MB, the entire file is encrypted, while larger files are encrypted in segments of blocks. The ransomware's configuration, along with details over whitelisted extensions, files, and services to terminate, are stored in an XOR-encrypted configuration file.

While the researchers have not detailed the exact process they used to decipher the decryption, more details related to the same cryptographic vulnerability are available from files related to the Recon 2024 event talk titled "*Cryptography is hard: Breaking the DoNex ransomware*." Gijs Rijnders, a malware reverse engineer and cyber threat intelligence analyst working for the Dutch National Police, hosted the talk.

DoNex primarily targeted victims in the US, Italy, and Belgium, using focused attacks. The researchers confirmed that all variants of the DoNex ransomware along with its earlier versions can be decrypted using the released DoNex decryptor.

Identifying DoNex Ransomware and Decryption

Victims of the DoNex ransomware can recognize an attack through the ransom note left by the malware. Although different variants (Fake LockBit, DarkRace and DoNex) of DoNex produce distinct ransom notes, they share a similar layout.

The researchers have shared instructions for using their decryptor against DoNex ransomware encrypted files:

1. Download the provided decyptor. (The researchers recommend running the 64-bit version of the program due to memory requirements.)

2. Run the decryptor's executable file as an administrator. The program should run as a wizard, automatically guiding you through the decryption process.

3. While the program lists all local drives by default, the user is requested to provide a list of possible locations meant to be decrypted.

4. Users are then requested to provide an encrypted file (from any variant of DoNex) as well as a copy of the original file before encryption. The researchers emphasize selecting the biggest possible pair of files for this process.

5. The next process of the wizard will begin the password cracking process. The researchers state that while this process of cracking only takes a second, it would require a huge volume of memory. After the step has been completed, users can get ready to begin with the decryption process for all the files on their entire system.

6. In the final step, users can opt to back up encrypted files on their system, which may help in the event of failures during the decryption process. The researchers stated that the option is set at default.

7. Users can let the program run in an attempt to decrypt all the DoNex encrypted files on their system.

The researchers have also shared Indicators of compromise (IOCs) of the FakeLockBit 3.0, Dark Race and DoNex variants of the ransomware.

25.India Calls for Quantum Standardization, Testing Labs for Quantum Communications Network Developments

by Matt Swayne
https://thequantuminsider.com/2024/07/08/india-calls-for-quantum-standardization-testing-labs-for-quantum-communications-network-developments/

India's Department of Telecommunications (DoT) has issued a call for research proposals from academic and research institutions focused on the standardization and testing of quantum technologies, based on Business Standard reporting. This initiative aims to develop innovative solutions that can enhance the efficiency, security and reliability of communication networks across the country.

The Business Standard reported that the official statement from the DoT specifically highlighted the initiative's alignment with Prime Minister Narendra Modi's 'Jai Anushandhan' vision, which emphasizes the importance of research and development in enhancing the lives of Indian citizens through advanced telecom products and technologies. By inviting proposals on 'Quantum Standardisation and Testing Labs,' the government is encouraging the country's researchers and entrepreneurs to create a robust infrastructure that supports the burgeoning field of quantum communication.

Quantum technologies, which leverage the principles of quantum mechanics, hold the promise of revolutionizing various sectors, especially telecommunications, according to the release. Quantum communication systems offer — still theoretically — unparalleled security features, including quantum key distribution (QKD), which is virtually unhackable. This makes them ideal for secure communication in a world increasingly threatened by cyber-attacks.

The proposed labs will serve as innovation hubs, bringing together quantum technology developers, testing equipment manufacturers, and academic researchers. These hubs will facilitate collaborative research efforts, driving the exploration and harnessing of quantum technologies' full potential for societal benefit. The establishment of these labs is expected to foster a vibrant ecosystem where ideas and innovations can flourish, paving the way for groundbreaking advancements in the field.

The Economic Times, India lists the two core objectives of the program:

- **Ensuring Interoperability, Reliability, and Security of Quantum Communication Systems:** The initiative aims to drive research and development in quantum technologies to develop communication systems that are interoperable, reliable, and secure. This includes leveraging quantum mechanics principles to create superior security features such as Quantum Key Distribution (QKD), which provides a highly secure method for encrypting communications and protecting them from cyber threats.

- **Fostering Innovation and Collaboration in Quantum Technologies**: The establishment of Quantum Standardisation and Testing Labs will serve as innovation hubs, bringing together quantum technology developers, testing equipment manufacturers, and academic researchers. These labs will support collaborative research efforts, fostering a vibrant ecosystem that nurtures innovative ideas and advancements in quantum communication, ultimately enhancing the digital experience and data security for Indian citizens.

The government's focus on quantum technologies is part of a broader strategy to make India self-reliant in high-tech domains and to set global benchmarks in this cutting-edge field. The initiative underscores the importance of developing secure, reliable, and efficient quantum communication systems that can improve everyday communication, enhance data security, and elevate the overall digital experience for Indian citizens.

By promoting research and development in quantum technologies, the DoT aims to ensure that India remains at the forefront of global technological innovation. This initiative is not only a step towards achieving technological sovereignty but also a means to provide Indian citizens with access to state-of-the-art communication technologies.

26.India has large gap to bridge in quantum capabilities

by Amitabh Sinha

https://indianexpress.com/article/technology/science/india-gap-bridge-quantum-capabilities-report-9429549/

India may have done the right thing by launching a Rs 6,000 crore-worth National Quantum Mission to develop some of the most sought-after technologies for the future, but it would have to overcome a significantly large gap that currently exists between its capabilities and those of other leading countries in these areas like the United States and China, a new assessment of India's potential in quantum technologies has revealed.

The assessment by Itihaasa, a non-profit that studies the evolution of technology and business domains in the country, shows that India was just one among 17 countries to have a dedicated government programme to back research in quantum technologies, and one of the 12 to have committed separate investments for the purpose. But several countries were much ahead of India, not just in terms of committed funding for research and development but also in their current capabilities.

India's Rs 6,000 crore translates to about USD 0.75 billion over five years. China, on the other hand, was estimated to be spending USD 15 billion for developing quantum technologies. The United Kingdom

(USD 4.3 billion), the United States (USD 3.75 billion), Germany (USD 3.3 billion) and South Korea (USD 2.35 billion).

India was far behind of the United States and China in terms of patents obtained in quantum technologies till now, and in publications in top journals.

“It is commendable that India is among the 17 countries with formal national quantum missions, and is among the top 12 countries in terms of committed investments. At the same time, we must recognise that India is lagging the global leaders in quantum technologies, and needs to ramp-up both R&D and translational aspects to catch up with them,” the assessment said.

Quantum technologies exploit the extremely weird and counter-intuitive — but very special nonetheless — properties of sub-atomic particles like an electron to develop processes and devices with capabilities and efficiencies that are impossible to achieve with classical, non-quantum, systems. A quantum computer, for example, can perform certain tasks that a normal computer, however fast or powerful it may be, might not be able to finish in any useful amount of time.

Quantum technologies, once they mature, will probably cause a disruption in almost every field, but some of the areas that are expected to be impacted first, and gain the most, happen to be computing, communications, cryptography, cybersecurity, and healthcare. Most of the technologies are still under development, with scientists still to gain full control over the quantum behaviour of the sub-atomic particles in a way that could be used to extract useful work.

India’s National Quantum Mission, launched last year, aims to develop capabilities in four areas – quantum computing, communications, sensors and metrology (the science of measurements), and materials.

Abhay Karandikar, Secretary in Department of Science and Technology which is executing the quantum mission, said in at least two of these areas, communications and sensing, India had a very realistic chance of joining the global leaders in about five years’ time.

“We already have fairly advanced capabilities in these areas (quantum communications, and sensing). We even have a few start-ups doing very good work. With a little push, we should be in the global lead. With other technologies, including quantum computing, we would have to work a lot more harder. But we are not starting at zero in any of these areas. We would be among the top-five, top ten or top 15 everywhere,” he said.

Principal Scientific Advisor Ajay Sood said the gap between India and other leading countries was not such that it could not be bridged.

“In some areas we are may be one year behind. In some others, we might be four to five years behind. In some areas we are at par with the best in the world. We have to work hard for the next few years, because the fruits of these technologies are going to be transformational,” Sood said.

The assessment report found about 110-145 Indian researchers, at the principal investigator level, already working on quantum technologies at major laboratories and institutions. About 75-100 Post-docs and 300-400 PhD students were working with them. In addition, there were about 50-100 MTech students in different areas related to quantum technologies.

Incidentally, India was producing the highest number of graduates in areas related to quantum technologies, the assessment found. These included subjects like biochemistry, chemistry, physics, electronics and chemical engineering, mathematics and statistics. More than 82,000 students were graduating in these subjects every year. Only European Union, taken as a whole, had higher number of students in these areas.

"These graduates will still need focused training on different aspects of quantum technologies to make them a relevant workforce in the field," the assessment said.

It said that the government should explore the possibility of facilitating a dedicated science and technology cadre in each of the four areas identified for National Quantum Mission, similar to the dedicated cadres in India's space and nuclear sectors

27.NIST picks Post-Quantum to ease cryptographic migration

by Ian Murphy
https://www.enterprisetimes.co.uk/2024/07/03/nist-picks-post-quantum-to-ease-cryptographic-migration/

NIST has picked Post-Quantum to join the National Cybersecurity Center of Excellence (NCCoE) Migration to Post-Quantum Cryptography (PQC) project. The project is focused on helping organisations migrate to a new world of cryptography. It will be essential as Quantum computing comes online and threatens many of the existing cryptography schemes people use.

Andersen Cheng, Executive Chairman, Post-Quantum, commented: "Our priority over the last few years has been on accelerating real-world implementations. For example, last year a new standard that we authored for a hybrid quantum-safe Virtual Private Networks (VPN) was ratified by the Internet Engineering Task Force (IETF).

"This new standard is now the glue that allows parties using different post-quantum key establishment algorithms to talk with one another, which is particularly important as we enter a situation where different nation states deploy a variety of different algorithms.

"We are looking forward to sharing implementation knowledge of our protocol and unique know-how in securing mobile end points with partners such as Palo Alto, Microsoft, and AWS, to accomplish an end-to-end secure quantum migration."

What is the problem here?

There are several problems with how we encrypt data today. First, future quantum technologies are expected to break many cryptographic algorithms that are in use today. Second, many breaches are Harvest Now and Decrypt Later (HNDL). Nation-states and malicious actors hold on to stolen data sets until they break the encryption to access the data.

To counter this, NIST has conducted a series of tests to find new cryptographic algorithms that can withstand quantum computing attacks. The successful algorithms are beginning to emerge from those tests. However, they must still be proven in a wider environment and get organisations to migrate to them.

That migration process is complex. It cannot be assumed that an organisation can apply a new algorithm. First, a lot of coding and technology needs to change. Additionally, once the new algorithm is in place, it is just not feasible for organisations to go through historical data sets and backups and re-encrypt them. At best, some will decide based on what they see as the most sensitive data.

Why Post-Quantum?

Post-Quantum says that its selection by NIST will see it playing a role in:

- Ensuring smooth transition and deployment of VPN that will protect us from HNDL attacks
- Ensuring that backward compatibility is supported
- Testing different PQC algorithm configurations in hybrid arrangement, not only those standardised by NIST but also other PQC algorithms.
- Providing in particular unique implementation know-how in securing edge to mobile end-points.

Key to this is the Post-Quantum Quantum-Safe Platform. The platform consists of modules covering identity, transmission, and encryption. There are three modules in the current platform. They are:

- **PQ Chat:** It is a secure end-to-end messaging app that runs on desktops, laptops and mobile devices. With all the attention on the problems of messaging apps like WhatsApp, this alternative meets government and military requirements. It is only available to enterprise and government customers.

- **Hybrid PQ VPN:** Based on the IETF standards, PQ VPN protects all traffic from eavesdropping and removes the risk of data compromise. The company says that its crypto-agility ensures it can use any NIST post-quantum algorithms. It means it has longevity and can be used in hostile areas where critical secure communications are.

- **Nomidio Identity:** It is described as a quantum-safe multi-factor biometric identity system. Users register once with it and then use the Nomidio identity to connect to other systems. Of interest to IT security teams is that this is a self-sovereign identity solution. It means that identity is only revealed when the user provides consent.

Enterprise Times: What does this mean?

The security risks that quantum computing will pose have been discussed since IBM first showed it in 2016. Since then, the technology has continued to evolve and is getting near the point where commercial use is expected to start. Once that happens, development will accelerate, and the technology will become more widely used.

As with other technologies, it can be used for good or bad. Since the technology was developed, breaking cryptographic algorithms has been a focus. Despite this, we are still awaiting NIST's final list of post-quantum algorithms.

Only once they have been widely tested will organisations start to implement them. This means a significant gap exists between the deployment of quantum-safe technology and the reality for many organisations.

It will be interesting to see how Post-Quantum changes this. Its solutions above will appeal to customers outside of organisations such as NATO, which it cites as a customer. The challenge will be getting them to adopt its technology. One area where it might well get traction is in the age-verification market with Nomidio. That market needs an ultra-secure solution, especially to protect minors.

Outside of that, its chat service will be interesting to organisations, although more information on end-to-end encryption would be helpful. For example, can the organisation provide access to all messages on demand from law enforcement?

28.How to Achieve Crypto Resilience for a Post-Quantum World

by Murali Palanisamy
https://securityboulevard.com/2024/07/how-to-achieve-crypto-resilience-for-a-post-quantum-world/

Quantum computing may be the greatest cybersecurity threat the world has ever seen – and that's no exaggeration. Soon, data encrypted with current cryptographic algorithms will be unlocked. The transition to new quantum-safe algorithms for the post-quantum cryptography (PQC) era will be neither simple nor quick. There's no question that the time to start preparing for quantum resilience is now.

Quantum computing threatens the security of current encryption algorithms for one simple reason: Speed. Today's prevailing public key infrastructure (PKI) standards, RSA and ECC, depend on the fact that decrypting text without a key involves an enormous amount of mathematical calculation, a process estimated to take current computers millions of years.

With quantum computing, the time needed to perform such calculations shrinks enormously. In a test conducted by Google in 2019, a quantum computer executed an operation that would take a supercomputer 10,000 years in about three minutes. The newest version of this quantum computer is said to be 241 million times faster. The point is, there are real computers that exist right now that could crack the technology used to protect virtually all of the sensitive data that exists outside of military and other top secret installations.

While it's unlikely that quantum computers are currently in the hands of cybercriminals or hostile nation-states, they will be. Several global powers, like China, are pushing the boundaries to achieve quantum computing. In anticipation, many bad actors are pursuing a "harvest now, decrypt later" strategy. Collecting sensitive data that is currently encrypted with RSA and ECC technologies, knowing that they will likely be able to decrypt it soon.

McKinsey estimates that 5,000 quantum computers will be available by 2030. In other words, quantum-enabled hacking could become a reality in just over five years. But given the resources available to state-sponsored organizations, that day might come much sooner.

The U.S. government isn't waiting. The National Institute of Standards and Technology (NIST) initiated a formalized effort to pursue PQC algorithms in 2016. The results were released in July 2023. Two algorithms belong to the so-called Cryptographic Suite for Algebraic Lattices, CRYSTALS-Kyber for general encryption and CRYSTALS-Dilithium for digital signatures. Two other signature algorithms were also released, SPHINCS+ and FALCON.

These algorithms will most likely be standardized by NIST by the end of this year. The existence of standardized PQC solutions will put even more pressure on CISOs to migrate beyond the RSA and ECC technologies now in place. Preparing against this threat is no simple matter. It takes time.

The history of SHA-1 is a good example of how slow and complex the process of migrating from one established security technology to another can be. Serious vulnerabilities in SHA-1 were discovered and published in 2005, and further successful attacks by academics soon followed. Ten years later, SHA-1 was still so popular that the Mozilla Foundation issued a security warning to developers to avoid using SHA-1 certificates. This was after NIST had formally deprecated SHA-1 in 2011. There is no reason to think that abandoning RSA and ECC will be any easier.

Quantum computing will not only redefine the threat landscape. It will redefine the regulatory landscape as well. Current guidelines will be revised to account for the threat of quantum-enabled attacks. Audits will include assessments of an organization's preparedness to defend against such attacks.

Financial, healthcare and government organizations will face heightened scrutiny due to the sensitive nature of the data they handle, but CISOs in every sector will need to be proactive. This is important not only for compliance but also because of the new risks that will emerge.

To protect their organizations, CISOs should consider implementing the following steps as soon as possible:

- **Risk Assessment:** Identify and catalog those assets that are most vulnerable to quantum attacks, including digital certificates and keys, along with the data, machines, applications and services they protect. This inventory will provide a sense of the scope, impact and cost of migration to PQC.

- **Migration Planning:** Prioritize systems, application, services and data assets for migration based on their risk profile. This will include systems that handle PPI and other data subject to regulatory compliance, but intellectual property may also be important. PQC algorithms should be evaluated and tested against actual business use cases. The result of this step is a well-defined process for the migration to PQC with minimal business disruption, along with a realistic timeline.

- **Crypto-Agility:** One overarching goal of the migration should be establishing a security process and supporting technologies that enable the rapid upgrade of system components like cryptographic algorithms or key exchange protocols to address emerging security threats and business requirements.

For years, quantum computing has been portrayed as a futuristic possibility. Now, it has arrived. Fortunately, new cryptographic algorithms that can resist quantum attacks exist and will be standardized soon. But, as experience has shown, implementing new cryptographic infrastructure is complex and time-consuming. CISOs must take the first steps now.

29.Quantum is unimportant to post-quantum

by Opal Wright
https://securityboulevard.com/2024/07/quantum-is-unimportant-to-post-quantum/

You might be hearing a lot about post-quantum (PQ) cryptography lately, and it's easy to wonder why it's such a big deal when nobody has actually seen a quantum computer. But even if a quantum computer is never built, new PQ standards are safer, more resilient, and more flexible than their classical counterparts.

Quantum computers are a big deal; just ask around, and you'll get plenty of opinions. Maybe quantum computers are *on the verge* of destroying public-key cryptography as we know it. Or maybe cryptographically significant quantum computers are an impossible pipe dream. Maybe the end of public-key cryptography isn't *now*, but it's only two decades away. Or maybe we have another 50 or 60 years because useful quantum computers have been two decades away for three decades, and we don't expect

that to change soon.

These opinions and predictions on quantum computers lead to many different viewpoints on post-quantum cryptography as well. Maybe we need to transition to post-quantum crypto right now, as quickly as we can. Maybe post-quantum crypto is a pipe dream because somebody will find a way to use quantum computers to break new algorithms, too. Maybe a major world government already has a quantum computer but is keeping it classified.

The fact of the matter is, it's hard to know when a cryptographically significant quantum computer will exist until we see one. We can guess, we can try to extrapolate based on the limited data we have so far, and we can hope for one outcome or the other. But we can't *know* with certainty.

That's okay, though, because quantum resistance isn't the main benefit of post-quantum crypto.

Current research and standards work will result in safer, more resilient cryptographic algorithms based on a diverse set of cryptographic problems. These algorithms benefit from the practical lessons of the last 40 years and provide use-case flexibility. Doomsayers and quantum skeptics alike should celebrate.

All in one basket

People who are worried about quantum computers often focus on one point, and they're absolutely right about it: almost all public-key cryptography in wide use right now could be broken with just a few uncertain-but-possible advances in quantum computing.

Loosely speaking, the most commonly-used public-key algorithms are based on three problems: factoring (RSA), finite field discrete logarithms (Diffie-Hellman), and elliptic curve discrete logarithms (ECDH and ECDSA). These are all special instances of a more general computational problem called the hidden subgroup problem. And quantum computers are good at solving the hidden subgroup problem. They're *really* good at it. So good that, if somebody builds a quantum computer of what *seems like* a reasonable size to many researchers, they can do all manner of nasty things. They can read encrypted messages. They can impersonate trusted organizations online. They can even use it to build tools for breaking some forms of encryption *without* quantum computers.

But even if quantum computing never becomes powerful enough to break current public keys, the fear of the quantum doomsayers is based on a completely valid observation: the internet has put nearly *all* of its cryptographic eggs into the single basket of the hidden subgroup problem. If somebody can efficiently solve the hidden subgroup problem, whether it's with quantum computers or classical computers, they will be able to break the vast majority of public-key cryptography used on the internet.

What often gets overlooked is that, for the last 40 years, the hidden subgroup basket has consistently proven less safe than we expected.

Advances in factoring and discrete logs

In the 1987 talk "From Crossbows to Cryptography: Techno-Thwarting the State," Chuck Hammill discussed RSA keys with 200 digits, or about 664 bits, saying that the most powerful supercomputers on earth wouldn't be able to factor such a number in 100 years. The Unix edition of PGP 1.0 supported 992-bit RSA keys as its highest security level, saying the key size was "military grade."

Nowadays, formulas provided by the National Institute of Standards and Technology (NIST) suggest that a 664-bit key offers only about 65 bits of security and is firmly within the reach of motivated academic researchers. A 992-bit key offers only about 78 bits of security and is speculated to be within reach of intelligence agencies.

(The smallest key size supported in PGP 1.0, 288 bits, can be broken in about 10 minutes on a modern desktop computer using readily available software like msieve. “Commercial grade” keys were 512 bits, which can be factored using AWS in less than a day for under $100.)

Ever-increasing key sizes

In response to advances in factoring and discrete logarithm algorithms over the years, we’ve responded by doing the only thing we really knew how to do: increasing key sizes. Typical RSA key sizes these days are 2048 to 4096 bits, roughly three to six times longer than Chuck Hammill suggested, and two to four times the length of what an early version of PGP called a “military grade” RSA key. The National Security Agency requires RSA keys no shorter than 3072 bits for classified data. The NIST formulas suggest that keys would need to be 15,360 bits long in order to match the security of a 256-bit AES key.

Finite field discrete logarithm key sizes have largely tracked RSA key sizes over the years. This is because the best algorithm for solving both problems is the same: index calculus using the general number field sieve (GNFS). There are some differences at the edges, but most of the hard work is the same. It’s worth pointing out that finite field discrete log cryptosystems have an additional downside: computing one discrete log in a finite field costs about the same as computing *a lot* of discrete logs.

Elliptic curves, which have become more popular over the last 15 years or so, have not seen the sort of changes in key size that happened with factoring and discrete log systems. Index calculus doesn’t translate well to elliptic curves, thank goodness, but elliptic curve discrete logarithms are an open area of research.

Implementation dangers

On top of the lack of problem diversity, another concern is that current algorithms are finicky and subject to subtle implementation failures.

Look, we’re Trail of Bits. We’re kinda famous for saying “fuck RSA,” and we say it mainly because RSA is *full of landmines*. Finite field Diffie-Hellman has subtle problems with parameter selection and weak subgroup attacks. Elliptic curve cryptosystems are subject to off-curve attacks, weak subgroup attacks, and attacks related to bad parameter selection.

Worse yet, *every one* of these algorithms requires careful attention to avoid timing side channel attacks!

Taken together, these pitfalls and subtle failure modes turn current public-key primitives into an absolute minefield for developers. It’s not uncommon for cryptography libraries to refer to their low-level functionality as “hazmat.” This is all *before* you move into higher-level protocols!

Many implementation concerns are at least partially mitigated through the use of good standards. Curve25519, for instance, was specifically designed for fast, constant-time implementations, as well as security against off-curve and weak subgroup attacks. Most finite field Diffie-Hellman key exchanges used for web traffic are done using a small number of standardized parameter sets that are designed to mitigate weak subgroup attacks. The ever-growing menagerie of known RSA attacks related to encryption and signing can (usually) be mitigated by using well-tested and audited RSA libraries that implement the latest standards.

Good standards have helped immensely, but they really just paper over some deeply embedded properties of these cryptosystems that make them difficult to use and dangerous to get wrong. Still, despite the consequences of errors and the availability of high-quality open-source libraries, Trail of Bits regularly finds dangerously flawed implementations of these algorithms in our code reviews.

What post-quantum crypto provides

So why is post-quantum crypto so much better? It's instructive to look at the ongoing NIST post-quantum crypto standardization effort.

Diversity of problems

First of all, upcoming NIST standards are based on multiple mathematical problems:

- CRYSTALS-KYBER, CRYSTALS-DILITHIUM, and Falcon are based on lattice problems: short integer solutions (SIS) and learning with errors (LWE) over various rings.
- SPHINCS+ is based on the difficulty of second-preimage attacks for the SHA-256 and SHA-3 hash functions.

Additionally, NIST is attempting to standardize one or more additional signature algorithms, possibly based on different problems. Submissions include signature algorithms based on problems related to elliptic curve isogenies, error correcting codes, and multivariate quadratics.

By the time the next phase of standardization is over, we can expect to have algorithms based on at least three or four different mathematical problems. If one of the selected problems were to fall to advances in quantum or classical algorithms, there are readily-available replacements that are highly unlikely to be affected by attacks on the fallen cryptosystems.

Modern design

The post-quantum proposals we see today have been developed with the advantage of hindsight. Modern cryptosystem designers have seen the myriad ways in which current public-key cryptography fails in practice, and those lessons are being integrated into the fabric of the resulting designs.

Here are some examples:

- Many post-quantum algorithms are designed to make constant-time implementations easy, reducing the risk of timing attacks.
- Many algorithms reduce reliance on random number generators (RNGs) by extending nonce values with deterministic functions like SHAKE, preventing reliance on insecure RNGs.
- Random sampling techniques for non-uniform distributions in the NIST finalists are fully specified and have been analyzed as part of the standardization effort, reducing the risk of attacks that rely on biased sampling.
- Many post-quantum algorithms are fully deterministic in their input (meaning that encrypting or signing the same values with the same nonces will always produce the same results), reducing nonce reuse issues and the risk of information leakage if values are reused.
- Many algorithms are designed to allow quick and easy generation of new keys, making it easier to provide forward secrecy.
- Rather than inviting developers to dream up their own parameters, every serious proposal for a post-quantum cryptosystem lists a small set of secure parameterizations.

These are intentional, carefully-made decisions. Each is based on real-world failures that have shown up over the last 40 years or so. In cryptography, we often refer to these failure scenarios as “footguns” because they make it easy to shoot yourself in the foot; the newer designs go out of their way to make it difficult.

Use-case flexibility

With new algorithms come new trade-offs, and there are plenty to be found in the post-quantum standards. Hash-based signatures can run to 50 kilobytes, but the public keys are tiny. Code-based systems like McEliece have small ciphertexts, and decrypt quickly—but the public keys can be hundreds of kilobytes.

This variety of different trade-offs gives developers a lot of flexibility. For an embedded device where speed and bandwidth are important but ROM space is cheap, McEliece might be a great option for key establishment. For server farms where processor time is cheap but saving a few bytes of network activity on each connection can add up to real savings, NTRUSign might be a good option for signatures. Some algorithms even provide multiple parameter sets to address different needs: SPHINCS+ includes parameter sets for “fast” signatures and “small” signatures at the same security level.

The downside of post-quantum: Uncertainty

Of course, one big concern is that everybody is trying to standardize cryptosystems that are relatively young. What if the industry (or NIST) picks something that’s *not* secure? What if they pick something that will break tomorrow?

The idea can even feel frighteningly plausible. RAINBOW made it to the third round of the NIST PQC standardization effort before it was broken. SIKE made it to the (unplanned) fourth round before it was broken.

Some folks worry that a new standard could suffer the same fate as RAINBOW and SIKE, but not until *after* it has been widely adopted in industry.

But here’s a scary fact: we *already* run that risk. From a mathematical standpoint, there’s no proof that RSA moduli can’t be factored easily. There’s no *proof* that breaking RSA, as it’s used today, is equivalent to factoring (the opposite is true, in fact). It’s completely possible that somebody could publish an algorithm tomorrow that totally destroys Diffie-Hellman key exchanges. Somebody could publish a clever paper next month that shows how to recover private ECDSA keys.

An even scarier fact? If you squint a little, you’ll see that *big breaks have already happened with factoring and finite field discrete logs*. As mentioned above, advances with the GNFS have been pushing up RSA and Diffie-Hellman key sizes for over two decades now. Keys that would have been considered fine in 1994 are considered laughable in 2024. RSA and Diffie-Hellman from the old cipherpunk days are *already broken*. You just didn’t notice they’re broken because it took 30 years to happen, with keys getting bigger all the while.

I don’t mean to sound glib. Serious researchers have put in a *lot* of effort over the last few years to study new post-quantum systems. And, sure, it’s possible they missed something. But if you’re really worried about the possibility that somebody will find a way to break SPHINCS or McEliece or CRYSTALS-KYBER or FALCON, you can keep using current algorithms for a while. Or you could switch to a hybrid cryptography system, which marries post-quantum and pre-quantum methods together in a way that should stay secure as long as *both* are not broken.

Summing up

Fear of quantum computers may or may not be overblown. We just don't know yet. But the effect of post-quantum crypto research and standardization efforts is that we've taken a ton of eggs out of one basket and we're building a *much* more diverse and modern set of baskets instead.

Post-quantum standards will eventually replace older, more finicky algorithms with algorithms that don't fall apart over the tiniest of subtleties. Several common sources of implementation error will be eliminated. Developers will be able to select algorithms to fit a broad range of use cases. The variety of new mathematical bases provides a "backup plan" if a mathematical breakthrough renders one of the algorithms insecure. Post quantum algorithms aren't a panacea, but they certainly treat a lot of the headaches we see at Trail of Bits.

Forget quantum computers, and look at post-quantum crypto research and standardization for what it is: a diversification and modernization effort.