Crypto News

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

December 06, 2024

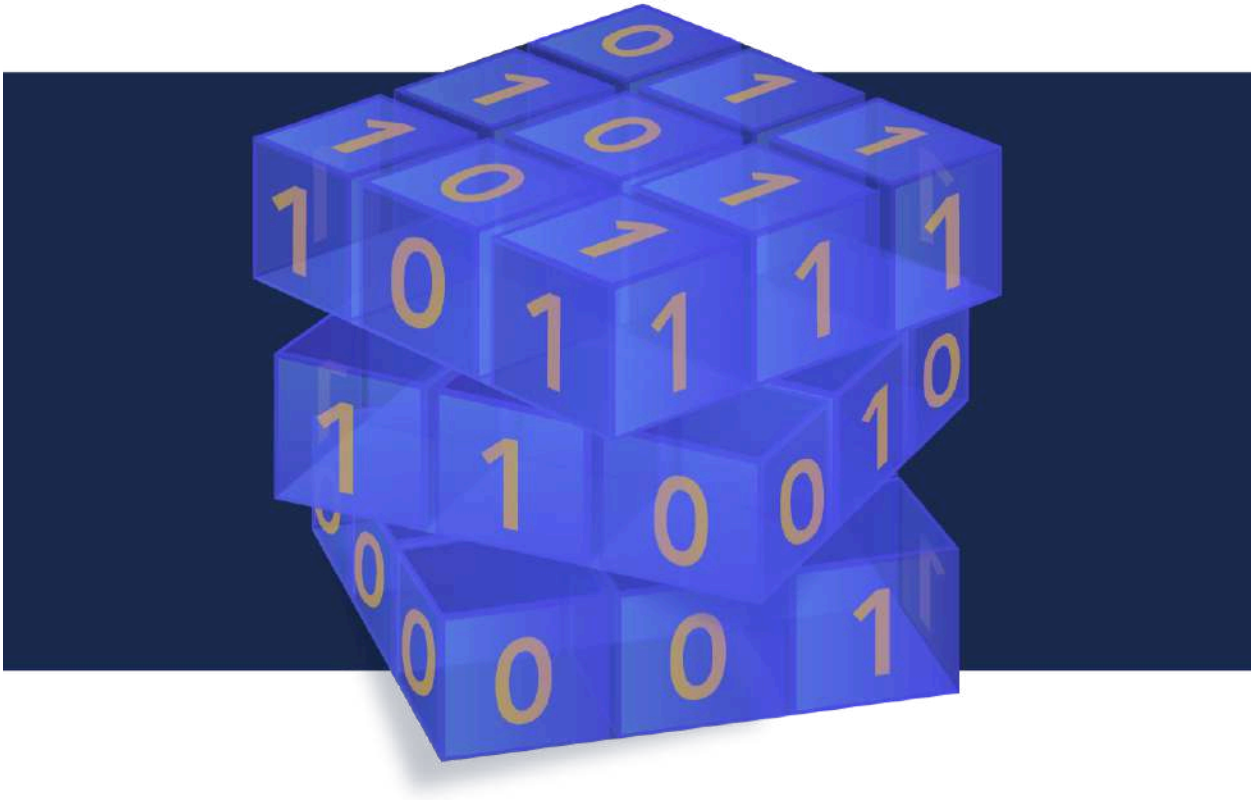


Table of Contents

Editorial

Dear Readers,

When I joined ID Quantique about ten years ago, and quickly afterwards became chair of the QSS working group of the CSA, a significant amount of my time was devoted to introducing people to the quantum threat and to convincing them that it is real. There was no quantum computer then. A few academics were playing with one or a few qubits. The only applications of quantum information technologies were random number generation and quantum key distribution.

Fast forward ten years. This feels like a different time. When you browse our monthly Crypto News, carefully selected by Dhananjoy and brought to you by the QSS working group of the CSA, you appreciate that we are already in the Quantum Era. IBM reveals the heron R2 quantum computer, we have a Roadmap to Quantum Supercomputers, D-Wave presents its 4,400 qubits Advantage2 processor. To counter the quantum threat, the NIST has already released its first batch of Post-Quantum encryption standards, with more to come, based on different mathematical problems to improve flexibility and security. The countdown to Q-day, the day when quantum computers effectively break existing asymmetric crypto, is well under way. Q-day is expected around 2030, inline with the prediction of the CSA quantum clock, which was released in 2022. The NIST has also published a draft version of its transition strategy and timeline. Quantum vulnerable algorithms, such as RSA and ECC, should be deprecated by 2030 and disallowed by 2035.

Today, every cybersecurity practitioner should understand the quantum threat and the possible solutions. The QSS workgroup of the CSA is here to help.

Of course, there are many other interesting articles. So, have a good read, and wherever possible, nice and relaxing end-of-year holidays. We will keep you posted with new Crypto News in 2025.

The Crypto News editorial is authored by the Chair of the Quantum-Safe Security Working Group (QSS WG) of the Cloud Security Alliance (CSA), Bruno Huttner, Director of Strategic Quantum Initiatives at ID Quantique SA and it is compiled by Dhananjoy Dey. Both are active members of the CSA QSS WG. The guiding principle of the QSS WG is to address key generation and transmission methods and to help the industry understand quantum-safe methods for protecting their networks and their data.

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

1. Researchers Say Here's How To Prepare Now For Post Quantum Cybersecurity

by Matt Swayne
https://thequantuminsider.com/2024/11/30/researchers-say-heres-how-to-prepare-now-for-post-quantum-cybersecurity/

Quantum computing's rapid advance demands more than just new technologies — it requires a global, multi-layered response to secure the digital landscape, according to a team of researchers, who offer five steps to secure data in the quantum future.

The team writes that as quantum computing advances, it threatens to undermine encryption systems like RSA and ECC, which secure communications and protect critical data. RSA (Rivest–Shamir–Adleman), one of the first public-key cryptosystems that is widely used for secure data transmission, relies on the mathematical difficulty of factoring the product of two large prime numbers. Elliptic Curve Cryptography, or ECC, another form of public-key cryptography, uses the properties of elliptic curves over finite fields instead of large prime factorization.

The study by the Indian Institute of Science in Bangalore researchers emphasizes that the shift to post-quantum cryptography (PQC) requires not only technical innovations but also a coordinated strategy across policy, international collaboration, and continuous research.

The researchers, including Simran Kaur and Rajat Singh, argue in their paper, Cybersecurity in the Age of Quantum Computing: Preparing for the Next Wave of Threats, that "the transition to quantum-safe encryption is not solely a technical challenge; it requires a strategic, multi-layered approach involving policy development, international collaboration, and ongoing research into quantum security standards."

THE QUANTUM THREAT

Quantum computers process information differently from classical machines by using qubits, which leverage quantum principles like superposition and entanglement. These properties enable quantum computers to solve problems exponentially faster in specific scenarios. While this computing power holds potential for breakthroughs in science and technology, it also poses a critical threat to cryptography.

Algorithms like Shor's, which are specifically designed for quantum systems, can break RSA and ECC encryption by efficiently solving problems that classical computers would take millennia to address.

"The rapid advancements in quantum computing bring with them an urgent need to reassess the security of current cryptographic systems," the researchers warn.

Because RSA and ECC encryption form the backbone of secure communications today, quantum algorithms could render these methods obsolete and expose sensitive information to adversaries.

RECOMMENDATIONS FOR THE QUANTUM ERA

The researchers outline a comprehensive strategy to mitigate quantum threats, offering five key steps. This approach emphasizes technical innovation and the critical role of policy and global collaboration. Their key recommendations include:

- **Developing Robust Policies:** Governments must lead the charge by establishing guidelines for transitioning to PQC. They write: "Governments and regulatory bodies also have a critical role to play in promoting quantum-safe standards and encouraging the adoption of PQC. By implementing forward-looking policies and providing funding for quantum research, policymakers can accelerate the development of technologies that will protect national security and critical infrastructure in a post-quantum era."

- **Encouraging International Cooperation:** Cybersecurity threats know no borders. The researchers advocate for international partnerships to share knowledge and establish universal standards. Global collaboration can ensure that no weak links exist in the chain of cybersecurity.

- **Investing in Ongoing Research:** Continuous funding and innovation are essential to staying ahead of evolving quantum threats. Ongoing research into quantum security standards is necessary to address the vulnerabilities that arise as quantum technology matures.

- **Adopting Hybrid Cryptographic Models:** During the transition period, organizations should combine classical and quantum-resistant algorithms — most of which are still in development — to maintain security while upgrading systems.

- **Workforce Development:** Training cybersecurity professionals to understand and implement PQC technologies will be critical. Without a skilled workforce, particularly in the complex quantum field, the best technologies will likely fail to be effectively deployed.

THE COST OF INACTION

The consequences of delaying preparations for a quantum future are stark. Sensitive data encrypted today could become vulnerable in the future due to a tactic called "harvest now, decrypt later." This risk is especially concerning for industries like finance, healthcare, and government, where confidentiality is paramount.

The researchers highlight the financial industry as a primary target. The financial industry relies heavily on encryption to secure transactions, protect customer data, and prevent fraud. Quantum attacks could disrupt secure communications between banks, compromise payment systems, and expose sensitive financial records.

Similarly, they stress the risk to governments, noting, “Governments around the world use encryption to protect classified information, secure diplomatic communications, and safeguard national security assets. A breach in encryption due to quantum computing could lead to espionage, data leaks, and the compromise of critical infrastructure.”

BUILDING A SECURE FUTURE

The transition to PQC will not be simple or quick. The researchers advocate for a phased approach that begins with risk assessments to identify vulnerabilities and prioritize critical systems. They also stress the importance of collaboration between academia, industry, and governments. Fostering collaboration across sectors can accelerate quantum-resistant technology adoption and ensure effectiveness.

Standards organizations, such as the U.S. National Institute of Standards and Technology (NIST), are working to finalize PQC protocols. However, the researchers emphasize that standardization alone is not enough. Standardization must be bolstered by widespread education and adoption efforts to ensure the effective implementation of these technologies.

The researchers “Preparing for the quantum era is no longer a future consideration but an immediate priority to ensure the long-term security and privacy of digital infrastructures in a rapidly evolving technological landscape.”

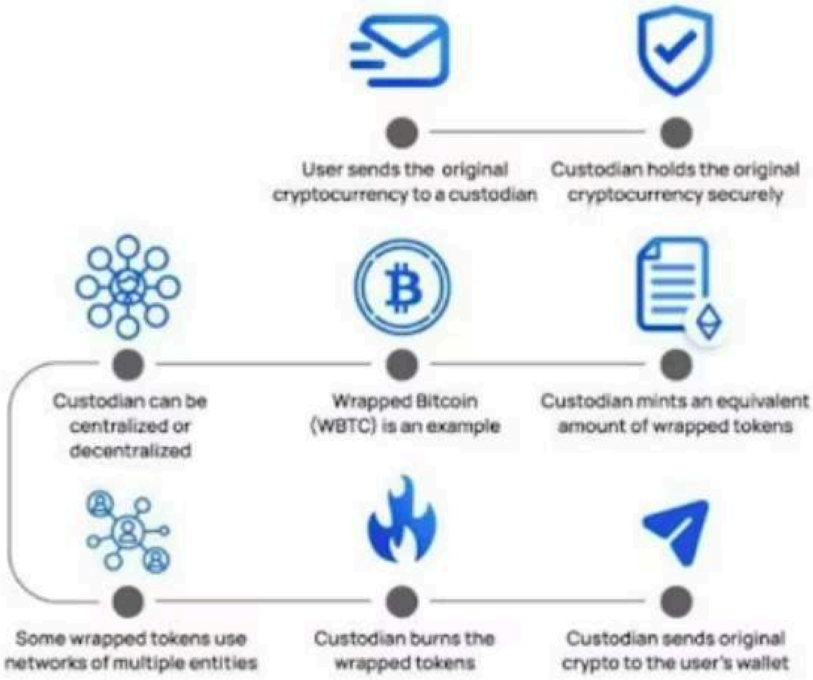
2. Can Chain-key Cryptography Eliminate Blockchain Bridges and Wrapped Tokens?

by Olayimika Oyebanji
https://hackernoon.com/can-chain-key-cryptography-eliminate-blockchain-bridges-and-wrapped-tokens

What interoperability means in this context is that two different blockchain networks can't communicate with each other except through a blockchain bridge. The absence of a unified blockchain ecosystem poses challenges for mass adoption and mainstream acceptance of blockchain technology.

This fundamental problem has its roots in the ways blockchain protocols are designed to function. For instance, blockchains have different token standards and consensus mechanisms, which make it practically impossible for the seamless transfer of digital assets from one network to another without the use of intermediaries such as blockchain bridges or wrapped tokens.

Illustration:


User sends the original cryptocurrency to a custodian
Custodian holds the original cryptocurrency securely
Custodian can be centralized or decentralized
Wrapped Bitcoin (WBTC) is an example
Custodian mints an equivalent amount of wrapped tokens
Some wrapped tokens use networks of multiple entities
Custodian burns the wrapped tokens
Custodian sends original crypto to the user's wallet

To transfer or use BTC on the Solana network, the requisite condition is that there has to be a wrapped BTC (i.e. a tokenized version of Bitcoin locked in a smart contract)to facilitate the use of such token on another blockchain network.

To keep it simple, this implies that the reason why BTC cannot be directly used on the Solana network is due to the fundamental differences between the two blockchains. Solana is a layer-1 blockchain with its own native token and specific rules for transaction processing. Bitcoin, on the other hand, operates on its own blockchain with its unique consensus mechanism and token economics.

However, despite the role played by blockchain bridges in cross-chain communication, they still pose a major challenge. Users grapple with poor or complex user interfaces, and high operation fees. Most especially, they are often compelled to find the right pairs for their digital assets because of the existence of a fragmented bridging landscape.

Another major drawback of blockchain bridges is that they are susceptible to hacks and are usually perceived as constituting a single point of failure, which undermines the principle of decentralization. According to Elliptic, a London-based blockchain analytics company, blockchain bridges lost a combined sum of over $1 billion to crypto hackers in 2022.

Blockchain networks have fundamental issues all related to user experience to address to gain mainstream adoption. The current terrain where a multi-chain ecosystem with very limited cross-chain functionality only breeds fragmented and abysmal user experience, which further makes interacting with blockchain networks and decentralized applications very complex and boring.

ckBTC : How ICP is Challenging Interoperability Model

The Internet Computer Protocol (ICP) 's Chain-key Cryptography is an innovative solution that enables chain key transactions to settle on-chain through the Internet Computer Protocol.

The underlying philosophy behind this innovation is to challenge the existing interoperability models on which most wrapped tokens operate today, thus paving the way for the emergence of user-friendly alternatives. It can potentially address the challenges that are commonly associated with wrapped tokens such as counterparty risks, price manipulation, poor user experience, etc.

Earlier this year, a pilot test was conducted in a Mexican university by the ICP Mexico in which 100 pesos worth of Chain-Key Bitcoin(ckBTC) was distributed to over 3000 students. The objective of this pilot was to demonstrate the viability of ckBTC as a payment method that does not require a bridge. This direct integration with the blockchain network can be regarded as a significant improvement in bitcoin interoperability.

Powered by chain-key cryptography and a pair of canister smart contracts holding Bitcoin directly without using blockchain bridges, chain-key Bitcoin functions as a multi-chain Bitcoin pair, which can be sent in a matter of seconds and at a very low fee.

Additionally, ckBTC is an ICRC-1-compliant token that is completely backed by Bitcoin (BTC). Having a 1:1 parity with Bitcoin, enables users to redeem ckBTC for redeemed for BTC and vice versa.

Conclusion

Blockchain protocols majorly work by obeying their own rules. However, there has been an increasing need for a unified interoperable ecosystem to unlock the full potential of blockchain technology. While blockchain bridges offer a temporary solution, they have several drawbacks limiting their widespread use and viability.

The ICP Pilot in Mexico involving chain-key Bitcoin offered fresh insights into the nature and scope of blockchain interoperability as well as the challenges it poses.

Innovations like ckBTC—a 1:1 Bitcoin-backed token with near-instant finality and negligible fees—demonstrate its practical application, as seen in a successful pilot test in Mexico. This approach not only enhances blockchain usability but also highlights the need for a unified, decentralized ecosystem, addressing the fragmentation and inefficiencies that hinder mass adoption and making blockchain interactions intuitive and accessible for mainstream users.

3. NTT Data launches Post-Quantum Cryptography consulting for finance sector

https://www.telecompaper.com/news/ntt-data-launches-post-quantum-cryptography-consulting-for-finance-sector--1520691

NTT Data will launch a consulting service for financial institutions to facilitate the transition to Post-Quantum Cryptography (PQC) from 1 December 2024. The service addresses the need for financial institutions to transition to PQC to mitigate the risk of cryptographic vulnerabilities posed by the practical use of quantum computers. It offers a comprehensive solution encompassing consulting, migration execution, and post-migration support to enhance the security of next-generation financial systems. By utilising its expertise in financial IT infrastructure development and security consulting, NTT Data said it supports the PQC transition from both operational and technological perspectives.

Tailored roadmaps will be created to align with each institution's cybersecurity action plans, addressing system requirements such as cryptographic inventory creation, priority setting, and the evaluation of data criticality. The service covers the entire transition process, from planning and execution to post-migration follow-up. The service will establish a detailed PQC migration roadmap that can be integrated into cybersecurity strategies. It will also create a cryptographic inventory to evaluate data types, usage, retention periods, importance, confidentiality, encryption algorithms, key lengths, and security levels.

The service will also identify systems unsuitable for migration and set optimal timelines for transitioning. NTT Data will conduct necessary system upgrades and actively provide updates on PQC safety evaluations. In creating cryptographic inventories, NTT Data will draw on the expertise of NTT Data Advanced Technology, its specialist security arm. NTT Data plans to extend this service to industries beyond financial institutions that are likely to require PQC migration.

The US National Institute of Standards and Technology (NIST) has predicted that quantum computers capable of breaking RSA cryptography with 2,048-bit keys may become a reality by 2030 and is advancing PQC standardisation. Reflecting this urgency, Japan’s Financial Services Agency published a report on 26 November outlining policies for domestic financial institutions to adopt PQC. Institutions are now required to devise transition plans considering factors such as data content, usage, retention periods, importance, confidentiality, and legal or regulatory obligations.

4. Which Browsers Still Use the Security Padlock Icon?

by Casey Crane
https://www.thesslstore.com/blog/which-browsers-still-use-the-security-padlock-icon/

The browser padlock icon has been widely used for decades, but some browsers have moved away from it.

The security padlock icon's meaning has been synonymous with website security for 30+ years. However, perceptions about the symbol have changed in recent years. Industry leaders debate whether the padlock symbol in front of a URL communicates the right message to users: that the connection is *secure*, meaning encrypted. Some worry it creates a false sense of security for users.

Unfortunately, according to Google's research, 89% of surveyed users misinterpreted the padlock icon's meaning. The visual clue was often misconstrued as meaning that a website is safe and trustworthy. However, the reality is that *safe* and *secure* don't mean the same thing — after all, bad guys can use encrypted connections by installing basic validation SSL/TLS certificates.

This is why some browsers dropped this visual security indicator altogether while others continue to display it. Today, we'll see which browsers still use the padlock symbol in front of the URL and which ones have traded it in for different visuals.

Let's hash it out.

Breaking Down Which of the Top 5 Browsers Use the Padlock Icon

Before diving into the list of browsers still using the padlock icon, we first must identify which browsers to check. Statscounter.com's October 2024 data indicates the following were among the six most popular browsers across all platforms (desktop, mobile, and tablet):

1. **Google Chrome** (66.68% of the market share)
2. **Apple Safari** (18.07% of the market share)
3. **Microsoft Edge** (5.25% of the market share)
4. **Mozilla Firefox** (2.65% of the market share)
5. **Opera** (2.2% of the market share)

Of course, it'll be interesting to see how the dynamics may change if Google is forced to sell its Chrome browser based on the groundbreaking August 2024 ruling against the tech giant. Google announced that it plans to fight the Department of Justice's divestiture demands by filing a counter-proposal and making a broader case in 2025.

Now that we have all that out of the way, it's time to see which browsers display the security padlock icon in their URL bars and on what platforms. For this example, we'll examine the browsers' desktop web clients (on Windows) and iOS mobile apps.

1. Google Chrome — NO

Although Google chose to display the security padlock for many years, it's now a thing of the past in Chrome. In Summer 2023, Chrome announced that it would drop the padlock icon in its browser (Chrome version 117) in favor of its more generic "tune" icon

But what about Google Chrome's iOS mobile app? The world's leading web browser doesn't display the padlock icon in the browser bar there, either. In fact, it doesn't display anything in the URL bar except the web address.

2. Apple Safari – YES

Apple Safari displays the security padlock icon in both its desktop browser and iOS mobile app.

What about iPhone iOS users – what will they see in the URL bar when they visit websites?

Displays the padlock icon for iPhone users using Safari's mobile app on an iOS device

3. Microsoft Edge – YES (and NO)

Alright, now that we've had our fun with Steve Jobs' beloved browser, let's swing back around to Bill Gates' Microsoft web client. Microsoft Edge, which initially launched in 2015 and released its Chromium-based version in 2020, eventually replaced Internet Explorer.

For those keeping track, Edge adds another checkmark to the "Yes" column for desktop browsers that display the security icon: *padlock symbol in the Microsoft Edge browser*

When you click on it, you're shown information about the site's connection encryption status and whether tracking prevention is enabled. It also offers an opportunity to review your browser's permissions and cookie settings.

How about its iOS counterpart? If you guessed YES, then you'd be wrong. The mobile app for iPhone users doesn't display the padlock icon but does show a blue shield icon

4. Mozilla Firefox – YES

Mozilla Firefox, which has been around for more than 20 years, continues to use the browser security icon. It does this in its desktop-based web client to let users know that they're using encrypted, secure connections

When you click on the lock, it'll display the "connection secure" message you're used to seeing, indicating that the connection is encrypted end to end.

What about Firefox's mobile browser for iOS devices? It, too, displays the padlock icon

5. Opera – YES (and NO)

The Opera browser has been around since the mid-1990s. While it never gained the level of notoriety shared by its Google and Microsoft counterparts, it's still loved by users who value privacy.

Now, on to the big question: does Opera show the padlock symbol in front of a URL in the desktop client? Ding, ding! It sure does, along with a VPN toggle that you can click on to turn on and off (it's set to "off" automatically)

How about Opera's iOS app – does the mobile browser have the VPN toggle or padlock symbol in front of the URL? Surprisingly, the company followed Google's lead and opted not to display the padlock – or, in this case, *any* symbol – in the URL bar

5. Is Signal Safe? A Closer Look at the Privacy Messaging App

by Naiyie Lamb
https://www.cyberghostvpn.com/privacyhub/is-signal-safe/

It's no secret that messaging apps collect and misuse data, often selling it to third-party advertisers. While WhatsApp and Facebook Messenger messages should be encrypted, these apps still collect your metadata to sell.

Signal, on the other hand, is widely considered one of the safest messaging apps available. It uses advanced end-to-end encryption, collects minimal metadata, and doesn't sell your data. Unlike many competitors, Signal is a nonprofit organization funded by donations, not ads.

In this article, we'll explore what makes Signal one of the world's most private messaging apps, who owns it, and why it's considered safe. We'll also look at the pros and cons of using Signal compared to other popular messaging platforms.

Who Owns Signal?

Signal is owned by the **Signal Foundation**, a nonprofit organization created to keep the app independent and free from ads or data tracking. It was co-founded in 2018 by **Moxie Marlinspike**, the app's original creator and a respected privacy advocate, and **Brian Acton**, who famously co-founded WhatsApp before leaving Facebook over concerns about how it handled user privacy. Acton even invested $50 million of his own money to help Signal stay true to its mission.

The app itself dates back to 2014, when Marlinspike and his team at Open Whisper Systems launched Signal to provide secure, private communication. They developed the **Signal Protocol**, a cutting-edge encryption standard so effective that it's used by apps like WhatsApp, Google Messages, and Skype.

Who Leads Signal Now?

Today, Signal is led by **Meredith Whittaker**, a privacy advocate and former Google employee who became CEO in 2022. Whittaker has continued to steer Signal toward its goal of offering a private messaging app that puts users – not advertisers – first.

Why Is Signal Unique?

What makes Signal unique is its nonprofit status. It doesn't rely on ads or sell user data to keep the lights on. Instead, Signal operates entirely on donations and grants, which gives it the freedom to focus entirely on protecting user privacy.

Signal's strong commitment to privacy has made it a favorite among security-conscious users, journalists, and even high-profile advocates like **Edward Snowden**. Its open-source design allows anyone to inspect the app's code for vulnerabilities, adding another layer of transparency that most messaging apps can't match.

Is Signal Safe?

Yes, Signal is safe and secure. Besides having staunch privacy advocates at the helm, Signal's features make it one of the most secure messaging apps available. Its strong encryption and minimal data collection practices ensure protection against surveillance.

Since its inception, Signal has been endorsed by major people in the tech and privacy arena — including NSA whistleblower Edward Snowden and Elon Musk.

What Makes Signal Secure

Signal is designed to prioritize privacy and security, making it one of the safest messaging apps available. Here's why:

- **Signal protocol.** Its end-to-end encryption means only the message sender and recipient can read the message. This makes it virtually impossible for third parties – even Signal – to snoop on conversations. Signal also uses a "Double Ratchet algorithm" to encrypt messages. This generates a new encryption key for every single message. It prevents anyone from reading conversations – even if they manage to decrypt one message.

- **Open-source.** Signal's iOS, Android, and Desktop source codes are open-source. This allows anyone to examine the code and spot potential security issues. It also makes it easy to verify and audit the app's privacy claims.

- **Minimal data collection.** Unlike other messaging apps, Signal only collects minimal metadata and doesn't sell it to third parties. And like all messaging apps, it receives government requests to provide user data. However, since it doesn't store your data, it can't provide any information except for very general timestamps. You can read Signal's responses in detail on its website's "Government Requests" page.

What Are the Limitations of Signal's Security?

While Signal is highly secure, no app is completely foolproof. Here are some limitations to consider:

- **Physical Access Risks:** If someone gains access to your phone, they could read your Signal messages. To protect yourself, enable a **Signal PIN** and lock your phone. Using disappearing messages can add an extra layer of security by deleting read messages automatically.

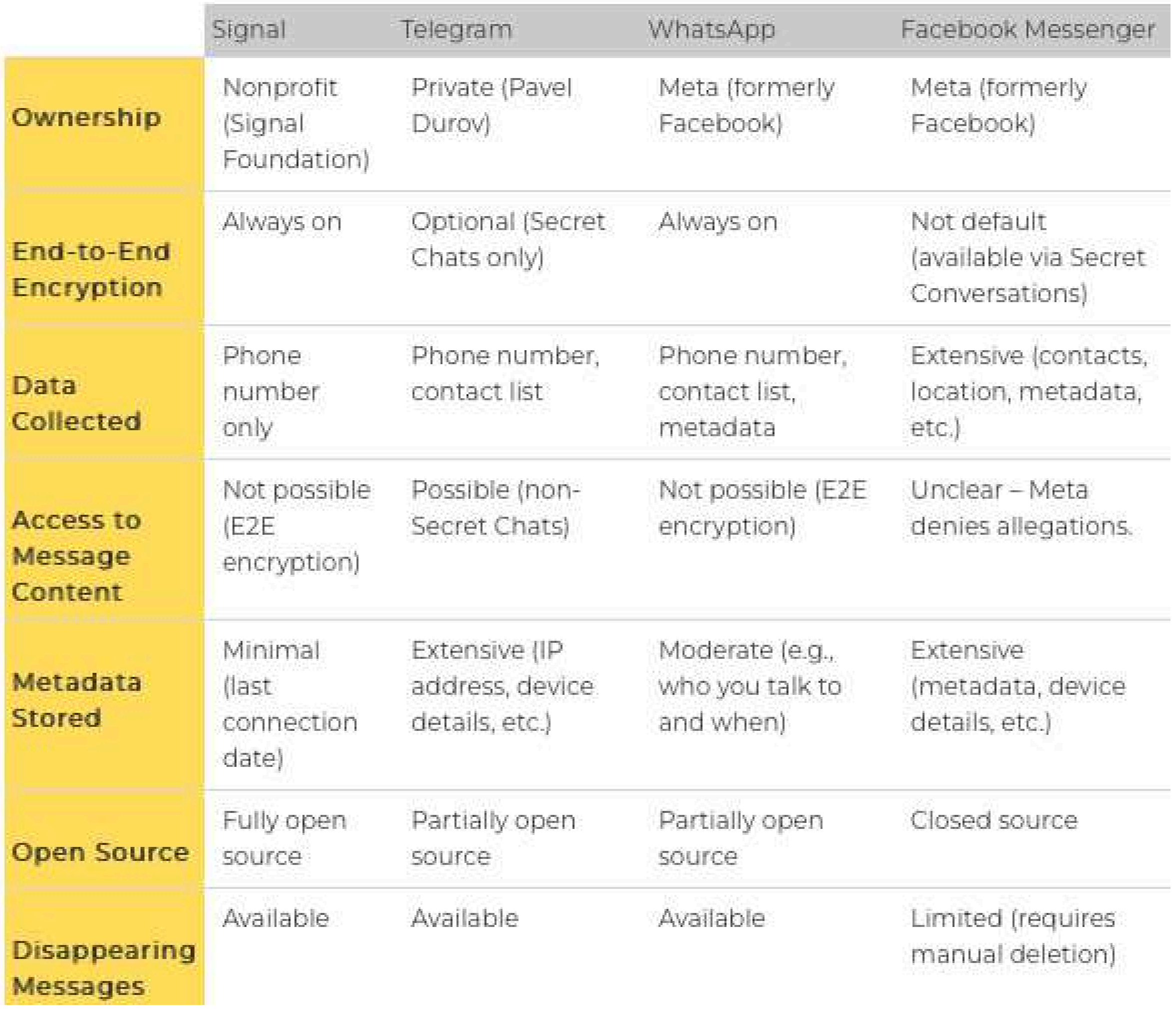
- **Phone Number Registration:** Signal requires a phone number to register, which could reveal your identity. However, you don't need to share your phone number with contacts—you can simply use a **Signal username** to communicate anonymously.

Signal versus Other Messaging Apps

Signal Messenger is now widely accepted as the most private and secure messaging app. Compared to its counterparts, it collects minimal metadata and its end-to-end encryption is always on by default. The fact that Signal's code is open source adds another level of trustworthiness and security.

It means anyone can check to see if its privacy claims are legitimate and spot security vulnerabilities. While you still need a phone number to sign up for Signal, you don't need to share your number with people you chat with – you only need to share your username.

Here's a table comparing Signal's features with other popular messaging apps.



	Signal	Telegram	WhatsApp	Facebook Messenger
Ownership	Nonprofit (Signal Foundation)	Private (Pavel Durov)	Meta (formerly Facebook)	Meta (formerly Facebook)
End-to-End Encryption	Always on	Optional (Secret Chats only)	Always on	Not default (available via Secret Conversations)
Data Collected	Phone number only	Phone number, contact list	Phone number, contact list, metadata	Extensive (contacts, location, metadata, etc.)
Access to Message Content	Not possible (E2E encryption)	Possible (non-Secret Chats)	Not possible (E2E encryption)	Unclear – Meta denies allegations.
Metadata Stored	Minimal (last connection date)	Extensive (IP address, device details, etc.)	Moderate (e.g., who you talk to and when)	Extensive (metadata, device details, etc.)
Open Source	Fully open source	Partially open source	Partially open source	Closed source
Disappearing Messages	Available	Available	Available	Limited (requires manual deletion)

6. NIST Finalizes Post-Quantum Encryption Standards

by Elizabeth Wallace
https://www.rtinsights.com/nist-finalizes-post-quantum-encryption-standards/

NIST has released its first set of finalized encryption standards designed to withstand the potential threats posed by quantum computers.

As the demand for compute power grows to support traditional high-performance computing, and now AI workloads, quantum computing is getting ever-more attention. However, developments in the market are a double-edged sword. The potential gains in raw compute power can also be applied to crack previously secure encryption algorithms.

As such, the National Institute of Standards and Technology (NIST) has released its first set of finalized encryption standards designed to withstand the potential threats posed by quantum computers. These new post-quantum cryptography (PQC) standards protect a wide range of electronic information, from confidential emails to e-commerce transactions, against future cyberattacks.

A Decade-Long Effort to Address Quantum Computing Threats

The finalized standards result from an eight-year effort by NIST to develop encryption algorithms that can resist attacks from quantum computers, which could break current encryption methods. Quantum computers, which are expected to be capable of such attacks within the next decade, represent a significant threat to digital security and privacy worldwide. The three new standards – **ML-KEM, ML-DSA,** and **SLH-DSA** – are built on different mathematical foundations to ensure resilience against both conventional and quantum computers.

These standards include detailed instructions for implementation, making them ready for immediate use by computer system administrators. NIST encourages organizations to integrate these algorithms into their systems as soon as possible to prepare for future quantum threats.

Next Steps and Future Developments

NIST continues to evaluate additional algorithms that could serve as backups to these standards, ensuring robust protection against evolving quantum computing capabilities. This ongoing effort includes a set of algorithms designed for general encryption and another for digital signatures. The results of this evaluation will be announced by the end of 2024.

In the meantime, NIST stresses the importance of adopting the finalized standards to protect against potential attacks. The new standards are expected to be the primary tools for securing digital communications and authenticating identities, reinforcing the nation's cybersecurity infrastructure.

By providing these new encryption standards, NIST reaffirms its commitment to safeguarding digital information against future threats, ensuring that America remains a global leader in technological innovation and security.

7. The Classical-Quantum Connection: Scientists Link Quantum Processors With Real-Time Classical Connection

by Matt Swayne
https://thequantuminsider.com/2024/11/21/the-classical-quantum-connection-scientists-link-quantum-processors-with-real-time-classical-communication/?utm_source=newsletter&utm_medium=email&utm_term=2024-11-2

8&utm_campaign=TQI+Weekly+Newsletter+--+Microsoft+Atom+Computing+s+Logical+Partnership+Super+Superconducting+Advance+And+More+Quantum+News+Industry+Updates

Linking quantum computers together — referred to as modularity — could help create scalable, powerful quantum systems. While that may sound as easy as stringing a bunch of cable together, it's actually very complicated. Problems, including latency — the delay in transmitting and processing data — can introduce errors that throw off calculations.

Now, IBM Quantum-led researchers report they may have found a way to make two quantum processors can work together as one by connecting them with a real-time classical communication link. According to the team, this work, published in Nature, represents a significant step toward modular quantum computing, addressing the scalability and connectivity limitations that have long constrained the field.

FINDINGS AND IMPLICATIONS

The study showed that by linking two 127-qubit quantum processing units (QPUs) via a classical connection, scientists could effectively create a 142-qubit system capable of handling computations beyond the limits of a single processor. This setup also introduced enhanced error mitigation, which boosted the system's ability to perform sophisticated tasks like creating graph states with periodic boundary conditions—a feat that exceeds the capabilities of standalone devices.

The implications, if it proves out, would be significant to quantum science and the quantum industry. Today's quantum computers are constrained by the number of qubits on a single chip and the planar connectivity — how qubits are arranged on a flat, grid-like structure — of those qubits. This research offers a path forward, demonstrating that multiple processors can be linked and operated as a unified system.

It's possible this work could move forward and create a modular system that could one day lead to fault-tolerant quantum computers, which would be essential for realizing applications in fields like cryptography, materials discovery and artificial intelligence.

DYNAMIC CIRCUITS, CIRCUIT CUTTING INNOVATIONS

The researchers report they relied on dynamic circuits, a cutting-edge quantum computing method that allows operations to be controlled in real time based on intermediate measurement results. This approach makes quantum computations more versatile by enabling on-the-fly adjustments within the coherence time of qubits — that's needed because of the fragile nature of quantum states.

Another key method employed was circuit cutting, which involves splitting large quantum circuits into smaller, manageable subcircuits. These subcircuits are run individually, and the results are recombined using classical computation. This approach gets around some of the limitations of individual processors while preserving computational integrity. For this experiment, the scientists used "cut Bell pairs" — quantum states that serve as virtual connections between processors — to enable computations that spanned both devices.

The processors communicated through a classical link, which transmitted the results of mid-circuit measurements to dynamically control subsequent operations. Error mitigation played a crucial role in this process, with techniques like dynamical decoupling and zero-noise extrapolation helping to address the delays introduced by the classical communication link.

RESULTS IN CONTEXT

The study's focus, arguably, was the creation of a graph state spanning two processors. Graph states, complex quantum states useful for a variety of applications, often require qubits to be connected in ways that exceed the physical constraints of a single processor, according to the researchers. By linking the two QPUs, the researchers were able to simulate the connectivity needed for this computation.

The experiment demonstrated that their approach could deliver results with high accuracy. Error rates were significantly lower compared to traditional methods, such as using swap gates to emulate connections, the study indicates. The integration of dynamic circuits further enhanced the system's performance, enabling the processors to operate cohesively despite their physical separation.

In addition to their technical achievements, the researchers provided a proof of concept for modular quantum computing. By tightly synchronizing the control systems of the two processors, they showed that distributed quantum systems could operate as a single, unified machine.

REMAINING CHALLENGES AND LIMITATIONS

Like all studies, several challenges remain before this moves from the lab to the proverbial living room. The classical communication link, while effective, may still face latency issues that can degrade performance. Although error mitigation techniques helped address this issue, researchers might need to contend with ways to ease the bottleneck of latency for scaling such systems. Additionally, circuit cutting, a cornerstone of the approach, comes with high computational costs. The process requires running a large number of subcircuits—a trade-off known as sampling overhead. This overhead increases exponentially with the complexity of the circuit, limiting scalability.

Another limitation: the classical link used in this experiment, though practical for near-term systems, might lack speed and coherence of a quantum link. Future systems will likely require quantum interconnects, which could transmit entangled states directly between processors, eliminating many of the challenges associated with classical communication.

FUTURE DIRECTIONS

The researchers outlined several strategies for improving and scaling their approach. Reducing the sampling overhead associated with circuit cutting is a priority. New algorithms and techniques could minimize the number of subcircuits required, making the process more efficient.

Another promising avenue is the development of quantum interconnects, as mentioned in the limitations section. These could replace classical links with quantum links that transmit entangled states, enabling faster and more coherent communication between processors. Technologies such as optical or microwave transduction could play a role in creating these interconnects, though significant technical hurdles remain.

Error mitigation will also continue to be a focus. Enhancements to techniques like dynamical decoupling and zero-noise extrapolation could further reduce the impact of latency and improve overall computation quality.

The team included scientists based at IBM Quantum and IBM Research Europe. This includes Almudena Carrera Vazquez, Stefan Woerner, and Daniel J. Egger, who collaborated to design and implement key elements of the study. Caroline Tornow is affiliated with IBM Research Europe and the Institute for Theoretical Physics at ETH Zurich. Diego Ristè contributed from IBM Quantum at IBM Research Cambridge and Maika Takita is affiliated with IBM Quantum at the T. J. Watson Research Center.

8. End-to-End Encryption Is a Critical National Security Tool

by Susan Landau
https://www.lawfaremedia.org/article/end-to-end-encryption-is-a-critical-national-security-tool

Law enforcement and national security officials have fought end-to-end encryption for decades—but the technology is more needed than ever.

For the past 50 years, governments have carried out a campaign against end-to-end encryption (E2EE), a technology that secures communications so that only the message endpoints (the sender and receiver of the message) can see the unencrypted communication. From the 1970s to the late 1990s, the fight against widespread use of E2EE was carried out largely by the National Security Agency (NSA), with the FBI joining the battle in the early 1990s. By the late 1990s, strong encryption was increasingly being adopted by nations around the world. At the same time, export controls were becoming increasingly bothersome to the computer industry. Members of Congress began introducing bills to liberalize the cryptographic export regime.

Two changes occurred in response. With increasing use of strong encryption by foreign governments, NSA increased efforts in computer network exploitation, extracting information from computer networks. The executive branch offered an olive branch to the computer industry by loosening export controls on encryption. Though not all controls ended, the ones that mattered most to the industry were lifted. The latter enabled U.S. products with strong encryption to be exported—and also made it much simpler for such products to be sold domestically.

But if NSA was comfortable with this change, law enforcement was definitely not. Within a decade, the FBI began speaking about "Going Dark"—being unable to access legally authorized wiretaps. FBI leadership repeatedly argued that it was increasingly unable to wiretap terrorists, organized crime, drug dealers, and child sexual abuse and exploitation cases. Law enforcement in the U.S. and abroad pressed hard to prevent widespread public access to E2EE.

Though the wiretap targets of interest changed over the years, the argument about the threat of encryption to wiretaps did not. And for decades, cryptographers, computer scientists, privacy experts, journalists, and human rights workers responded by pointing out the importance of ubiquitous E2EE for public safety, business security, and personal and national security. By the 2010s, members of the defense establishment were publicly voicing this argument as well.

Former NSA Director Mike McConnell, former Secretary of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn III wrote, “We believe the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.” Similarly, Michael Hayden, former director of NSA and of the CIA, stated, “American security is better served with end-to-end unbreakable encryption.” And Robert Hannigan, former head of the British General Communications Headquarters, said, “I am not in favour of banning encryption. Nor am I asking for mandatory ‘back doors.’”

Increasing cybersecurity threats also led some law enforcement officials—who had in the past strongly pressed for controls on E2EE—to shift their viewpoints. Notable among them was Jim Baker, who had been FBI general counsel during the period in which the FBI and the Department of Justice were pressing hard about Going Dark. In 2019, Baker wrote:

> *One of the most important cybersecurity risk factors is that digital isolationism is not possible. Governments, corporations and individuals in the United States and other democratic societies communicate regularly with people all over the world. Civilian and military governmental organizations operate worldwide, as do all major transnational corporations.*
>
> *As a result, many communications vital to the security and well-being of the United States are, and increasingly will be, transmitted via telecommunications equipment that is manufactured and operated by foreign companies over which the U.S. government has insufficient control in light of the risks involved.*

Baker concluded:

> *In light of the serious nature of this profound and overarching [cybersecurity] threat, and in order to execute fully their responsibility to protect the nation from catastrophic attack and ensure the continuing operation of basic societal institutions, public safety officials should embrace encryption. They should embrace it because it is one very important and effective way—although certainly not the only way and definitely not a complete way—to enhance society’s ability to protect its most valuable digital assets in a highly degraded cybersecurity environment.*

The risks that Baker was writing about have come to pass, although not exactly as Baker described. Last week, the FBI and the Cybersecurity and Infrastructure Security Agency announced that, “PRC-affiliated actors have compromised networks at multiple telecommunications companies to enable the theft of customer call records data, the compromise of private communications of a limited number of individuals who are primarily involved in government or political activity, and the copying of certain information that was subject to U.S. law enforcement requests pursuant to court orders." According to the New York Times, the targeted individuals included "President Donald J. Trump's family, as well as Biden administration and State Department officials."

As I described last week, this breach appears to be a result of wiretapping capabilities built into telecommunications networks as required by the Communications Assistance for Law Enforcement Act (CALEA). That the Chinese exploitation of U.S. telecommunications was through CALEA does not obviate Baker's argument. Our computer and communications systems are under constant attack. These are complex systems, and like all complex systems, they have vulnerabilities. This bears repeating: Complexity means the systems are insecure. Baker's point is spot on. Communications—whether between campaign managers and presidential candidates, chip engineers and software designers, or members of a research team investigating a new virus—must be protected.

For decades, technologists have been making the point that the strongest and best form of communications security is provided by end-to-end encryption; it is well past time for law enforcement to embrace its widespread public use. Anything less thwarts the nation's basic security needs.

9. Quantum Cryptography: What's Coming Next

by Mike Luken
https://blogs.cisco.com/security/quantum-cryptography-whats-coming-next?utm_source=substack&utm_medium=email

This is the second in our series of blogs about the quantum threat and preparing for "Q-Day," the moment when cryptanalytically relevant quantum computing (CRQC) will be able to break all public-key cryptography systems in operation today. The first blog provided an overview of cryptography in a post-quantum world, and this one explores what comes next.

What it will take to operationalize the new NIST PQC standards

The US government directed the National Institute of Standards (NIST) to develop new quantum-resistant cryptographic standards out of concern about Q-Day and "harvest now, decrypt later" (HNDL) risks. NIST has now released the final standards for the initial PQC algorithms. This is an impressive and rare consensus among industry stakeholders and the research community holds that the standards' algorithms represent an effective means to mitigate quantum risk. However, the standards alone are not enough to realize the goal of quantum-safe computing in practical terms. The standards are key to developing PQC solutions, but they are not a fait accompli. Operationalizing them will require more work.

Incorporating PQC algorithms into transport protocols

To accommodate the new algorithms, it will be necessary to create new, or modify existing, transport protocols. These changes can range from simply allowing the selection of the new PQC algorithms, to developing completely new standards to address factors like larger key sizes and protocol limitations. The Internet Engineering Task Force (IETF) has been working on these issues and should be soon releasing the key standards for TLS, SSH, IKEv2, and others.

Developing quantum-resistant software products

Crypto software libraries that support NIST's PQC algorithms and these protocol standards are being created and validated. There are a lot of moving parts, so the process promises to be challenging. Industry groups like the Linux Foundation's Open Quantum Safe (OQS) project have the potential to smooth the transition by facilitating agreement on standards implementation. OQS is part of the Linux Foundation's Post-Quantum Cryptography Alliance, of which Cisco is a founding member. The project is focused on the development of liboqs, an open-source C library for quantum-resistant cryptographic algorithms, as well as on prototype integrations into protocols and applications. This includes a fork of the OpenSSL library.

The IETF is also bringing industry stakeholders together to develop a new quantum-safe version of the Internet X.509 Public Key Infrastructure (PKI).This will incorporate algorithm Identifiers for the Module-Lattice-Based Digital Signature Standard (ML-DSA) that bring the public key infrastructure up to production quality.

Products will need to be updated to include these new crypto libraries and PKI capabilities. We expect products to provide PQC transport protocols initially, to address the harvest-now, decrypt-later (HNDL) vulnerability. The PQC PKI standards and industry support will likely take a bit longer to become available. As these are not directly involved in HNDL attacks, this delay does not currently pose a significant risk.

Creating quantum-resistant hardware

Cryptography is essential for secure functioning of computers and networking hardware. Cryptography makes it possible for hardware to establish trust with other hardware, as well as within itself, e.g., the operating system (OS) trusting that the hardware has not been compromised. Making hardware quantum safe will therefore mean updating a variety of hardware components and functions that rely on cryptography.

For example, the Unified Extensible Firmware Interface (UEFI) needs to be adapted so it can handle PQC algorithms and keys. Similarly, chipmakers will have to revise Trusted Platform Module (TPM) chips to support PQC standards. This affects servers, network hardware, and storage. As quantum-safe UEFI and TPM become available, hardware makers will then have to redesign products that depend on them for security. This is a two-stage process—chips first, products later—that will affect the timeline for delivering new quantum-safe hardware.

PQC hardware availability

Cisco has offered quantum-safe hardware since 2013. Many products, including the Cisco 8100 router, Cisco Catalyst 9500 network switch, and Cisco Firewall 4515, provide quantum-safe secure boot using LDWM hash-based signatures (HBS), a precursor to the NIST approved LMS. Cisco's Secure Boot checks for signed images to help ensure that the code running on Cisco hardware has not been modified by a malicious actor. New quantum-safe editions of Secure Boot and Cisco Trust Anchor Technologies will be coming out soon, implementing the new NIST PQC standards. The Cisco white paper, "Post Quantum Trust Anchors," goes into depth about how Cisco establishes quantum-safe computing using HBS and PQ signatures.

Cisco PQC hardware based on the new NIST standards is expected to become available in late 2025 or 2026. The availability of Cisco products that utilize standard industry components, such as CPUs or TPMs, will be dependent on their availability. This will likely delay their availability until late 2026 or 2027.

Next steps

What should you do to make sure you're ready for the next steps in the PQC journey? Visit the Cisco Trust Center to learn more about what Cisco is doing, the company's current capabilities and its plans for new PQC products and technologies. The next blog in this series will discuss the impacts of government regulations on PQC product availability.

10. CBP exploring post-quantum cryptography to protect sensitive data

by Anthony Kimery
https://www.biometricupdate.com/202411/cbp-exploring-post-quantum-cryptography-to-protect-sensitive-data

U.S. Customs and Border Protection (CBP) is proactively addressing the challenges posed by advancements in quantum computing, particularly concerning the security of personally identifiable information (PII) and biometric data within its IT systems. Recognizing the potential for quantum computers to compromise current cryptographic methods, CBP is implementing several key strategies to enhance data protection.

"Right now," CBP said, "encryption keeps personal and system data safe by transforming information or data into a code, making it impossible for others to read without the right key. Soon, quantum computers will be able to read coded/encrypted data easily without using a key. This will leave things like bank accounts, health records, private messages, and government data at risk."

Consequently, CBP is among the first federal agencies to explore and integrate Adoption of Post-Quantum Cryptography (PQC) into its systems. This initiative aims to strengthen data security against future quantum threats.

CBP said, “PQC addresses the ‘harvest now, decrypt later’ threat, where adversaries may be collecting encrypted data now with plans to decrypt it once quantum computing becomes sufficiently advanced. In response to this threat, CBP has taken decisive action.”

CBP’s Chief Information Officer, Sonny Bhagowalia, emphasized the necessity of this proactive approach, stating, “It is necessary to strengthen our agency’s data through post-quantum cryptography encryptions now, in order to be prepared for the security threats of the future.”

“Once previously protected data is made clear and readable through quantum decryption, it can be exposed, potentially leading to espionage, financial fraud, and other malicious activities with potential implications for national security and prosperity,” added CBP Office of Information and Technology (OIT) Deputy Assistant Commissioner Dr. Ed Mays. “In light of this imminent challenge, it is imperative to stay ahead of forthcoming challenges that may need to be mitigated during the transition to quantum-resistant cryptography.”

The federal government first recognized the importance of post-quantum cryptography with the Office of Management and Budget (OMB) Memorandum M-23-02 and the Quantum Computing Cybersecurity Preparedness Act.

CBP is aligning its cryptographic practices with the National Institute of Standards and Technology (NIST) standards. In August 2024, NIST finalized three encryption algorithms designed to withstand quantum cyberattacks. CBP said its “adherence to these standards ensures that its encryption methods remain robust against emerging quantum computing capabilities.”

To safeguard PII and biometric data, CBP is conducting thorough audits of its IT infrastructure. These audits identify components vulnerable to quantum attacks and facilitate timely updates and the integration of PQC algorithms. This proactive stance is crucial for maintaining the integrity of sensitive information.

CBP said it also employs facial recognition technology for traveler verification, ensuring that biometric data is protected through strong technical safeguards. For instance, new photos of U.S. citizens are deleted within 12 hours, and photos of most foreign nationals are stored securely within Department of Homeland Security systems. These measures are designed to limit the amount of PII used in the facial biometric process and to comply with privacy obligations.

CBP also is investing in training programs to educate its personnel about the implications of quantum computing on data security. By fostering a culture of awareness, CBP ensures that its workforce is equipped to implement and maintain PQC measures effectively.

Through these initiatives, CBP is actively fortifying its IT systems to protect PII and biometric data against the evolving landscape of quantum computing threats.

CBP said it “blocks approximately 100 million network cyber attempts each workday,” and emphasized that “these attacks are increasingly sophisticated, targeting government systems and critical infrastructure with the intent to intimidate targets, steal sensitive information, or disrupt operations. Given the criticality of our IT systems and the immense value of the data stored within them, this threat landscape requires constant vigilance and innovation."

In November 2022, CBP initiated a Quantum Safe Risk Framing Workshop to "establish how we would inventory our cryptographic systems and chart a path forward for PQC as part of our broader Zero Trust Architecture implementation."

The workshop included key personnel from CBP's Chief Information Security Officer and Chief Technology Officer organizations, the Office of the National Cyber Director, and the DHS Office of the Chief Information Officer.

"The insights gained have been instrumental in identifying cryptographic systems that require transitioning and considering factors such as hybrid approaches, dependencies, and third-party libraries," CBP said.

The workshop was also pivotal in generating a CBP PQC proof of concept, which was completed in November 2023 and documented in a *PQC Exploration Final Report*.

CBP said "the proof of concept focused on mitigating the threat to security, which allowed OIT to gain an understanding of the timeline and technical details of the transition to quantum-resistant algorithms, impacts to our operations, and necessary planning to fully transition the organization. Notably, in August 2024, the National Institute of Standards and Technology (NIST) approved the CRYSTALS-Kyber key encapsulation and the CRYSTALS-Dilithium digital signature algorithm – technologies that CBP had already tested as part of our proof of concept."

11. Countdown to Q-Day

by Issam Toufik
https://www.iotworldtoday.com/quantum/countdown-to-q-day

The next generation of quantum computers is set to unlock a panoply of new opportunities, but simultaneously pose enormous risks to the security of data, systems and critical infrastructure. Up to now, encrypting data in a way that prevents third parties such as hackers, advertisers and government bodies from viewing it via the use of a virtual private network (VPN) has been the standard and accepted way of securing and protecting digital assets. Yet while the most robust VPNs remain the most reliable cybersecurity tools available today, in the future most, if not all of them, may be rendered obsolete. That's because eventually quantum computers will be advanced enough to break the majority of encryption algorithms that are today being used to protect a lot of the world's online data.

Cryptographers call it **Q-Day** and for many, it represents a seismic event—from this point onwards, a quantum computer will be able to crack public encryption systems. The encryption schemes that are most vulnerable to quantum attacks are those that rely on large prime numbers; crucially, it is these encryption schemes that underpin almost all digital communication systems. Naturally, Q-Day will have serious implications for businesses and people worldwide—internet companies, financial institutions and governments, as well as for an individual's personal privacy. For this reason, politicians and technology leaders alike need to assess the risks of this future scenario and plan how to transition to quantum-resistant cryptography while at the same time overcoming its associated complexities.

To guarantee the smooth and ultimately successful migration to quantum-resistant methods, the starting point should be to define essential post-quantum cryptography standards. Such standards will be the initial step in terms of securing data and the first line of defense against adversaries and their newly acquired abilities to break the mathematical foundations of current encryption methods.

Preparing for an Uncertain Future

The point at which quantum computers will be able to break the encryption used to protect the world's most sensitive data remains unknown, though some experts predict it is likely to happen in the next five years. Even in the face of this uncertainty, organizations and governments globally need to take pre-emptive steps to protect their data from the impending threat of quantum-powered attacks.

This urgency is particularly acute given that "harvest now, decrypt later" (HNDL) attacks are already happening today, so the concept that "encrypted data is safe" can no longer be relied upon. Fundamentally, many organizations, businesses and governments will be negatively impacted if they fail to prepare for post-quantum cryptography risks. Adversaries and bad actors—sponsored by nation-states or criminal enterprises—will be able to access and unencrypt critical data, so data that has a lifespan beyond three years from now is at risk. If a person with nefarious intent takes a copy of existing encrypted communications data—anything over the public internet, for instance—all that it will take to expose that data a few years from now is a quantum computer. Only by securing it today will it be possible to keep it private in the future.

New Standards for a New Era

Given that many classical cryptographic systems are susceptible to quantum-enabled decryption, a new approach is required to secure sensitive data, access and communications. For this reason, cryptographers have been anticipating the arrival of quantum computers by developing new cryptographic algorithms that can credibly defend against attackers equipped with quantum computers and can also be run on classical systems.

One particularly well-known quantum algorithm developed in the 1990s, the eponymously titled "Shor's algorithm", proved that sufficiently powerful future quantum computers would be able to find the prime factors of integers much more easily than classical computers. It was the first algorithm ever developed for quantum computers, foreshadowing the weaknesses of established algorithms in a quantum future.

Today, newly standardized algorithms replace the classical systems by focusing on problems that are equally difficult for both classical and quantum computers to solve. The drive to develop new standards specifically aimed at addressing the critical need to secure digital infrastructure before quantum computing makes these attacks feasible is underway and gathering momentum. They are expected to be widely adopted in security protocols and applications in the near future.

Quantum Key Distribution: The Future of Quantum Secure Networks

In addition to the development of new cryptographic algorithms, researchers are also exploring the use of quantum key distribution (QKD) as a viable avenue to secure global communication infrastructures.

QKD is a pioneering way of securing communication that exploits the underlying principles of quantum mechanics to encode, transmit and decode messages. Simply put, it is a way to share cryptographic keys between two parties in order to protect that data and keep it inviolably secure. In practice, QKD makes it possible to send information using quantum bits that only the sender and receiver can read. All confidential information that is encrypted using this secure key will have an unparalleled level of protection, even against potential future quantum computer attacks.

Important progress has been made in the deployment of QKD-enabled communication infrastructures, with several of these types of networks under construction across the world. For example, the London Quantum Secure Network effectively delivers security key payloads to customer sites—all made possible through QKD. This foundational use case deftly highlights how quantum technology can be applied to exchange a secret that is then used to encrypt data communication between two parties. So far it is helping early customers make tentative steps towards achieving quantum secure data transmission between various sites across a wide geographic area.

To help facilitate and sustain this current growth in quantum communications there is a pressing need to develop industrial standards to help this nascent technology to succeed. This is why ETSI's Industry Specification Group (ISG) on QKD is leading activities to help accomplish this ambition by developing common interfaces and specifications for the quantum communications industry that will stimulate markets for components, systems and applications.

In addition, ETSI's TC CYBER working group on quantum-safe cryptography (QSC) looks at developing recommendations on the various proposals from industry and academia regarding real-world deployments of QSC and the development of a framework for quantum-safe algorithms. Such efforts aim to ensure that cryptographic systems remain inviolable in the post-quantum era.

Standards: The First Milestone on the Path to a Quantum-Resistant Future

As quantum computing capabilities continue to advance, governments, businesses and organizations across Europe and the rest of the world should think carefully about how they prepare for Q-Day, today. In the time-sensitive race against bad actors with quantum capabilities, the transition to a quantum-resistant future has multiple stages, with the development of standards being a foundational step. Only by standardizing post-quantum cryptographic algorithms and regulatory mandates will it be possible to ultimately move away from classic encryption and instead embrace post-quantum cryptography to address emerging quantum threats.

12. IBM reveals faster Heron R2 quantum computing chip: Why this matters

by Jayesh Shinde
https://www.digit.in/features/general/ibm-heron-r2-quantum-computing-chip-why-this-matters.html

When it comes to the cutting edge, the computing world is oversaturated with AI advancements. Unless you're talking about quantum computing, where IBM continues to position itself at the forefront of innovation. That's right, at its IBM Quantum Developer Conference 2024, the company announced significant milestones in quantum computing, including its brand new Heron R2 quantum processor. Let's see what all the fuss was about, shall we?

Back in 2022, IBM had set itself an ambitious goal known as the 100×100 challenge. Its objective was to develop a quantum computer that could run circuits with 100 qubits at a depth of 100 gates, delivering accurate results within a day's runtime. If you're new to quantum jargon, think of qubits as the quantum equivalent of classical bits – 0s and 1s – the fundamental units of information in computing. Unlike bits, which are binary, qubits can exist in multiple states simultaneously, thanks to the principles of quantum mechanics. This property allows quantum computers to process vast amounts of data at unbelievably fast speeds.

Fast forward to November 2024, and IBM has not only met but exceeded this challenge. They've developed a quantum computer capable of executing circuits with up to 5,000 two-qubit gate operations. This isn't just a feather in IBM's cap, but a significant leap for quantum computing as a whole. It demonstrates that complex quantum algorithms can be run more efficiently and accurately than ever before, inching us closer to more powerful quantum computers in the near future.

IBM Heron R2 quantum processor

Undoubtedly one of the highlights of IBM Quantum Developer Conference 2024 was its unveiling of the Quantum Heron R2 processor. Sporting 156 qubits arranged in a heavy-hex lattice, this processor employs a tunable coupler architecture. In simpler terms, it's designed to reduce "crosstalk" – the unwanted interactions between qubits that can introduce errors in computations. Reducing errors in computation – either classical or quantum – is how you increase the accuracy, reliability and overall performance of the platform. The IBM Heron R2 chip sports larger qubit count and performance capability compared to Google's 70-qubits Sycamore chip unveiled in 2023 or Intel's 12-qubit silicon-based Tunnel Falls chip from June 2023.

Imagine trying to have a conversation in a moving train compartment, where the background noise makes it hard to focus. The IBM Heron R2 processor effectively silences that background noise, allowing qubits to communicate more clearly and reliably. For example, it extends users' ability to return accurate results from quantum circuits of nearly two times the size of IBM's 2023 demonstration of quantum utility, while running up to 50 times faster in a timeframe slashed from 112 hours to 2.2 hours.

These advancements have real-world implications that could touch many aspects of our lives very soon. Quantum computers have the potential to solve complex problems that are currently too difficult or nearly impossible for classical computers – problems like optimising supply chains, discovering new pharmaceuticals, improving cryptography, and even tackling climate change models.

IBM's progress in refining and upgrading its quantum hardware, specifically with the Heron R2 chip, allows it to process more qubits while improving computational accuracy. Thanks to these computational strides, a future where quantum computers could complement or even surpass classical computers in certain tasks is very much possible to achieve.

Quantum software upgrades

Hardware isn't the only area where IBM has made strides. The company has also enhanced its quantum software stack, integrating significant improvements into Qiskit – IBM's open-source quantum computing framework. These software upgrades optimise data movement and introduce a new generation runtime, resulting in speeds exceeding 150,000 circuit layer operations per second (CLOPS).

For researchers and developers, this means they can run complex quantum experiments more efficiently – up to 50 times faster than before. This accessibility accelerates innovation, allowing for more sophisticated experimentation and a quicker path to discovering practical quantum applications.

One of the longstanding challenges in quantum computing has been bridging the gap between theoretical potential and practical application. IBM's recent achievements are significant steps in that direction. By improving both hardware and software, they're addressing the two sides of the quantum coin. It's an exciting time to be alive, and to witness such quantum computing breakthroughs!

Quantum computing challenges

However, the journey is far from over. Quantum computing still faces hurdles, particularly in error correction and scalability. While the Heron R2 processor reduces noise, completely eliminating errors remains a challenge – something that even IBM admits. Developing effective quantum error correction methods is essential for scaling up quantum systems without sacrificing accuracy.

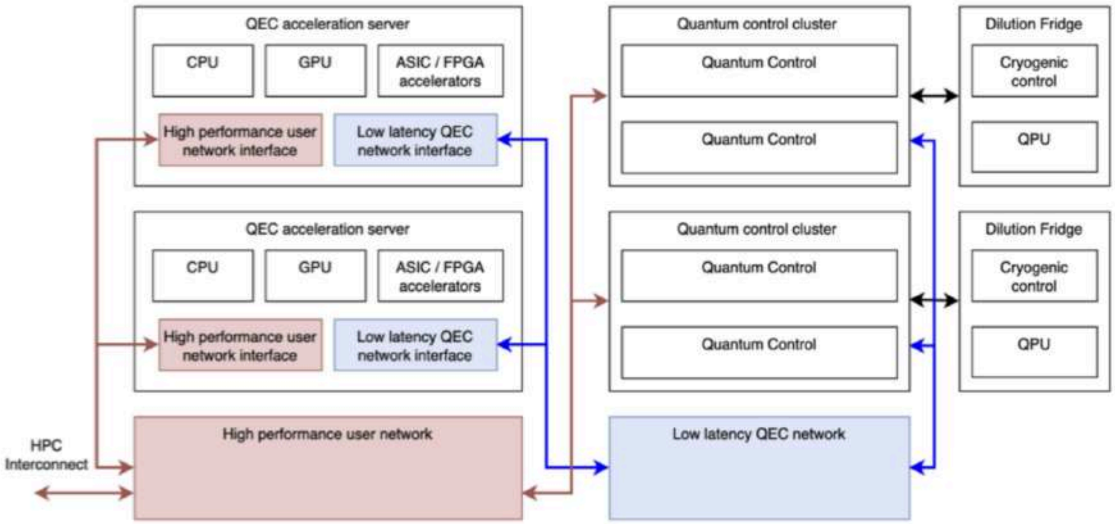
Another key challenge in this field is transitioning from theory to application. You see, as companies like IBM, Intel or Google build larger quantum computers, engineering challenges multiply exponentially. Maintaining qubit coherence (their ability to maintain quantum states, a key requirement for any quantum computer) becomes increasingly difficult as systems grow in size and complexity. All of which demands a skilled workforce adept in quantum mechanics, engineering, and software development to drive the field forward at the necessary pace.

As far as IBM's concerned, by successfully completing the 100×100 challenge and introducing the Heron R2 processor, IBM is pushing the boundaries of what's possible in quantum computing. One qubit at a time.

13. Study Offers Roadmap for Building Tomorrow’s Quantum Supercomputers

by Matt Swayne
https://thequantuminsider.com/2024/11/18/study-offers-roadmap-for-building-tomorrows-quantum-supercomputers/?utm_source=newsletter&utm_medium=email&utm_term=2024-12-01&utm_campaign=TQI+Weekly+Newsletter+--+Hard+to+Top+Topological+Rigetti+s+%24100+Million+Boost+And+More+Quantum+News+Industry+Updates

Scientists have mapped out a detailed strategy to scale quantum computers into supercomputers capable of solving problems beyond the reach of classical machines, according to a research study — How to Build a Quantum Supercomputer — posted on the pre-print server ArXiv. The team also explains their vision for this quantum supercomputer, which would require the integration of both quantum computers and classical high-performance computing systems.



The study, published by a team of researchers from several quantum startups and institutions like Hewlett Packard Labs, NASA Ames, and the University of Wisconsin, highlights both the challenges and opportunities in building utility-scale quantum systems and merging them with high performance computing systems.

They write: “Rather than replacing classical computers as general-purpose processors, quantum computers can be better understood as accelerators or coprocessors that can efficiently carry out specialized tasks within an HPC framework. Hybrid quantum–classical frameworks will be crucial not only in the near term—the noisy, intermediate scale quantum (NISQ) era [10]—but also for future fault-tolerant quantum computation (FTQC), as error-correction schemes will rely heavily on classical HPC and the number of logical qubits will be fairly small for the foreseeable future. To achieve true utility-scale quantum computing, successful integration with existing heterogeneous HPC infrastructures and the development of a hybrid quantum–classical full computing stack are necessary."

The paper also breaks down engineering hurdles, such as qubit fabrication and fault-tolerant error correction, and proposes integrating quantum processors with high-performance computing (HPC) systems. The findings could help shape the trajectory of quantum computing, potentially unlocking applications in drug development, optimization, and cryptography.

According to the researchers, building quantum supercomputers will need to emphasize systems engineering approaches to bridge the gap between research-scale and practical systems. The team explains that systems engineering is the idea that many system parameters must be simultaneously optimized for a complex system. They further argue that any advances, or breakthroughs, will depend on adopting modern semiconductor tools, improving qubit quality, and designing hybrid quantum-classical architectures.

SCALING FROM CONCEPT TO REALITY

Quantum computing, still largely experimental, faces scalability issues that prevent practical use. Existing quantum devices can handle problems involving up to hundreds of qubits, but utility-scale systems will require millions. Key findings from the study include:

- **Qubit Quality and Fabrication**: The researchers call for advanced fabrication techniques using semiconductor processes to produce qubits with consistent quality. Unlike traditional electronics, quantum bits, or qubits, are highly error-prone. The study notes that current processes often yield uneven results, with a small percentage of qubits degrading overall system performance.

- **Hybrid Quantum-Classical Systems**: The paper emphasizes the importance of pairing quantum computers with classical systems. By distributing workloads between classical and quantum processors, the researchers argue, hybrid systems can overcome bottlenecks in data management and processing.

- **Fault-Tolerant Design**: Quantum error correction is essential for scaling. The study introduces approaches to manage errors in real time, such as integrating quantum decoders with GPUs to accelerate error detection and correction.

- **Wafer-Scale Integration**: Borrowing from semiconductor manufacturing, the team proposes wafer-scale integration to embed thousands of qubits on a single chip. This would reduce communication delays and improve efficiency.

The authors write that these approaches, taken together, provide a realistic pathway to building quantum supercomputers.

SCALING QUANTUM COMPUTING FACES TECHNICAL HURDLES AT EVERY LEVEL

The researchers acknowledge that building large-scale quantum computers demands innovative solutions to challenges that evolve with the size and complexity of the system. As processors scale from hundreds of physical qubits in today's noisy intermediate-scale quantum (NISQ) machines to the millions required for utility-scale fault-tolerant quantum computing (FTQC), researchers face a mix of familiar — and potentially unprecedented — obstacles.

At smaller scales, systems with 100 to 1,000 physical qubits encounter challenges in hardware quality and stability. Variability in qubit performance, such as "fat-tail" error distributions — where a few poorly performing qubits degrade the system — poses significant risks. Frequent recalibration, driven by time-varying defects in two-level systems (TLS), hampers reliability, while external factors like cosmic rays exacerbate error rates.

Moving to 1,000 to 10,000 qubits introduces problems of integration and cost. The dense wiring needed for control and readout complicates scaling within dilution refrigerators, where space is limited. Cooling systems and control electronics become cost drivers, requiring semiconductor-inspired designs to reduce expense and power consumption.

For systems with 10,000 to 100,000 qubits, managing error correction becomes a bottleneck. Fault-tolerant protocols demand significant physical resources to correct errors faster than they accumulate. Cross-talk and gate errors further strain scalability, and debugging such complex systems grows increasingly difficult. Verification tools and diagnostic techniques, akin to those used in classical semiconductor circuits, must be adapted for quantum architectures.

Reaching scales of 100,000 to 1 million qubits will likely require distributed quantum computing, with interconnects between multiple quantum processors housed in separate dilution refrigerators. Such an approach introduces new technical hurdles, including managing inter-processor communication and dynamically allocating computational workloads.

Throughout these scales, the study emphasizes the need for adaptive solutions, such as hybrid quantum-classical systems, innovative error correction codes, and advanced fabrication techniques. The researchers argue that tackling these issues at every stage will be crucial to achieving utility-scale quantum computers capable of solving real-world problems.

PAVING THE ROADMAP

The study is grounded in a systematic analysis of challenges at different scales of quantum systems. It outlines a step-by-step progression from today's noisy intermediate-scale quantum (NISQ) systems to fault-tolerant machines with millions of qubits.

1. **Hardware Design**: The researchers evaluated superconducting qubits, focusing on ways to improve coherence times, reduce errors, and optimize performance.

2. **Architectural Integration**: By designing hybrid systems, the team seeks to make quantum processors act as accelerators rather than standalone devices. This approach mimics classical supercomputing systems that use GPUs to complement CPUs.

3. **Error Correction**: The study highlights the importance of quantum error correction codes that can mitigate noise and prevent errors from cascading through calculations.

QUANTUM RESOURCE ESTIMATION HIGHLIGHTS CHEMISTRY'S ROLE IN SCALING

The researchers also explore how improvements in qubit quality can reduce hardware demands and computational overhead for practical applications. The study focuses on quantum resource estimation (QRE) for utility-scale systems, particularly in simulating electronic structures in molecules critical to chemistry and biology.

Quantum chemistry offers a key application for FTQC, the team write, as the accurate computation of molecular ground-state energies is vital for fields like drug discovery and materials science. The study examines two molecules of interest: para-benzyne, a candidate for cancer drug design and FeMoco, an iron-molybdenum cofactor central to nitrogen fixation in agriculture. Simulating such systems is beyond the reach of classical computers for large molecules, making them prime targets for quantum advantage.

The research evaluates two approaches to implementing the quantum phase estimation (QPE) algorithm: traditional Trotterization and modern qubitization techniques. Both methods translate molecular specifications into quantum circuits, but they differ in efficiency. Qubitization significantly reduces gate complexity, requiring fewer qubits and achieving faster runtimes compared to Trotterization.

For para-benzyne, the study finds that achieving chemical accuracy—errors below 1.6 milliHartree—requires 10 million to 100 million physical qubits depending on hardware quality. Simulating FeMoco, which involves larger active spaces, demands up to 150 million qubits and runtimes spanning days to years.

However, the team writes improving qubit fidelity and algorithmic design can reduce resource requirements by up to two orders of magnitude. On advanced hardware, qubitization can outperform Trotterization by a factor of 50 in runtime, according to the study.

The researchers write: "While there is no such sharp transition line between what is classically tractable and intractable (which highly depends on the extent of quantum correlations in the studied systems), a quantum advantage gradually appears for orbital numbers beyond Norb ≈ 50. These insights also motivate future research, namely, developing quantum heuristic algorithms that could bring the transition to a quantum advantage down to smaller problem sizes. This naturally follows the development of classical algorithms, where the transition from the guarantees of FCI to the heuristics of DMRG greatly reduced the necessary resources."

THE CHALLENGES OF BRIDGING QUANTUM AND CLASSICAL

Integrating quantum computing into high-performance computing (HPC) systems presents significant design and operational challenges, according to the study. These stem from not just the physical and operational differences between quantum processors (QPUs) and classical components, but also as a result of the algorithmic hurdles in managing memory, data movement and program efficiency.

On the hardware side, quantum and classical components differ in reliability, operational timescales and communication bandwidth. Physically co-locating these resources within the same hardware node may be necessary to minimize latency and maximize synchronization for hybrid quantum-classical algorithms. For example, variational algorithms — where quantum and classical computations must interact frequently — are particularly sensitive to the overhead of data transfers, which can erode performance gains.

To address these challenges, researchers advocate for tight integration of QPUs with classical CPUs, GPUs, and FPGAs, all sharing system resources like memory and high-speed interconnects. This design ensures that hybrid systems can handle data-intensive tasks efficiently.

Equally important is the software infrastructure enabling users to program these systems seamlessly. Extending existing HPC programming environments, such as the HPE Cray Programming Environment (CPE), provides a natural solution. By incorporating tools for quantum programming, compiling, and dispatching within the familiar HPC framework, developers can build hybrid applications without extensive changes to classical workflows. This approach leverages existing infrastructure while supporting new quantum capabilities.

The integration strategy also focuses on modularity to accommodate diverse quantum technologies, from superconducting qubits to photonic systems. The team writes that quantum-specific software development kits (SDKs) such as CUDA-Q, Qiskit, Cirq, Pennylane and Classiq can interface with HPC systems, enabling scalable execution of quantum workloads.

By addressing both hardware and software challenges, the proposed quantum-HPC systems would be positioned to better deliver a user-friendly environment for hybrid computing.

LIMITATIONS AND CHALLENGES

While the study provides a comprehensive roadmap, there are limitations. The study suggests several of these challenges.

For example, scaling quantum systems is expensive, with significant costs tied to fabrication, cooling, and control systems. For instance, dilution refrigerators required for superconducting qubits are costly to operate and have size limitations.

The study also highlights the difficulty of designing error correction codes that can keep up with the demands of large-scale systems. Even with fault-tolerant designs, error rates induced by environmental factors, such as cosmic rays, present a challenge.

Quantum computing is not immune to supply chain issues, the researchers indicate, emphasizing the need for collaboration between chip manufacturers, system integrators, and quantum startups.

For the tech industry, the study offers guidance on collaborating across sectors. “The development of quantum computers must leverage expertise from the semiconductor, HPC, and quantum research communities,” the researchers write, advocating for consortia to accelerate progress.

WHERE QUANTUM GOES NEXT

The roadmap offers — or indicates — a few recommendations.

- **Standardizing Architectures**: The authors call for the development of a universal quantum operating system that can manage workloads across different quantum and classical hardware platforms.

- **Collaborative Consortia**: Building on existing models in classical computing, the study suggests forming cross-disciplinary teams to solve engineering bottlenecks.

- **Improved Algorithms**: As hardware scales, developing efficient quantum algorithms will be crucial for unlocking practical applications.

Because the paper is comprehensive and technical with material that could not be used in this article that attempts to summarize key points, it’s recommended you read the paper for a deeper, more technical dive into the roadmap.

14. Post-quantum cryptography is ready, Europe can be too

by ALESSANDRO CURIONI
https://www.politico.eu/sponsored-content/post-quantum-cryptography-is-ready-europe-can-be-too/

The key to Europe’s digital security is clear. It lies in the strength of its cryptography, which underpins everything from the data we use to chat, shop and travel to our critical supply chain, commercial and defense systems.

IBM Research has always looked toward the future of computing. We expect quantum computers to fundamentally change the paradigms of software development and computing, but they will also have major implications for our digital lines of defence.

Today’s quantum computers are not capable of breaking traditional cryptography –- yet. They are rapidly progressing toward ‘cryptographic relevance’. Meanwhile, cybercriminals may be stealing and storing data, a practice known as ‘harvest now, decrypt later’, in hopes of accessing sensitive information later with more powerful quantum machines. With data in hand that could range from personal to intellectual property or national security data, for those actors, it could be worth the wait.

The good news is that researchers around the world, including the IBM Research team in Zurich and trusted global partners, have been working proactively with governments and regulators to prepare quantum-proof cryptography for this moment. In August this year, an eight-year competition held by the United States’ National Institute of Standards and Technology (NIST) concluded with the formal publication of three standardized post-quantum encryption algorithms. These powerful new cryptographic tools will be part of the United States’ federal government’s mandatory migration to post-quantum cryptography (PQC) by 2035. This is a significant step forward for quantum safety preparedness.

IBM researchers, including many who are based in Europe, helped to lead the development of two of the three PQC algorithms selected by NIST, working alongside academic and industry collaborators who share the conviction that collaboration and interoperability together can be the lynchpin of long-term security.

In Europe there are ample efforts by member states, EU organizations and the European Commission. However, it’s imperative that these initiatives collaborate on a shared mission to drive synergy and efficient EU-wide strategies.

As the EU is currently undergoing a holistic effort to harmonize its cybersecurity standards and bring several landmark measures into practice, it should not overlook how and when to prepare for new security challenges in the quantum era. Rather, Europe must leverage this momentum and European expertise to accelerate its planning for quantum safety.

In October, the EU formally passed the Cyber Resilience Act, which will advance holistic efforts like Software Bill of Materials templates across the EU, as well as NIS 2, which placed critical infrastructure at the forefront of European national agendas. And in early 2025, the EU’s financial services-focused Digital Operations Resilience Act will officially come to life.

As Europe works to bring overlapping cybersecurity strategies together, it has the opportunity to bolster its quantum safe planning so that organizations can plan for present challenges as well as the realities they will soon face in the quantum era.

Europe is the birthplace of quantum physics, and many Europeans are shaping its future. The IBM Quantum Data Center in Europe, launched on October 1, 2024, in Ehningen, Germany – our second global quantum data center deployed worldwide – will help propel our partners’ quantum journey and soon offer access to a quantum system powered by IBM’s most-performant quantum chip to date, IBM Quantum Heron. European organizations, including over 80 in the global IBM Quantum Network in industries like government, banking, manufacturing and telecommunications, are now exploring quantum algorithms that could offer value to their industries and countries.

European governments are more equipped than ever to adopt policies that encourage rapid adoption, while maintaining the spirit of collaboration, harmonization and leadership. Advancing PQC planning is no simple feat, but the timing has never been better for dialogue, interoperability and sharing benchmarks between trusted partners. Post-quantum cryptography is ready. Bad actors aren't waiting. Europe shouldn't wait either to stay one step ahead of them.

15. NIST Issues Draft Post Quantum Cryptography Transition Strategy and Timeline

by HPC Wire
https://www.hpcwire.com/2024/11/14/nist-issues-draft-post-quantum-cryptography-transition-strategy-and-timeline/

Last summer, the National Institutes of Standards and Technology (NIST) issued the first Post Quantum Cryptography standards. Earlier this week NIST issued a draft report (Transition to Post-Quantum Cryptography Standards) to guide transition efforts. It's intended as the guide for government agencies and also sets broad goals for others (commercial and private) making the transition.

Here's the NIST summary:

> "*This report describes NIST's expected approach to transitioning from quantum-vulnerable cryptographic algorithms to post-quantum digital signature algorithms and key-establishment schemes. It identifies existing quantum-vulnerable cryptographic standards and the current quantum-resistant standards that will be used in the migration. This report should inform the efforts and timelines of federal agencies, industry, and standards organizations for migrating information technology products, services, and infrastructure to PQC. Comments received on this draft will be used to revise this transition plan and feed into other algorithm- and application-specific guidance for the transition to PQC.*"

The report is available and open for public comment until January 10, 2025.

The timeline for actual implementation isn't firm. As noted in the report, "National Security Memorandum 10 (NSM-10) establishes the year 2035 as the primary target for completing the migration to PQC across Federal systems [NSM10]: "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable to an attack by a Cryptographically Relevant Quantum Computer (CRQC). To mitigate this risk, the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."

Making the transition to PQC is expected to be difficult and costly. Dustin Moody, a NIST PQC leader and one of the authors of the draft transition document told HPCwire back in June, "The United States government is mandating their agencies to it, but industry as well as going to need to be doing this migration. The migration is not going to be easy [and] it's not going to be pain free," said Moody, whose Ph.D. specialized in elliptic curves, a commonly used base for encryption.

"Very often, you're going to need to use sophisticated tools that are being developed to assist with that. Also talk to your vendors, your CIOs, your CEOs to make sure they're aware and that they're planning for budgets to do this. Just because a quantum computer [able to decrypt] isn't going to be built for, who knows, maybe 15 years, they may think I can just put this off, but understanding that threat is coming sooner than you realize is important," said Moody. (See HPCwire article, NIST Q&A: Getting Ready for the Post Quantum Cryptography Threat? You Should be.)

Currently, there are no quantum computers capable of breaking most codes. The latest NIST reports notes, "This date reflects (2035) the urgency of transitioning to cryptographic methods that can withstand future quantum threats. However, it is important to recognize that migration timelines may vary based on the specific use case or application. Some systems, particularly those with long-term confidentiality needs or more complex cryptographic infrastructures, may require earlier transitions, while others may adopt PQC at a slower pace due to legacy constraints or lower risk profiles...NIST will work to ensure that these varying timelines are acknowledged and supported while maintaining the overall goal of achieving widespread PQC adoption by 2035."

Industry is already weighing in.

Tomas Gustavsson, Chief PKI Officer, Keyfactor, told HPCwire, "The National Institute of Standards and Technology (NIST) released its initial public draft of a post-quantum cryptography (PQC) timeline – a huge milestone that will have massive influence. With this new development, NIST has established a clear timeline for organizations to transition away from RSA and ECC, answering one of the most common questions around PQC, with expectations that other compliance frameworks will soon align with this guidance.

"For example, Federal Information Processing Standards (FIPS) are U.S. government-issued guidelines for ensuring security and interoperability in computer systems used by federal agencies and contractors, ranging across a variety of sectors including like the financial industry, telecom, automotive, manufacturing, rail, etc. Therefore, every sector and business must consider these timelines, and it is impossible to ignore them. Given that previous transitions, like SHA-1 to SHA-2, took over a decade, starting early is essential as the timeframe for PQC adoption is much shorter."

16. IBM Launches Its Most Advanced Quantum Computers

by Erin Angelini

https://newsroom.ibm.com/2024-11-13-ibm-launches-its-most-advanced-quantum-computers,-fueling-new-scientific-value-and-progress-towards-quantum-advantage

Today (Nov. 13, 2024) at its inaugural IBM Quantum Developer Conference, IBM announced quantum hardware and software advancements to execute complex algorithms on IBM quantum computers with record levels of scale, speed, and accuracy.

IBM Quantum Heron, the company's most performant quantum processor to-date and available in IBM's global quantum data centers, can now leverage Qiskit to accurately run certain classes of quantum circuits with up to 5,000 two-qubit gate operations. Users can now use these capabilities to expand explorations in how quantum computers can tackle scientific problems across materials, chemistry, life sciences, high-energy physics, and more.

This continues the achievement of milestones on IBM's Quantum Development Roadmap, and further advances the era of quantum utility as IBM and its partners progress towards quantum advantage and IBM's advanced, error-corrected system planned for 2029.

The combined improvements across IBM Heron and Qiskit can execute certain mirrored kicked Ising quantum circuits of up to 5,000 gates, which is nearly twice the number of gates accurately run in IBM's 2023 demonstration of quantum utility. This work further extends the performance of IBM's quantum computers beyond the capabilities of brute-force classical simulation methods. The 2023 utility experiment, published in Nature, demonstrated the speed results in terms of time to process, per data point, which totaled 112 hours. The same experiment, using the same data points, was run on the latest IBM Heron processor and can be completed in 2.2 hours, which is 50 times faster.

IBM has further evolved Qiskit into the world's most performant quantum software to allow developers to more easily build complex quantum circuits with stability, accuracy, and speed. This is evidenced by results gathered and published on arXiv.org using Benchpress, an open-source benchmarking tool which IBM used to measure Qiskit across 1,000 tests, largely from third parties, and found it to be the highest-performing, most reliable quantum software development kit against other selected platforms.

"Advances across our hardware and Qiskit are enabling our users to build new algorithms in which advanced quantum and classical supercomputing resources can be knit together to combine their respective strengths," said Jay Gambetta, Vice President, IBM Quantum. "As we advance on our roadmap towards error-corrected quantum systems, the algorithms discovered today across industries will be key to realizing the potential to solve new problems realized through the convergence of QPUs, CPUs, and GPUs."

New Software Tools to Advance Development of Next-Generation Algorithms

The IBM Quantum Platform is further expanding options with new Qiskit services such as generative AI-based capabilities and software from IBM partners, allowing a growing network of experts across industries to build next-generation algorithms for scientific research.

This includes tools such as the **Qiskit Transpiler Service** to power the efficient optimization of quantum circuits for quantum hardware with AI; **Qiskit Code Assistant** to help developers generate quantum code with IBM Granite-based generative AI models; **Qiskit Serverless** to run initial quantum-centric supercomputing approaches across quantum and classical systems; and the IBM Qiskit Functions Catalog to make services available from **IBM, Algorithmiq, Qedma, QunaSys, Q-CTRL,** and **Multiverse Computing** for capabilities such as reducing the performance management of quantum noise, as well as abstracting away the complexities of quantum circuits to simplify the development of quantum algorithms.

"Algorithmiq's tensor error network mitigation algorithm (TEM), available through the IBM Qiskit Functions Catalog, offers state-of-the-art error mitigation for circuits at utility scale by leveraging steps towards quantum-centric supercomputing approaches, delivering the fastest quantum runtime we've yet offered to users," said Matteo Rossi, CTO, Algorithmiq. "With the recent advancements we've made to combine quantum computers with post-processing on GPUs, we are pushing TEM's capabilities to support circuits with up to 5,000 entangled quantum gates – a milestone for scaling quantum experiments and tackling complex problems. This could open the door to quantum simulations and computations previously constrained by noise limitations."

"Progress across IBM quantum hardware and software are instrumental to Qedma's mission to build services that will allow our users to run the longest and most complex quantum circuits," said Dorit Aharonov, Chief Scientific Officer, Qedma. "Combined with our own achievements in error mitigation, which we offer via Qedma's service in the IBM Qiskit Functions Catalog, we look forward to furthering our mission of enabling global users to build algorithms with today's quantum systems – and to achieve increasingly accurate results of scientific value."

Qiskit Fuels Quantum and Classical Integration Towards Future of Computing

As the next evolution of high-performance computing, IBM's vision of quantum-centric supercomputing aims to integrate advanced quantum and classical computers executing parallelized workloads to easily break apart complex problems with performant software, allowing each architecture to solve parts of an algorithm for which it is best suited. Such software is being designed to seamlessly and quickly knit problems back together, allowing algorithms to be run that are inaccessible or difficult for each computing paradigm on its own.

RIKEN, a national scientific research institute in Japan, and Cleveland Clinic, a leading academic medical center and biomedical research institution with an on-site and utility-scale IBM Quantum System One, are exploring algorithms for electronic structure problems that are fundamental to chemistry.

These initiatives represent the first steps towards quantum-centric supercomputing approaches to realistically model complex chemical and biological systems, a task historically believed to require fault-tolerant quantum computers.

Early examples of these types of workflows are methods based on parallel classical processing of individual samples from quantum computers. Building on prior techniques, such as QunaSys's QSCI method, IBM and RIKEN researchers have performed sample-based quantum diagonalizations in quantum-centric supercomputing environments, which make use of quantum hardware to accurately model the electronic structure of iron sulfides, a compound present widely in nature and organic systems.

Now available as a deployable Qiskit service, this same technique is being leveraged by Cleveland Clinic to explore how it could be used to implement quantum-centric simulations of noncovalent interactions: bonds between molecules that are essential to many chemical, biological, and pharmaceutical science processes.

"This research is an example of what makes our research partnership successful – bringing together IBM's next-generation technologies with Cleveland Clinic's world-renowned expertise in healthcare and life sciences," said Lara Jehi, MD, Chief Research Information Officer at Cleveland Clinic. "Together, we are pushing through traditional scientific boundaries using cutting-edge technology such as Qiskit to advance research and find new treatments for patients around the globe."

"With our partners at IBM, we were able to leverage their advanced quantum computing electronic structure algorithm to study – for the first time – intermolecular interactions on the on-site IBM Quantum System One at Cleveland Clinic, which are important for potential future applications in drug discovery and design," said Kennie Merz, PhD and quantum molecular scientist at Cleveland Clinic.

"The RIKEN Center for Computational Science (R-CCS) is conducting the Japan High Performance Computing-Quantum (JHPC-Quantum) project, which aims to build a quantum-HPC hybrid computing platform by integrating our supercomputer, Fugaku, with an on-premises IBM Quantum System Two powered by an IBM Quantum Heron processor. In the era of quantum utility, we will strongly support the initiative's goal of demonstrating quantum-centric supercomputing approaches by using our platform as a first step towards this new computing architecture," said Mitsuhisa Sato, the director of Quantum-HPC Hybrid Platform Division, RIKEN Center for Computational Science.

Additionally, Rensselaer Polytechnic Institute is using Qiskit tools to take initial steps to build IBM's first realization of quantum-centric supercomputing on a university campus. With performant software, RPI and IBM are aiming to successfully connect workloads across the AiMOS classical supercomputer and IBM Quantum System One, both located on RPI's campus, into a single computational environment managed by a standard high-performance computing resource manager.

"Since unveiling IBM Quantum System One on the RPI campus earlier this year, we have taken steps toward another significant first by starting the work to link the quantum system and our AiMOS supercomputer," said Martin A. Schmidt, Ph.D., president of RPI. "This moment is a testament to our longstanding partnership with IBM, and, like the pairing of quantum computing and supercomputing, our two institutions together will drive exciting breakthroughs in the years to come."

17. US Gov Agency Urges Employees to Limit Phone Use After China 'Salt Typhoon' Hack

by SecurityWeek News

https://www.securityweek.com/us-gov-agency-urges-employees-to-limit-phone-use-after-china-salt-typhoon-hack/

The US government's Consumer Financial Protection Bureau (CFPB) is directing employees to minimize the use of cellphones for work-related activities, following an intrusion into major telco systems attributed to Chinese government hackers.

According to a *Wall Street Journal* report, the agency sent an email to all employees and contractors with a simple directive: "Do NOT conduct CFPB work using mobile voice calls or text messages."

The warning comes on the heels of a series of hacks into US telcos and broadband providers blamed on Salt Typhoon, a Chinese government-backed cyberespionage hacking operation. The group has reportedly broken into companies like Verizon, AT&T and Lumen Technologies and has used that access to surveil politicians and critical communications systems.

"While there is no evidence that CFPB has been targeted by this unauthorized access, I ask for your compliance with these directives so we reduce the risk that we will be compromised," the CFPB said in the email.

The *Journal* said the CFPB's security leadership has advised staff to avoid discussing nonpublic data via voice calls or text messages on either work-issued or personal phones. Instead, government employees were instructed to use secure platforms like Microsoft Teams and Cisco WebEx to mitigate risks.

While the CFPB confirmed no direct targeting of its systems, the directive aligns with federal concerns over the scope of the Salt Typhoon intrusions that has ensnared sensitive communications of key U.S. government officials, senior policymakers, and political figures.

According to reports, the Chinese hacking team has already siphoned data on calls recorded phone audio from high-value targets in the US, including individuals associated with both US presidential campaigns.

Technical details and official information on the Salt Typhoon intrusions are being kept under wraps.

18. The Trump Administration Must Make Quantum Technology a Priority in the First 100 Days

by Sam Howell

https://www.justsecurity.org/104566/next-us-president-must-make-quantum-tech-priority/?utm_source=substack&utm_medium=email

The world is at the brink of a quantum revolution, and America's quantum technology lead is narrowing rapidly. The United Nations recently proclaimed 2025 as the International Year of Quantum Science and Technology, predicting that quantum will be a "key cross-cutting scientific field of the 21st century" with "tremendous impact on critical social challenges." Yet just when the global quantum ecosystem is nearing significant technical breakthroughs, the United States' historic edge in the technology is diminishing.

Incoming President Donald Trump has a unique opportunity to reverse this trend and should act quickly in the first 100 days to reinvigorate America's quantum competitiveness. Technology competition is a defining feature of today's geopolitical landscape and the strategic competition between the United States and China. Quantum – a technology with extraordinary economic and military potential – is set to play an outsized role in determining which country prevails. China already outperforms the United States in quantum communications and is making rapid progress in other subsets of quantum technology as well. But there are critical steps that the incoming administration can still take to win the quantum race.

Winning the Quantum Race

Quantum technology is an interdisciplinary field that combines quantum mechanics and information theory to produce new types of computers, sensors, and networks. The speed, precision, and functionality of quantum technologies far exceed that of classical technologies, which could help unlock transformative advancements across a range of industries. The far-reaching potential of quantum technology is what makes it so powerful—the countries with the best quantum technologies will also have the best pharmaceuticals, batteries, fertilizers, intelligence collection, and weapons systems. Quantum technology leadership enhances overall national competitiveness while lagging in quantum could mean falling behind in vital sectors, from energy to pharmaceuticals to material design and agriculture.

Given its prospective impact, quantum has become a key battleground in the technology competition between the United States and China. The first-mover benefits associated with quantum technologies are substantial. The first country to scale, commercialize, and integrate quantum will unlock a toolkit of capabilities—such as the ability to crack public key encryption or conduct complex surveillance operations—that non-quantum equipped adversaries will struggle to counter. The country leading in quantum also will possess science and engineering expertise that is extremely difficult to cultivate and could take competitors years to replicate.

The quantum frontrunner could even establish early market dominance, set technology standards, and shape governance frameworks that influence whether quantum technologies are used to promote or undermine democratic principles. Absent action to boost America's quantum competitiveness, the United States risks repeating mistakes made in the race to develop and deploy 5G technology. The United States' failure to outpace China in 5G means that Chinese firms now connect 80 percent of global 5G devices, maintain 70 percent of 5G base stations, and hold one third of 5G-related "standard-essential" patents. At a minimum, this China-dominated ecosystem challenges U.S. companies' ability to compete abroad, complicates the United States' ability to partner with countries dependent on potentially compromised Chinese infrastructure, and reduces U.S. influence over the ways in which 5G technologies are employed.

The United States can leverage several advantages to avoid a similar outcome in quantum. The United States is widely considered the global leader in two of the three quantum technology subsets – quantum computing and quantum sensing – thanks to its cohesive national quantum strategy, top-notch research facilities, diverse quantum industry, high private investment, and consistent output of quality quantum-relevant publications. But

China is closing the gap. The Chinese Communist Party pours dramatically more public funding into general quantum technology research and development (R&D) than the United States, Chinese researchers publish more frequently than their U.S. counterparts, and Chinese scientists have achieved several notable technical breakthroughs.

China is already using its dominance in the third quantum technology subset—quantum communications—to support broader geopolitical objectives. In January 2024, Chinese scientists announced the establishment of a 3,800-kilometer quantum network connecting Urumqi to Moscow, Russia. China and Russia reportedly plan to expand the network to Brazil, India, and South Africa, which would render communications and data sharing between the BRICS partners unbreakable. In short, China actively intends to undermine the United States' strengths and become the global quantum superpower.

Recommendations for the Next U.S. Administration

The incoming Trump Administration has a responsibility and rare opportunity to tip the quantum scales in the United States' favor. Changes in presidential administrations present a unique chance to readjust national security priorities, reallocate resources, and set a new tone for U.S. policy. The new administration can signal American strength in quantum technology by taking a few immediate actions to boost the U.S. quantum ecosystem.

First, the administration should award implementation funding to The Bloch Tech Hub, one of the U.S. Economic Development Administration's (EDA) two quantum-focused Tech Hubs. The Tech Hubs Program coalesces relevant regional institutions to "manufacture, commercialize, and deploy technology that will advance American competitiveness." The Bloch—led by the Chicago Quantum Exchange and located across Illinois, Indiana, and Wisconsin — seeks to advance quantum computing and communications technology, "enabling new solutions for sectors such as finance, energy, biotechnology, and manufacturing." If successful, The Bloch could play a key role in driving U.S. quantum technology research, broadening the United States' pool of quantum talent, and improving supply chain security.

Though The Bloch received a $500,000 Consortium Accelerator Award in July 2024, it was not included on the EDA's list of recipients of $504 million in Tech Hub Program implementation support. Elevate Quantum — the EDA's second quantum-specific Tech Hub — was included on the list and noted that implementation funding helped attract additional private capital, secure new consortia participants, and establish world-class quantum facilities. Similar support for The Bloch is critical for the hub to deliver on its promise to accelerate the development and adoption of quantum technologies.

Second, the president should pressure Congress to pass the National Quantum Initiative Reauthorization Act. The House Science, Space and Technology Committee unanimously approved the legislation in November 2023, which has continued slowly moving through the House. But the status of the Senate's version—which is not yet publicly available—is unknown.

The National Quantum Initiative (NQI) — initially enacted in 2018 for a five-year period – launched a whole-of-government, coordinated approach to quantum R&D, established various funding mechanisms for quantum technology, and legislated quantum oversight authority to specific government bodies. The reauthorization would build upon the NQI and address its weaknesses by appropriating funds for new quantum institutes and foundries, workforce development, supply chain diversification, and the transition from fundamental research to more advanced R&D and commercialization. U.S. quantum leadership hinges on reauthorization of the NQI and the president cannot afford further delays to get it across the finish line.

Finally, the new administration should establish a quantum-focused international body to enhance cooperation between the United States and its allies on quantum R&D, supply chain security, workforce development, standards, and regulation. Such cooperation is important because no single country holds all of the keys to the quantum puzzle—quantum technology is deeply international with globally diffused talent, infrastructure, and industrial capabilities. Like-minded countries must maximize their comparative advantages to outpace competitors in the race to produce the most advanced quantum technologies.

Most U.S. international engagement on quantum technology has taken the form of bilateral agreements negotiated by the U.S. Department of State, such as those with Japan, the United Kingdom, and Australia. Bilateral agreements are valuable, but comprehensive multilateral frameworks—none of which currently exist—are equally important, particularly as countries begin to implement and attempt to align quantum technology export controls. The international body for quantum could model the spirit of the EU-US Trade and Technology Council or the Chip 4 Alliance and should include representatives from government, industry, and academia.

The United States' long-standing supremacy in quantum technology—a bedrock of U.S. economic and national security—is in peril at an important inflection point. Quantum technologies are rapidly nearing market readiness and U.S. adversaries are more determined than ever to beat the United States to the quantum punch. But the change in administration presents a unique opportunity to reassert American leadership in quantum and shape a brighter future. The incoming Trump Administration can seize the moment by fully resourcing the Tech Hubs Program, passing the NQI reauthorization, and leveraging the power of the United States' alliances.

19. Embracing the Future of Cryptography and Identity Management

by Tony Bradley
https://www.forbes.com/sites/tonybradley/2024/11/08/embracing-the-future-of-cryptography-and-identity-management/

As we prepare to step into 2025, the cybersecurity landscape is shifting rapidly, driven by advances in quantum computing, the proliferation of IoT and OT devices, and a wave of stringent new regulations.

These forces are reshaping the very fabric of digital security. For businesses and governments alike, the key to thriving in this evolving landscape is proactive preparation. Experts across the industry are already charting a path forward to address these emerging challenges.

I recently spoke with experts from Keyfactor and Thales about emerging trends and thinks to watch for in 2025—touching on the growing importance of post-quantum cryptography, the imperative for IoT/OT security, new regulatory dynamics, the rise of short-lived certificates, and how certificate and identity management will be critical in safeguarding the future.

Post-Quantum Cryptography Moves to the Forefront

Quantum computing is poised to shift from an abstract concept to an urgent topic of action in 2025. Unlike traditional computers, quantum systems use quantum bits, allowing them to solve complex mathematical problems exponentially faster—posing a potential existential risk to current encryption techniques that protect much of today's digital communications.

Historically, the discussion around post-quantum cryptography was often speculative, akin to a distant Y2K. But the urgency is growing. Chris Hickman, Chief Security Officer at Keyfactor highlighted that quantum computing timelines are becoming clearer, with real impacts possible as early as 2029. This means organizations can no longer afford to wait; instead, they must prepare today for a quantum-safe tomorrow by investing in crypto-agility—being ready to adapt to quantum-resistant standards as soon as they are needed.

Todd Moore, Vice President of Encryption Products at Thales, echoes this sentiment by emphasizing the importance of crypto-agility. "Crypto-agility is key for ensuring that as soon as quantum threats become real, organizations can pivot to new cryptographic standards without major disruptions," Moore noted. This proactive approach will be essential as quantum computing continues to develop, bringing both opportunities and threats to the forefront of cybersecurity.

IoT and OT Security Reach Critical Maturity

The complexity of IoT and OT devices introduces unique security challenges. These devices are now ubiquitous—used everywhere from factories to hospitals—and often lack user interfaces that make traditional security practices applicable. As a result, managing certificates for these environments presents distinct hurdles, especially in highly regulated industries.

In 2025, IoT and OT security will take center stage. Particularly in critical sectors like industry and government, a high degree of assurance is required for device security. Solutions that focus on automated certificate lifecycle management and tailored public key infrastructure deployments are crucial for ensuring resilience. Customization and consultation are key, and partnerships that bring industry expertise are driving secure, scalable solutions for these environments.

The Compliance Wave: Regulatory Requirements as a Catalyst for Security

Another significant driver of change in 2025 will be regulatory pressure. The European Union's Cyber Resilience Act, for instance, is anticipated to significantly impact cybersecurity practices, potentially surpassing even GDPR in terms of its scope. It emphasizes improving product security throughout their entire lifecycle—requiring businesses to take accountability for cybersecurity from the outset.

Jordan Rackie, CEO of Keyfactor, highlights that compliance isn't just about avoiding penalties; it's about embedding security deeply enough that organizations can confidently operate in this changing landscape. The CRA and similar regulations make it clear that proactive, identity-centric security measures are needed. This includes focusing on public key infrastructure and certificate lifecycle management to ensure that all digital assets are covered.

For companies looking to stay ahead of compliance requirements, consolidating their PKI infrastructure and automating renewals are effective ways to manage security efficiently and meet emerging standards. This proactive stance will help organizations not only stay compliant but also protect their assets against increasingly sophisticated cyber threats.

Short-Lived Certificates and Crypto-Agility as the New Normal

Long gone are the days when certificates were renewed every few years. As we approach 2025, short-lived certificates will become a new norm, driven by companies like Google and Apple pushing for tighter security through shorter certificate validity—90 days or even as low as 45 days.

Short-lived certificates mean increased agility is essential. "The days of setting it and forgetting it are over," Chris Hickman mentioned, underscoring the need for automated, streamlined certificate lifecycle management to keep pace with these changes. By investing in crypto-agility—both in infrastructure and in processes—organizations can minimize risks associated with certificate compromise and expiration, thereby reducing the chances of breaches and system outages.

The future will favor organizations that can securely automate and adapt. Solutions that allow for rapid deployment, validation, and renewal of certificates will be crucial in minimizing exposure to cyber threats. In this way, companies not only meet new security standards but also enhance their ability to respond to evolving cyber risks.

Safeguarding Critical Infrastructure with Identity Management

Securing critical infrastructure is set to be one of the most pressing challenges in 2025. The digitalization of critical services—ranging from power grids to defense systems—brings enhanced efficiency and real-time monitoring but also new vulnerabilities. According to the 2024 Thales Data Threat Report, a staggering 93% of critical infrastructure respondents reported an increase in attacks over the past year. Moore noted that "Identity and Access Management is increasingly the backbone of critical infrastructure cybersecurity, ensuring that only authorized individuals have access to sensitive systems."

With threats on the rise, identity and certificate management are no longer optional—they're foundational elements for ensuring that only trusted entities interact with sensitive systems. As infrastructure grows more connected, solutions such as centralized encryption key lifecycle management become essential. IAM, combined with effective encryption management, will play a critical role in securing the essential services on which societies depend.

The convergence of different PKI infrastructures—bringing together multiple solutions under one management platform—will also be a priority for many organizations. This convergence will allow for greater security coverage and a unified approach, which is vital for protecting critical systems while maintaining efficiency.

Looking Ahead: Setting the Standard for Cybersecurity

The cybersecurity challenges facing organizations in 2025 are considerable, but they also present an opportunity to establish stronger, more proactive security measures. From preparing for quantum threats to embracing IoT/OT security and meeting new regulatory requirements, the emphasis is shifting from reactive measures to building an inherently secure infrastructure.

Keyfactor's Rackie stressed that preparing for the quantum age and ensuring compliance with new regulations are tasks that require immediate attention. By investing in crypto-agility, automated lifecycle management, and identity-first security practices, organizations are not just reacting to change—they're leading it. Proactive engagement with cybersecurity isn't just about defending against threats; it's about setting the standard for security excellence and being ready for what's next.

As the landscape evolves, those who anticipate and prepare for these changes will not only protect their assets but also thrive in an increasingly digital world. Embracing a secure tomorrow begins with action today. To learn more about how to prepare for these shifts and connect with industry leaders, attend Keyfactor's Tech Days 2025. Register now and be part of the conversation shaping the future of cybersecurity.

20. Central banks hail 'ground-breaking' post-quantum cryptography experiment

by Ian Hall
https://www.globalgovernmentfintech.com/banque-de-france-singapore-quantum-cryptography-resilience/

The successful completion of a 'ground-breaking' joint experiment in 'post-quantum cryptography' (PQC) has been announced by two influential central banks.

Banque de France (BdF) and the Monetary Authority of Singapore (MAS) said this week (5 November) that their technical experimentation 'marks a crucial milestone in the evolution of the protection of international electronic communications against the cybersecurity threats posed by quantum computing.'

The authorities trialled use of 'quantum-resistant' cryptographic algorithms for the signing and encryption of emails across continents over conventional internet technologies. Their aim was to bolster security levels for electronic communications in the future 'while retaining compatibility with existing internet standards, technologies and communication channels.'

'Emails are particularly sensitive, as they may carry confidential information, making them a prime target for cyberattacks,' notes a BdF/MAS joint-announcement (which is accompanied by a 16-page technical report). 'This experiment not only demonstrates the practical feasibility of these new security methods but also their effectiveness in widely-adopted application environments.'

BdF and MAS will now progress to a further stage of experimentation that will look to 'extend PQC to critical financial transactions, particularly cross-border transactions on payment networks.'

Next step: payment systems

The project's first stage included what is described as a 'hybrid' approach, meaning that present-day algorithms were combined with post-quantum algorithms to ensure security and compatibility with existing systems, while preparing for the cybersecurity threats posed by quantum computing.

This approach was taken based on recommendations from the French Cybersecurity Agency (ANSSI) and the US National Institute of Standards and Technology (NIST).

The algorithms tested and implemented for email encryption and signature are described as 'versatile' and able to be applied to other 'critical settings', such as secure payment systems.

'By integrating PQC algorithms into payment networks, financial institutions can future-proof their security measures against the looming threat of quantum computing, ensuring the long-term integrity and confidentiality of sensitive financial data,' the authorities state as eye their co-working's next step.

'By collaborating on this pioneering experiment, BdF and MAS affirm their commitment to anticipating future threats and ensuring the security of global financial systems. This initiative also highlights the importance of international cooperation in addressing emerging cyber threats,' the authorities state.

Inter-institutional communications resiliency

"Although quantum computing opens up promising new prospects in various fields, it also brings a threat to cyber security, particularly in protecting our communications," said BdF first deputy governor Denis Beau, saying that the authority "has been anticipating and multiplying experiments in post-quantum cryptography with its partners since 2022".

"The results of this first cooperation with the Monetary Authority of Singapore in the field of post-quantum cryptography reassure us of our ability to make our inter-institutional communications resilient," Beau added.

“The looming threat of quantum-powered decryption is transforming cybersecurity strategies in financial services globally,” said MAS deputy managing director (corporate development) Jacqueline Loh. “The focus is now shifting towards cryptographic agility and ensuring systems can adapt by integrating with quantum-resistant algorithms. Financial institutions that prepare early for the quantum era will not only mitigate future risks but also position themselves to retain public trust in digital financial services.”

Senior figures involved in the work have included, on the BdF side: Olivier Lantran and My Phuong Dulman, who are respectively, head and head of digital at BdF’s innovation centre Le Lab, and cryptography project manager Nicolas Margaine; and, on the MAS side: deputy director Edwin Goh, executive director (data and technology architecture) Damien Pang (who is also MAS’s deputy chief fintech officer) and chief information security officer Claudean Zheng.

21. Cops Suspect iOS 18 iPhones Are Communicating to Force Reboots, Making Unlocking Harder

by Juli Clover
https://www.macrumors.com/2024/11/07/ios-18-forcing-reboots-law-enforcement/

Law enforcement officials in Detroit, Michigan are warning other police officers about an alleged iPhone change that causes Apple devices stored for forensic examination to spontaneously restart, reports *404 Media*.

iPhones that are undergoing examination have apparently been rebooting, which makes them harder to unlock with brute force methods, and Michigan police think that it's due to a security feature that Apple added in iOS 18. A document found by *404 Media* speculates that iPhones running iOS 18 are causing other iPhones to restart when those iPhones have been disconnected from a cellular network.

> *The purpose of this notice is to spread awareness of a situation involving iPhones, which is causing iPhone devices to reboot in a short amount of time (observations are possibly within 24 hours) when removed from a cellular network. If the iPhone was in an After First Unlock (AFU) state, the device returns to a Before First Unlock (BFU) state after the reboot. This can be very detrimental to the acquisition of digital evidence from devices that are not supported in any state outside of AFU.*
>
> *It is believed that the iPhone devices with iOS 18.0 brought into the lab, if conditions were available, communicated with the other iPhone devices that were powered on in the vault in AFU. That communication sent a signal to devices to reboot after so much time had transpired since device activity or being off network.*

After First Unlock, or AFU, denotes a device state where the owner has unlocked their device with a passcode or Face ID at least one time since it was powered on. It is easier for law enforcement to get into a device in AFU mode with iPhone unlocking tools from companies like Cellebrite. A restart apparently makes the process more difficult.

The digital forensics lab that noticed the issue had several iPhones in AFU state reboot, including iPhones in Airplane mode and one in a faraday box. Since a faraday box blocks all electronic signals from reaching a device, there wouldn't be a way for an iPhone running iOS 18 to communicate with an iPhone in a functional faraday box.

The police document speculates that this is "an iOS 18.0 security feature addition" because one device running iOS 18 also rebooted after a period of isolation and inactivity. Several other devices in the same area did not, however, restart, and there is no evidence that Apple has added a feature that causes older iPhones to reboot when in contact with an iPhone running iOS 18.

Law enforcement officials recommend isolating iOS 18 devices from other iPhones that are in an AFU state as further testing takes place.

> *The specific conditions that must exist for these reboots to occur is unknown and further testing and research would nee to be conducted to add more specifics to the new hurdle we are now faced with. What is known is that this new "feature" of some sort has increased the difficulty with forensically preserving digital evidence.*

Matthew Green, a cryptographer and Johns Hopkins professor told *404 Media* that the law enforcement officials' hypothesis about iOS 18 devices is "deeply suspect," but he was impressed with the concept.

"The idea that phones should reboot periodically after an extended period with no network is absolutely brilliant and I'm amazed if indeed Apple did it on purpose," he said.

Update: Apple added an "inactivity reboot" feature in the iOS 18.1 update, but it does not relate to phone/wireless network state.

Note: Due to the political or social nature of the discussion regarding this topic, the discussion thread is located in our Political News forum. All forum members and site visitors are welcome to read and follow the thread, but posting is limited to forum members with at least 100 posts.

22. D-Wave Achieves Significant Milestone with Calibration of 4,400+ Qubit Advantage2 Processor

by Alex Daigle
https://www.dwavesys.com/company/newsroom/press-release/d-wave-achieves-significant-milestone-with-calibration-of-4-400-qubit-advantage2-processor/

D-Wave Quantum Inc., a leader in quantum computing systems, software, and services and the world's first commercial supplier of quantum computers, today announced that it has completed the calibration and benchmarking of a 4,400+ qubit Advantage2™ processor. This milestone marks a significant step forward in

D-Wave's ongoing development of its sixth-generation annealing quantum computing system. The latest Advantage2 processor shows substantial performance gains over the current AdvantageTM system in solving customers' complex computational problems in areas such as optimization, AI, and materials science.

Recent performance benchmarks demonstrate that the 4,400+ qubit Advantage2 processor is computationally more powerful than the current Advantage system, solving a range of problems – including 3D lattice problems common in materials science – 25,000 times faster. The processor also delivers five times better solutions on problems requiring a high degree of precision. Furthermore, it surpasses the current Advantage system in 99% of tests on satisfiability problems, highlighting its capabilities across a wide range of quantum applications.

Compared with the current Advantage system, the 4,400+ qubits Advantage2 processor delivers significant improvements in:

- **Qubit coherence time:** doubled, which drives faster time to solution
- **Energy scale:** increased by 40% to deliver higher-quality solutions
- **Qubit connectivity:** increased from 15 to 20-way connectivity to enable solutions to larger problems

"Our strategic decision to focus development efforts on enhancing the connectivity and coherence of our next annealing quantum computing system has proven successful," said Trevor Lanting, chief development officer at D-Wave. "We're thrilled with the performance of our recently calibrated processor, and we believe this technology will deliver amazing results for our customers, solving bigger and more complex problems."

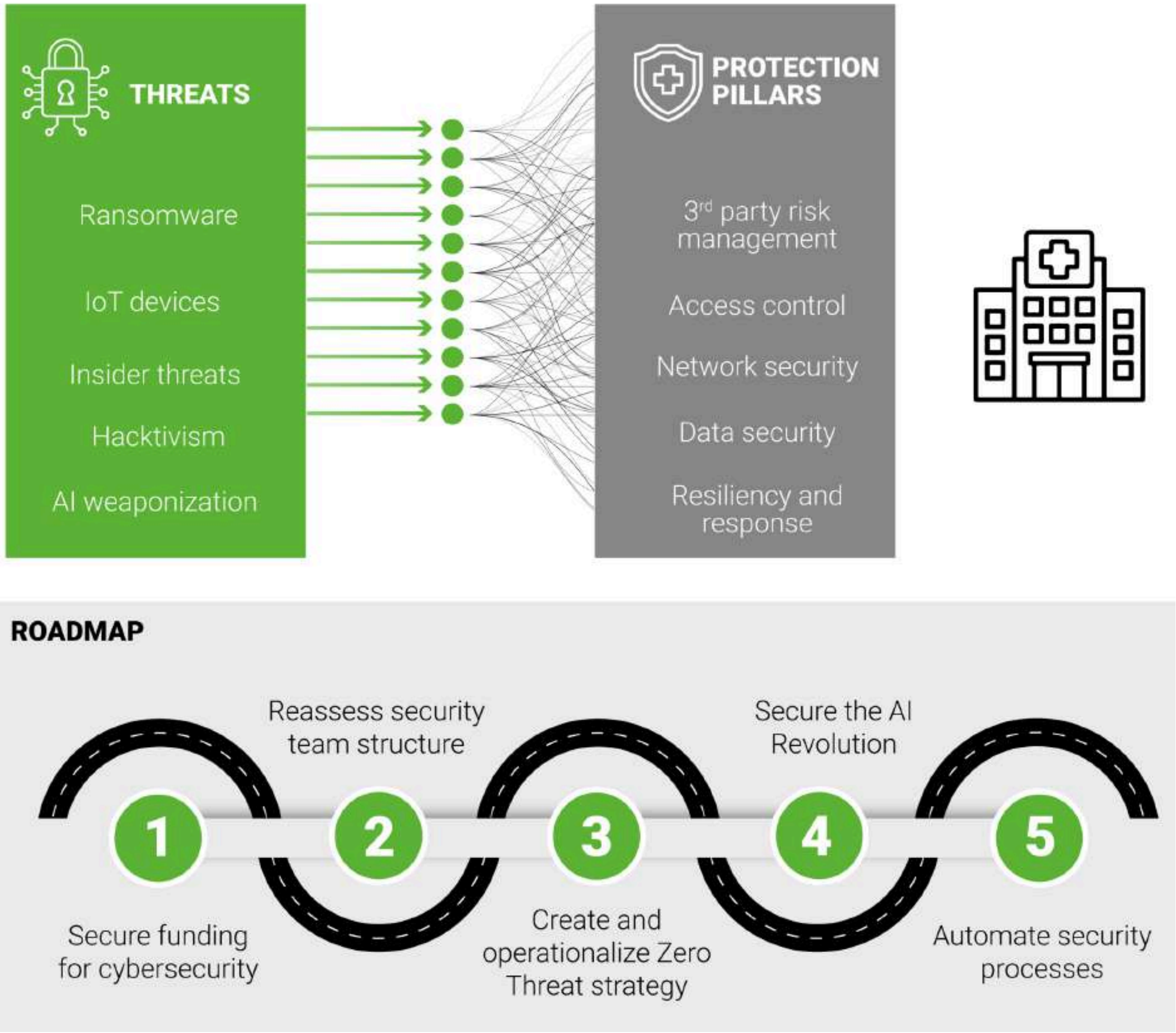
23. From life-saving to life-threatening: The cybersecurity crisis in healthcare

by Megha Kalsi, Arnie Basu, Edward Chua, Jerry Wang
https://www.alixpartners.com/insights/102jnbs/from-life-saving-to-life-threatening-the-cybersecurity-crisis-in-healthcare/

As pernicious attacks increase, the industry faces an imperative to introduce strategies for warding off bad actors

The healthcare industry is a primary target for cybercriminals due to its massive repositories of sensitive patient information and widespread adoption of digital technologies. In 2023, for the 13th year in a row, it experienced the most costly data breaches of any other sector globally, averaging close to $11 million per breach—almost twice as much as the financial industry, according to the World Bank. The impact can be devastating to both patient care operations and the very survival of a hard-hit institution. St. Margaret's Hospital in Spring Valley, Illinois, for example, permanently shut down operations in 2023, in part due to a cyberattack that took place in 2021.

At the same time, industry executives often fail to take consistent, aggressive steps to address these threats when other priorities take over. But the magnitude of the problem calls for a comprehensive, sophisticated effort to guard against the most prevalent and consequential threats they might face. Each successive breach of a healthcare institution only further underscores the need to focus on cybersecurity controls to safeguard patient care operations and protect and preserve business value.



While healthcare companies face a plethora of cyberthreats, there are five particularly prevalent and destructive examples of note.

1. Ransomware

A type of malware, ransomware permanently shuts down access to a victim's data unless a ransom is paid. So far this year, 91% of healthcare data breaches have involved ransomware. What's more, threat actors continue to adapt to the changing technical landscape with new tools, techniques, and procedures (TTPs), the processes and actions used to develop threats and engage in cyberattacks.

Noteworthy ransomware attacks in 2024 included:

- A ransomware attack in February on healthcare technology company Change Healthcare exposed the information of more than one-third of all Americans, rendering the platform unavailable for over a month and impacting payments and revenue lifecycle.
- An April ransomware event by the group LockBit3.0 targeted the Simone Veil Hospital in Cannes. This event resulted in the theft of 61GB of data.
- One month later, a file download triggered a ransomware attack on faith-based healthcare organization Ascension. Its electronic medical record system was affected for one month.

There are a few areas of controls to reduce ransomware risks, including a ransomware assessment and incident response plan, performing purple team exercises, continuing backup resilience, and implementing Zero Trust principles and furthering microsegmentation.

2. IoT and cloud devices

As organizations continue to shift their operations to the cloud, they've become more vulnerable to the exploitation of that technology by bad actors. That's especially true for opportunities created by Internet of Things (IoT) systems. These interconnected devices, which use multiple sensors, offer healthcare institutions additional metrics, analytics, and reporting, but they also create device security considerations. An exposed Internet port, for example, or a misconfiguration on an external server or IoT device, may provide an avenue of entry for a persistent threat actor. In 2023, a report showed a 400% increase in malware IoT attacks, demonstrating the need for continued focus on IoT security.

To protect themselves, organizations must review asset management capabilities to ensure asset protection, automated discovery of assets, reconciliation, and periodic review and assessment of configurations. These will help an organization understand assets living within the environment, protection capabilities surrounding these assets, and whether further protection is needed.

3. Insider threat

Employees and contractors operating within a healthcare organization who have access to sensitive IP and protected health information (PHI) data may be able to exfiltrate the data or otherwise cause intentional or unintentional harm to the institution’s assets. Such attacks can potentially impact patient care and result in reputational and HIPAA compliance risks to an organization. These threats have increased 7.9% year-over-year, with the average cost of insider risk at $16.2 million, according to a 2023 Ponemon report.

Employee monitoring, awareness training, data security, and regular background checks serve as controls to protect from threats and provide insights into user behavior, as well as the potential risk level of particular employees.

4. Hacktivism

This involves a cyberattack on a particular entity or sector by a group of individuals aiming to spread a political message, usually in times of conflict. For example, in January 2023, a pro-Russian hacktivist group named Killnet targeted 14 U.S. healthcare organizations with distributed denial of service (DDoS) attacks, which disrupt a website or server by flooding it with excessive traffic, after officials sent additional military aid to Ukraine.

In October 2023, in response to the rise of hacktivism in recent years, the European Union Agency for Cybersecurity (ENISA) reported a set of recommended actions to counter the increase in DDoS attacks against the healthcare industry, such as a redundant backup strategy, scanning and addressing vulnerabilities, and improvement of detections. Additionally, AlixPartners would recommend a “well-architected" infrastructure review that focuses on core infrastructure pillars to ensure continued resilience against common and emerging threats.

5. Weaponization of AI

When AI is used alongside another threat vector, it may be weaponized to increase the success rate of an attack. For example, bad actors can ask Generative AI to ingest the writing style of a particular public-facing company spokesperson and then craft an email to send to a target. Such instances of business email compromise increased 46% from 2022 to 2023, according to a report by Ponemon Sullivan. Generative AI may also be used to spread misinformation or disinformation by, for instance, producing articles and deepfake videos on controversial medical topics.

Without tools or training to help internal users and the general population learn how to defend themselves against these attacks, they may fall victim to them. Cybersecurity teams should perform regular tests to understand the organization’s ability to identify and respond to such attacks, and consider focusing on higher-risk group areas that may be more susceptible to these threats, including executive leadership and administrators. This may include deployment of tools that report to the user a warning of potential malicious AI usage, and a reporting mechanism for further validation.

An urgent need to plan ahead

As cyberattacks increase, healthcare organizations face an urgent imperative: to consider these vulnerabilities as part of a cybersecurity strategy and create a plan for the upcoming year to reduce risks from persisting threats. To quickly address this need, healthcare organizations must focus on implementing or enhancing core Cybersecurity program pillars, such as data security, resiliency and response, access control, network security, third-party risk management, and regulatory and compliance.

AlixPartners has a playbook to develop a bespoke solution that addresses healthcare cybersecurity needs, bringing in inputs from environment, process, and manpower, and tailoring an output focused directly on high impact quick wins as part of a go-forward strategy. Organizations may begin by ensuring assets and data are accounted for, then stepping through controls against a common healthcare cybersecurity framework like HITRUST to ensure compliance with controls. A focus on rapid risk reduction and addressing the impact of these threats can help organizations continue to provide quality patient care, meet and preserve their business objectives, regulatory and compliance goals, along with optimization and value creation efforts.

24. A Long Goodbye to RSA and ECDSA, and Quick Hello to SLH-DSA

by Prof Bill Buchanan OBE FRSE
https://medium.com/asecuritysite-when-bob-met-alice/a-long-goodbye-to-rsa-and-ecdsa-and-quick-hello-to-slh-dsa-3e53e36a941b

There are two NIST-approved PQC (Post Quantum Cryptography) alternatives for digital signatures. One uses the “darling” lattice method (Dilithium), and the other uses good old hash-based signatures (SPHINCS+). Some, though, worry that the Learning With Error (LWE) approach of lattice methods might be cracked at some time in the future, and so NIST wants alternatives, and one of the most robust from a security point-of-view is hash-based signatures. So let’s meet the might SLH-DSA (aka SPHINCS+) method.

Introduction

Well, as if cybersecurity doesn’t have enough acronyms. There’s RIP, OSPF, TCP, IP, SSH, AES, and so many others. Now, there are three really important ones to remember: ML-KEM (Module Lattice-Based Key Encapsulation Mechanism), ML-DSA (Module Lattice-Based Signature Standard) and SLH-DSA (Stateless Hash-based Digital Signature Standard). ML-KEM is defined in the FIPS 203 standard, ML-DSA is FIPS 204, and for SLH-DSA, we have FIPS 205.

Many, though, would recognise ML-KEM as CRYSTALS-Kyber, ML-DSA as CRYSTALS Dilithium and SLH-DSA as the SPHINCS+ method. And, so, on the 13th of August 2024, FIPS 204 was born, on the same day, NIST published FIPS 205, and also FIPS 203.

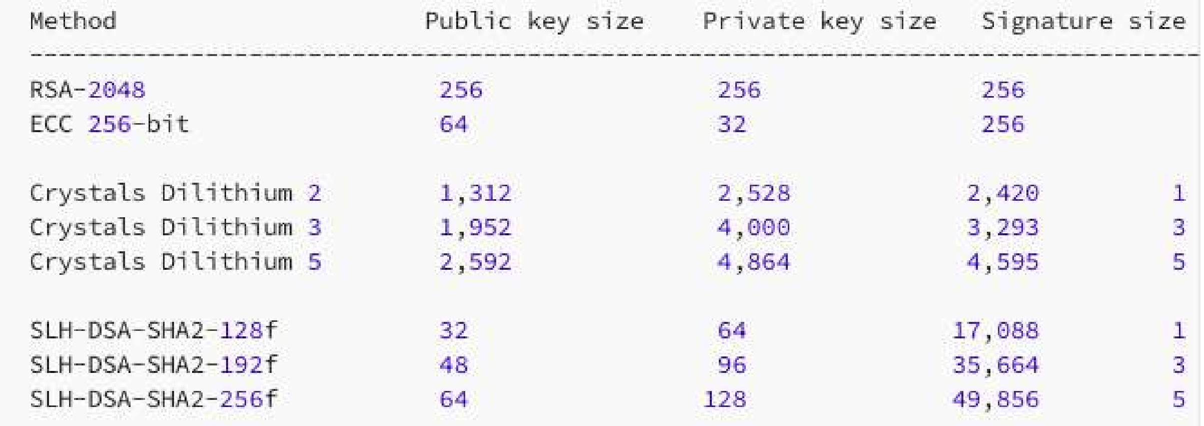
At present, there is only one replacement for our key exchange methods: ML-KEM, and two replacements for digital signatures (e.g., RSA, ECDSA and EdDSA): ML-DSA and SLH-DSA. Both ML-KEM and ML-DSA are lattice-based, while SLH-DSA uses a hash-based signature approach, which is stateless.

SLH-DSA

With this, we have a number of private keys, and which can then be hashed within a Merkle Tree to produce a root public key signature. The problem with this method is that we cannot reuse one of our private keys, as we have shown the path it takes to get to the root public key. For this, SPHINCS+ converts the method into a stateless method, and uses trees of hashes.

SPHINCS+ was one of the winners in the NIST standard for PQC (Post Quantum Cryptography), was proposed by Bernstein et al. in 2015 and updated in 2019. SPHINCS+ 256 128-bit has a public key size of 32 bytes, a private key size of 64 bytes, and a signature of 17KB. It has now been standardized by NIST as FIPS 205, and can be used with SHA-256 or SHAKE-256. These include SLH-DSA-SHAKE-128f and SLH-DSA-SHA2–128f.

The following provides an analysis of the PCQ methods for digital signing:



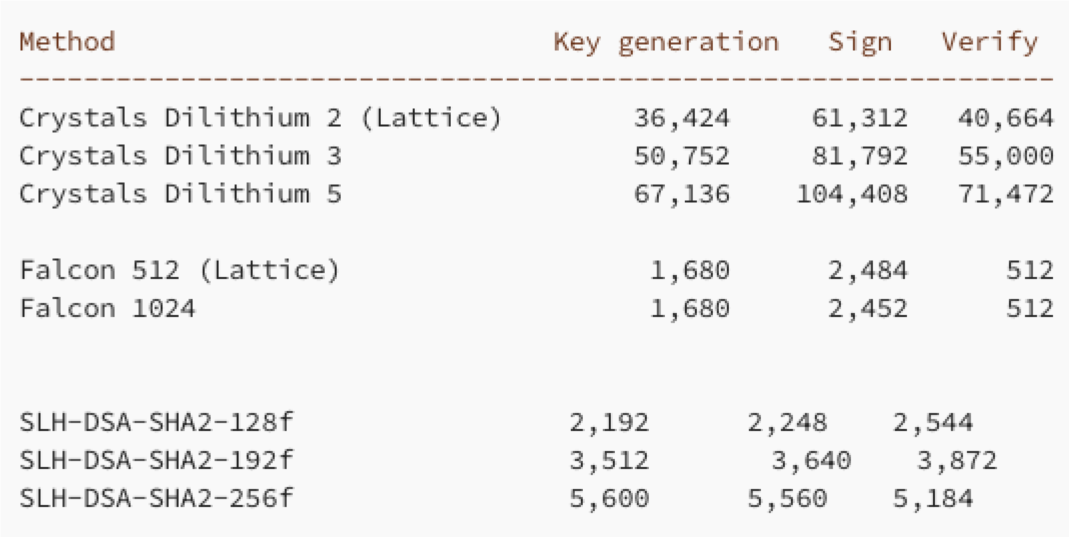
```
Method                     Public key size    Private key size   Signature size
--------------------------------------------------------------------------------
RSA-2048                    256                256                256
ECC 256-bit                 64                 32                 256

Crystals Dilithium 2        1,312              2,528            2,420          1
Crystals Dilithium 3        1,952              4,000            3,293          3
Crystals Dilithium 5        2,592              4,864            4,595          5

SLH-DSA-SHA2-128f           32                 64              17,088          1
SLH-DSA-SHA2-192f           48                 96              35,664          3
SLH-DSA-SHA2-256f           64                128              49,856          5
```

We can see that the public and private key are small, with only 32 bytes for the public key and 64 bytes for the private key for SLH-DSA-SHA2–128f. This is much smaller than Dilithium (ML-DSA-512). But the digital signature is larger, with 17,088 bytes against 2,420 for the equivalent Dilithium signature.

For stack memory size on an ARM Cortex-M4 device and measured in bytes:

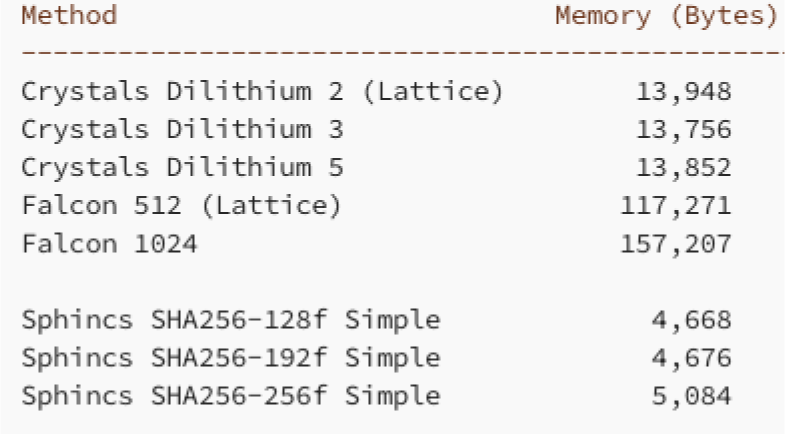


```
Method                              Key generation   Sign   Verify
----------------------------------------------------------------
Crystals Dilithium 2 (Lattice)          36,424     61,312   40,664
Crystals Dilithium 3                    50,752     81,792   55,000
Crystals Dilithium 5                    67,136    104,408   71,472

Falcon 512 (Lattice)                     1,680      2,484      512
Falcon 1024                              1,680      2,452      512


SLH-DSA-SHA2-128f                  2,192      2,248    2,544
SLH-DSA-SHA2-192f                  3,512        3,640    3,872
SLH-DSA-SHA2-256f                  5,600      5,560    5,184
```

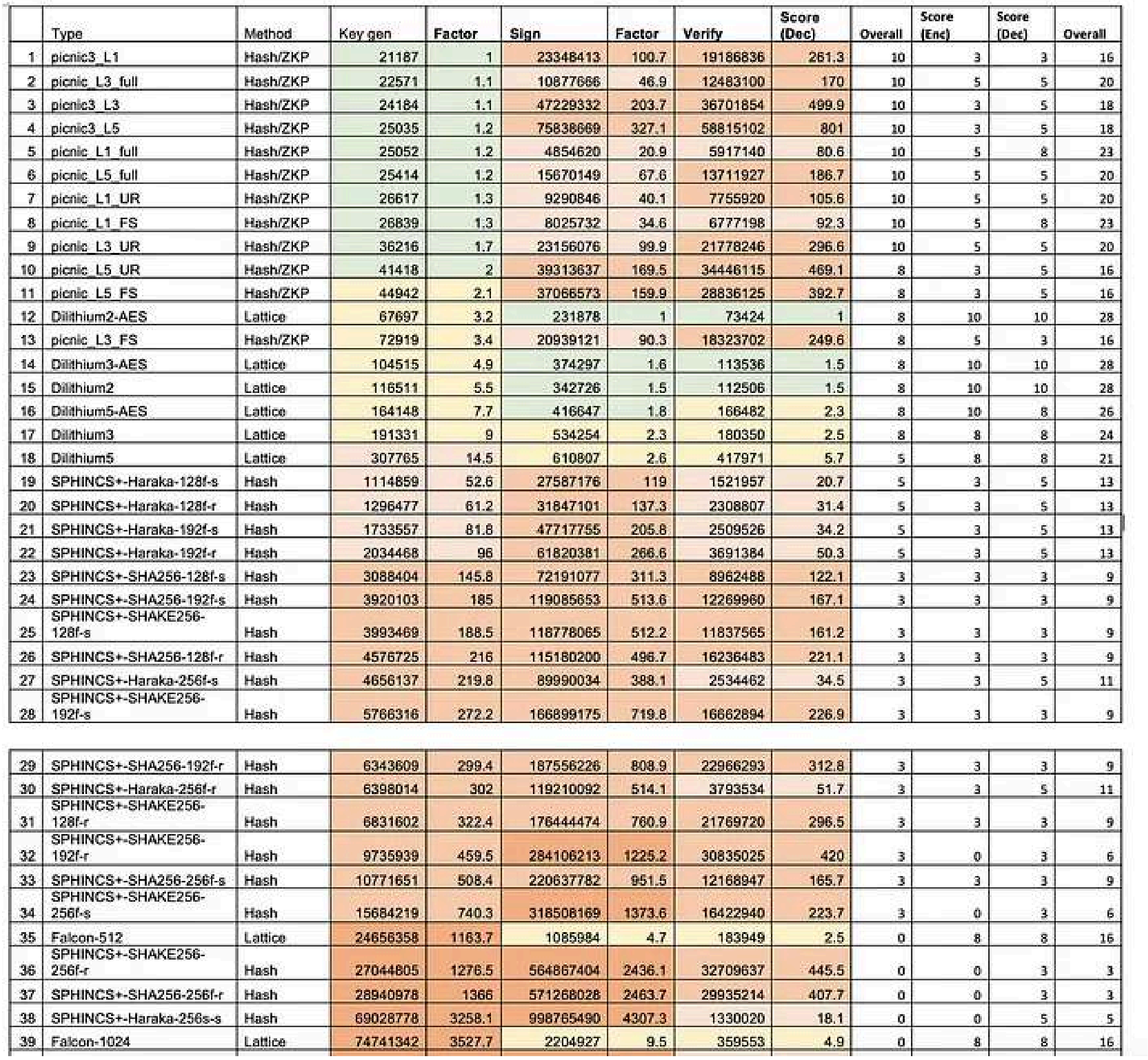
For code size on an ARM Cortex-M4 device [1] and measured in bytes. Note, no Rainbow assessment has been performed in [1], so LUOV (an Oil-and-Vinegar method) has been used to give an indication of performance levels:



```
Method                             Memory (Bytes)
-----------------------------------------------
Crystals Dilithium 2 (Lattice)          13,948
Crystals Dilithium 3                    13,756
Crystals Dilithium 5                    13,852
Falcon 512 (Lattice)                   117,271
Falcon 1024                            157,207

Sphincs SHA256-128f Simple               4,668
Sphincs SHA256-192f Simple               4,676
Sphincs SHA256-256f Simple               5,084
```

For performance, it is much slower than ML-DSA (Dilithium) for key generation, signing and verification



	Type	Method	Key gen	Factor	Sign	Factor	Verify	Score (Dec)	Overall	Score (Enc)	Score (Dec)	Overall
1	picnic3_L1	Hash/ZKP	21187	1	23348413	100.7	19186836	261.3	10	3	3	16
2	picnic_L3_full	Hash/ZKP	22571	1.1	10877666	46.9	12483100	170	10	5	5	20
3	picnic3_L3	Hash/ZKP	24184	1.1	47229332	203.7	36701854	499.9	10	3	5	18
4	picnic3_L5	Hash/ZKP	25035	1.2	75838669	327.1	58815102	801	10	3	5	18
5	picnic_L1_full	Hash/ZKP	25052	1.2	4854620	20.9	5917140	80.6	10	5	8	23
6	picnic_L5_full	Hash/ZKP	25414	1.2	15670149	67.6	13711927	186.7	10	5	5	20
7	picnic_L1_UR	Hash/ZKP	26617	1.3	9290846	40.1	7755920	105.6	10	5	5	20
8	picnic_L1_FS	Hash/ZKP	26839	1.3	8025732	34.6	6777198	92.3	10	5	8	23
9	picnic_L3_UR	Hash/ZKP	36216	1.7	23156076	99.9	21778246	296.6	10	5	5	20
10	picnic_L5_UR	Hash/ZKP	41418	2	39313637	169.5	34446115	469.1	8	3	5	16
11	picnic_L5_FS	Hash/ZKP	44942	2.1	37066573	159.9	28836125	392.7	8	3	5	16
12	Dilithium2-AES	Lattice	67697	3.2	231878	1	73424	1	8	10	10	28
13	picnic_L3_FS	Hash/ZKP	72919	3.4	20939121	90.3	18323702	249.6	8	5	3	16
14	Dilithium3-AES	Lattice	104515	4.9	374297	1.6	113536	1.5	8	10	10	28
15	Dilithium2	Lattice	116511	5.5	342726	1.5	112506	1.5	8	10	10	28
16	Dilithium5-AES	Lattice	164148	7.7	416647	1.8	166482	2.3	8	10	8	26
17	Dilithium3	Lattice	191331	9	534254	2.3	180350	2.5	8	8	8	24
18	Dilithium5	Lattice	307765	14.5	610807	2.6	417971	5.7	5	8	8	21
19	SPHINCS+-Haraka-128f-s	Hash	1114859	52.6	27587176	119	1521957	20.7	5	3	5	13
20	SPHINCS+-Haraka-128f-r	Hash	1296477	61.2	31847101	137.3	2308807	31.4	5	3	5	13
21	SPHINCS+-Haraka-192f-s	Hash	1733557	81.8	47717755	205.8	2509526	34.2	5	3	5	13
22	SPHINCS+-Haraka-192f-r	Hash	2034468	96	61820381	266.6	3691384	50.3	5	3	5	13
23	SPHINCS+-SHA256-128f-s	Hash	3088404	145.8	72191077	311.3	8962488	122.1	3	3	3	9
24	SPHINCS+-SHA256-192f-s	Hash	3920103	185	119085653	513.6	12269960	167.1	3	3	3	9
25	SPHINCS+-SHAKE256-128f-s	Hash	3993469	188.5	118778065	512.2	11837565	161.2	3	3	3	9
26	SPHINCS+-SHA256-128f-r	Hash	4576725	216	115180200	496.7	16236483	221.1	3	3	3	9
27	SPHINCS+-Haraka-256f-s	Hash	4656137	219.8	89990034	388.1	2534462	34.5	3	3	5	11
28	SPHINCS+-SHAKE256-192f-s	Hash	5766316	272.2	166899175	719.8	16662894	226.9	3	3	3	9
29	SPHINCS+-SHA256-192f-r	Hash	6343609	299.4	187556226	808.9	22966293	312.8	3	3	3	9
30	SPHINCS+-Haraka-256f-r	Hash	6398014	302	119210092	514.1	3793534	51.7	3	3	5	11
31	SPHINCS+-SHAKE256-128f-r	Hash	6831602	322.4	176444474	760.9	21769720	296.5	3	3	3	9
32	SPHINCS+-SHAKE256-192f-r	Hash	9735939	459.5	284106213	1225.2	30835025	420	3	0	3	6
33	SPHINCS+-SHA256-256f-s	Hash	10771651	508.4	220637782	951.5	12168947	165.7	3	3	3	9
34	SPHINCS+-SHAKE256-256f-s	Hash	15684219	740.3	318508169	1373.6	16422940	223.7	3	0	3	6
35	Falcon-512	Lattice	24656358	1163.7	1085984	4.7	183949	2.5	0	8	8	16
36	SPHINCS+-SHAKE256-256f-r	Hash	27044805	1276.5	564867404	2436.1	32709637	445.5	0	0	3	3
37	SPHINCS+-SHA256-256f-r	Hash	28940978	1366	571268028	2463.7	29935214	407.7	0	0	3	3
38	SPHINCS+-Haraka-256s-s	Hash	69028778	3258.1	998765490	4307.3	1330020	18.1	0	0	5	5
39	Falcon-1024	Lattice	74741342	3527.7	2204927	9.5	359553	4.9	0	8	8	16

Overall, the Haraka hashing method is the fastest but has not been approved as a FIPS standard. The two main standards use the NIST-approved hashes of SHA2 and SHAKE. Overall, there are two main methods for signing: a "pure" version (slh_sign) and a "pre-hash" version (hash_slh_sign). With the pre-hash version, we hash the message before it is sent for signature. This means that there is less data to deal with for the signature and can thus reduce the computational load on the signing application.

Conclusions

SLH-DSA is a solid signature and has small keys, but the signature is larger than RSA, ECDSA and ML-DSA. It also has rock-solid security proofs, which is not quite the case for RSA, ECDSA and ML-DSA. So, as an alternative to ML-DSA, it's a great method. A little slow in places but highly secure.

25. Every Cybersecurity List Should Be a Risk-Ranked List

by Roger Grimes

https://www.linkedin.com/pulse/every-cybersecurity-list-should-risk-ranked-roger-grimes-ippze/

Cybersecurity is all about risk management and reduction. You cannot get rid of all risk. Well, I guess you could, but you (and everyone else) would probably not want to work in a true zero-risk environment. It would be too locked down, super slow, and incredibly inflexible. Cybersecurity is all about identifying the most likely and impactful risks and reducing them first and best.

To repeat again, cybersecurity is about risk management. Identify the biggest risks and mitigate those the best you can. That is your job.

Unfortunately, most of the industry and most defenders really do not do it well. There are thousands of threats and hundreds of shiny objects that distract most cyber defenders away from directly focusing on the most important risks. We are distracted and focusing on less risky things while not focusing on the right, more likely, more damaging risks. It is literally the number one reason why hackers and their malware creations are so continually successful over the decades.

I do not blame most defenders. We are tasked with protecting all the valuable digital data, but our industry almost never uses or talks about our own industry's data to drive what we should be focusing on first and best. I know, it is ironic.

Part of the problem is that we are constantly handed lists – list of required controls – list of things we are being asked to fix or improve – lists of new projects – lists of threats, and so on, that are not ranked for risks. For example, we are often given a cybersecurity guideline (e.g., PCI-DSS, HIPAA, SOX, NIST, etc.) with hundreds of recommendations. They are all great recommendations, which if followed, will reduce risk in your environment.

What they do not tell you is which of the recommended things will have the most impact on best reducing risk in your environment. They do not tell you that one, two or three of these things – among the hundreds that have been given to you, will reduce more risk than all the others.

More often we are told we need to do all the hundreds of things well at once. And no one can do more than a few things very well at once. And so, defenders are very likely to concentrate on things that will not impact risk while at the same time, not focusing as much on things that matter more. It is bound to happen. The list of controls is not risk-ranked. And any time anyone is concentrating more on a less risk-reducing control means you are being less efficient at reducing risk than you otherwise could.

The solution?

Here is one big one: Do not use or rely on un-risk-ranked lists. Require any list of controls, threats, defenses, solutions to be risk-ranked according to how much actual risk they will reduce in the current environment if implemented.

This is easy to say and harder to do.

But any time you see an un-ranked list of cybersecurity things, risk-rank it as the first step, before you start to consider which ones you will rely on. Everything else is inefficient.

It does not help that nearly every "official" cybersecurity document with recommendations or requirements is ALWAYS un-ranked. All the recommendations, good at reducing risk or not so good, are co-mingled together, often randomly, or in ways that defy explanation.

Here is a recent example: CISA's Proposed Security Requirements for Restricted Transactions

I am a huge fan of the Cybersecurity Infrastructure Security Agency (CISA). I am a huge fan of Director Easterly and her staff. I think they have the best U.S. government agency dedicated to fighting hackers and malware ever! But I am a bit of an editor on their published documents. Specifically, that CISA documents are often full of un-ranked recommendations (and sometimes missing some critical ones).

This specific CISA document has at least 21 main recommendations, many of which lead to two or more other more specific recommendations. Overall, it has several dozen recommendations, each of which individually will likely take weeks to months to fulfill in any environment if not already accomplished. Any person following this document is...rightly – going to be expected to evaluate and implement all those recommendations. And doing so will absolutely reduce risk.

The catch is: There are two recommendations that WILL DO MORE THAN ALL THE REST ADDED TOGETHER TO REDUCE CYBERSECURITY RISK most efficiently: patching and using multifactor authentication (MFA). Patching is listed third. MFA is listed eighth. And there is nothing to indicate their ability to significantly reduce cybersecurity risk as compared to the other recommendations. Two of these things are not like the others, but how is anyone reading the document supposed to know that patching and using MFA really matter more than all the rest?

And I am ignoring that the biggest possible risk reducer...that of giving aggressive security awareness training to your employees which is better at reducing risk than any of them added up all together – is not even mentioned. But I do not want to get off topic.

And this is a huge problem that does not get enough focus.

If someone is breaking into your house over and over, using the windows, what good is putting more locks on your door going to do? But imagine that thieves are breaking in through your windows and the people gave 20 things to do, only one of which it was to better secure your windows, and that recommendation was co-mingled in the middle with all the rest. How likely would a homeowner be to look at the list of 20 things and figure out that one of the things in the middle would solve their problems and all the other things in front and around it would not matter at all?

Well, that is how we often practice IT security. We make lots of recommendations – hundreds of recommendations, but we usually do not pick out the ones that mean more than all the others. We certainly do not highlight them.

And so, we end up teaching ourselves to work in a distracted manner trying to implement a ton of things that really will not matter that much while often neglecting the things that will matter. It is not that we neglect them completely or ignore them – it is just that they are added into the dozens to hundreds of things as if they have the same importance. And they do not.

If you want to become a superior computer security professional, stop creating or accepting lists of un-ranked things. When you create a list of things that require action of some sort, rank them. If you create a list of controls, risk-rank them. If you create a list of things that need to be fixed, risk-rank them. If someone hands you a list of un-ranked things, hand it back and tell them to risk-rank them…or rank them yourself before performing.

Running off to do a bunch of things before you risk-rank them just is not very efficient. If your objective is to best reduce risk as efficiently as you can, risk-rank everything that should be risk-ranked. Stop accepting un-risk-ranked lists. Become known as the person in your company that does not accept un-risk-ranked lists. If you do it, more people in your organization will do it. And you can build a great career solely on being a person that does that – because most practitioners do not.