

Security in the quantum computing era

The risk is real, the need is now

Experts on this topic



Ray Harishankar

IBM Fellow, IBM Quantum
[linkedin.com/in/rayharishankar/](https://www.linkedin.com/in/rayharishankar/)
harishan@us.ibm.com

Ray Harishankar is responsible for leading the business and technical strategies for quantum-safe technology, advocating IBM capabilities and leadership to clients and driving the evaluation and definition of the required technical assets and tooling for success. With his extensive client experience, Ray focuses on leveraging IBM's deep technical expertise in broader security services and post-quantum cryptography, and pragmatically applying it to benefit clients.

Dr. Sridhar Muppidi

IBM Fellow, VP, and CTO, IBM Security
[linkedin.com/in/smuppidi/](https://www.linkedin.com/in/smuppidi/)
muppidi@us.ibm.com

Dr. Sridhar Muppidi is responsible for driving the technical strategy, architecture, and research for the IBM Security portfolio of products and services that help clients manage defenses against threats and protect digital assets. He is a results-oriented technical thought leader with 25 years of experience in building security products, delivering solution architecture for clients, driving open standards, and leading technical teams.

Michael Osborne

CTO, IBM Quantum
[linkedin.com/in/michael-osborne-QSafe](https://www.linkedin.com/in/michael-osborne-QSafe)
osb@zurich.ibm.com

In addition to his global role as CTO for quantum-safe technology, Michael Osborne also leads the security and privacy activities at the IBM Research center in Rüschlikon (Zurich), Switzerland. His current focus includes advancing new generations of advanced cryptography and leading IBM's quantum-safe cryptography. This includes efforts to develop and standardize quantum-resistant technology and transferring this technology to IBM products and services.

Dr. Walid Rjaibi

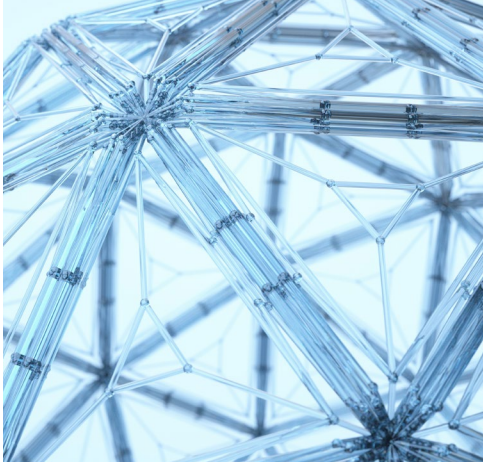
Distinguished Engineer, CTO,
Data Security, IBM
[linkedin.com/in/walid-rjaibi-phd-cissp-8325077/](https://www.linkedin.com/in/walid-rjaibi-phd-cissp-8325077/)
wrjaibi@ca.ibm.com

Dr. Walid Rjaibi drives the research for data security as well as the technical architecture and vision for products and services. Prior to his current position, Walid held several technical and management roles within IBM, including Research Staff Member at the IBM Zurich Research Lab, Security Architect for DB2, Development Manager, and Chief Security Architect for Data and AI. His data security work resulted in 27 granted patents, publications in leading scientific journals, and industry-proven commercial capabilities that are relied upon by thousands of organizations globally to protect critical data and meet security and compliance mandates.

Dr. Joachim Schaefer

Technical Delivery Lead, IBM Quantum
[linkedin.com/in/joschaefer/](https://www.linkedin.com/in/joschaefer/)
JSchaefer@be.ibm.com

Dr. Joachim Schaefer delivers solutions that help clients understand quantum threats, prioritize mitigation actions, and execute long-term crypto-transformation programs. He has broad experience delivering security solutions for the financial services industry and the telecommunications sector. Joachim holds a Ph.D. in Quantum Communication and is passionate about all topics surrounding quantum technologies.



Quantum computing will profoundly alter how we think of computing and, critically, how we secure our digital economy through encryption.

Key takeaways

- The quantum computing era will unfold over time, but the need for quantum-safe cryptographic solutions is *immediate*.

Developing these “quantum-safe” capabilities is crucial to maintaining data security and integrity for critical applications and infrastructure.

- Help is on the way.

In an initial round of evaluations, the US government’s National Institute of Standards and Technology (NIST) has initially narrowed quantum-safe cryptographic algorithms from 82 submissions down to four finalists. Three of these four finalists were created by IBM in collaboration with industry and academic partners. Four alternate candidates are progressing to additional evaluation.

- Infusing crypto-agility into systems as they’re modernized is more than a CISO-driven initiative.

It’s an ambitious albeit necessary strategy shaped by leaders across the organization and partners outside the organization, including vendors, industry peers, customers and consumers, and standards bodies such as NIST.

A pivotal moment for the digital economy

Quantum computing is evolving from the fantastical to the feasible. Accelerated developments show promise for solving previously intractable problems in materials science, machine learning, optimization, and much more. The potential benefits for business are immense, and the social implications of quantum technologies are likely to be far-reaching.¹ By decade's end, practical quantum computing solutions could impact computing strategies across industries.

Widespread data encryption mechanisms, such as public-key cryptography (PKC), could become vulnerable.

What does this mean for business leaders? Over upcoming investment cycles, quantum computing will profoundly alter how we think of computing and, critically, how we secure our digital economy through cryptography.

Developing “quantum-safe” cryptography capabilities is crucial to maintaining data security and integrity for critical applications. *The quantum era will unfold over time, but the need for quantum-safe solutions is immediate.* Business, technology, and security leaders face an urgent need to develop a quantum-safe strategy and roadmap now. In fact, both the historic and current complexity of cryptography migrations—even pre-quantum computing—can require several years of strategic planning, remediation, and transformation.²

Conquering a cryptography crisis

While issues such as data encryption and operational disruption have long troubled Chief Information Security Officers (CISOs), the threat posed by emerging quantum computing capabilities is far more profound. Indeed, quantum computing poses an existential risk to the classical encryption protocols that enable virtually all digital transactions.

Over the next several years, widespread data encryption mechanisms, such as public-key cryptography (PKC), could become vulnerable. In fact, any classically encrypted communication that could be wiretapped is at risk, and potentially already subject to exfiltration, with the intention of harvesting that data once quantum decryption solutions are viable. These tactics are referred to as “harvest now, decrypt later” attacks.

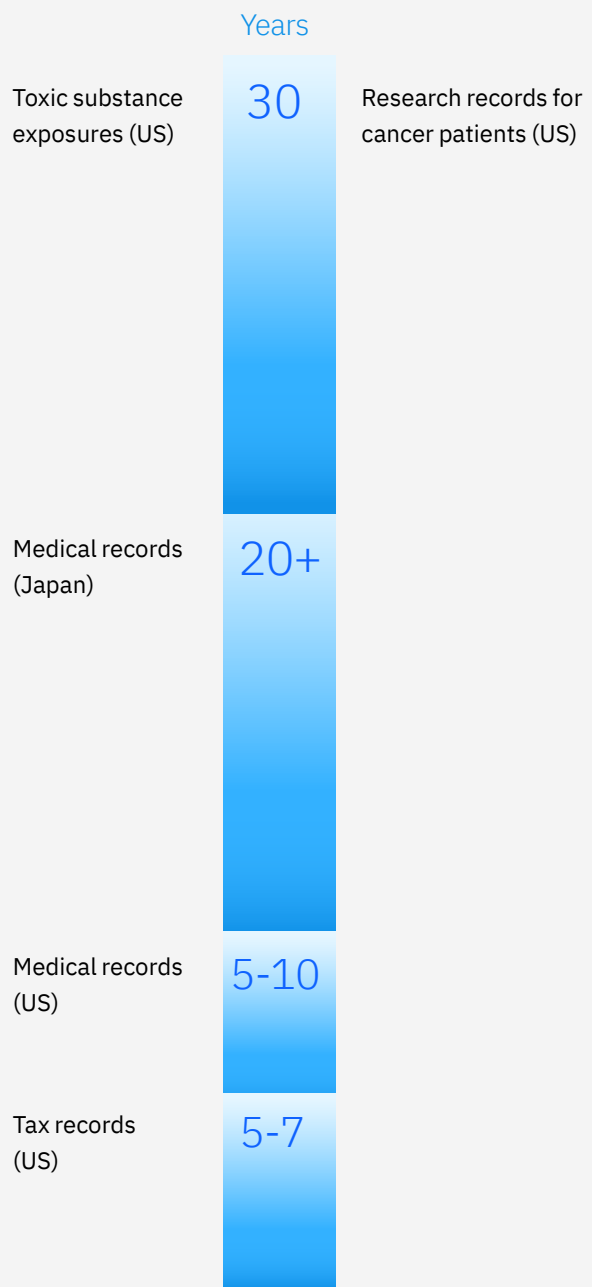
As such, ensuring that data encryption remains secure requires our urgent attention—even before quantum computing solutions become generally available. Even if some data is irrelevant or quickly loses its value to hackers, data related to national security, infrastructure, medical records, intellectual capital, and more could well retain or increase in value over time.³ (See Figure 1.) As an executive at one European bank told us, “We want to keep our data forever confidential.”⁴

And while the simple exposure of data is threat enough, risk scenarios escalate from there. We use cryptography to protect communications networks, verify electronic transactions, and secure digital evidence. Today’s smarter automobiles and airplanes rely upon highly connected digital ecosystems, with decades of service life ahead of them. Even critical infrastructure systems, which traditionally have been segregated from digital networks, are increasingly reliant on over-the-air updates and Internet of Things (IoT) field data capture capabilities.⁵

FIGURE 1

Evergreen, ever valuable

Retention requirements for various data types



With the power of quantum computing behind them, adversaries could craft fraudulent identities for websites and create fake software downloads and software updates. Cybercriminals could launch extortion attacks by threatening to disclose harvested data. They could design fake land records or lease documents that are indistinguishable from digitally encrypted originals. Considering that the digital economy is estimated to be worth \$20.8 trillion by 2025,⁶ the repercussions could be staggering.

Make no mistake. The impact is coming—and it's not a question of if, but how soon and how disruptive. But there's hopeful news, too. As we'll explore, researchers are actively developing quantum-safe remediation techniques and algorithms. The ultimate goal? For organizations—and society—to reap the substantial benefits of quantum computing's power, while simultaneously shielding against the same technologies when used by cyber adversaries.

*Make no mistake.
The impact is coming—and it's
not a question of if, but how
soon and how disruptive.*

Securing critical infrastructure

The earliest adopters of quantum-driven cryptography solutions are likely to be sophisticated threat actors (think nation-states) applying quantum computing's potential to crack today's cryptography. For industries operating critical infrastructure, the stakes are high.⁷

In fact, in a May 2022 memo, the US government warned, "When it becomes available, a cryptanalytically relevant quantum computer (CRQC) could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions."⁸ Cybersecurity experts, their business counterparts, and laypeople alike are increasingly on alert.⁹

Consider RSA-2048, a widely used public-key cryptosystem that facilitates secure data transmission. In a 2021 survey, a majority of leading authorities believed that RSA-2048 could be cracked by quantum computers within a mere 24 hours.¹⁰ How soon that might happen is a matter of debate. But the very question of when cryptography will be broken by quantum computing can be misleading, as it implies a specific threshold date that leaders can anticipate. Add the troubling truth that implementing solutions and safeguards can take longer than expected, and technology leaders are recognizing the urgent need to act now. The question: can they convince their line of business peers there is a business benefit in doing so?

Perspective

The science of cryptography meets the practice of encryption

Although the two terms are often used interchangeably, *cryptography* is the science of encrypting and decrypting information, often involving advanced degrees and a theoretical approach. Data confidentiality, data integrity, authentication, and nonrepudiation—core concepts related to information security—are essential to cryptography.¹¹

Encryption is how information is converted into a secret code that obscures its true meaning.¹² In other words, encryption is boots on the ground—one practical way cryptography is used in day-to-day operations, along with decryption and authentication, as two additional examples. Today, most organizations have libraries of encryption/decryption algorithms. From there, those algorithms need to be implemented properly. The same holds true going forward, but the encryption/decryption algorithms need to be more robust and capable of resisting quantum-based exploits. This characteristic is known as being “quantum safe”—and related protocols are designed to address emerging government and regulatory standards.



Crypto-agility: Algorithms to the rescue

A threatening trio

Given our reliance on data encryption, the ramifications for security are profound: 2.5 quintillion bytes of new data are being created every day.¹³ The longer we postpone the migration to quantum-safe standards, the greater the exposure for our exponentially increasing volumes of data. Below, we outline three significant threats (see Figure 2).

The threat to data confidentiality

It's the primary threat we associate with quantum computers: the unauthorized decryption of confidential data in the future. Cybercriminals could target information generated from events, such as critical government or industry gatherings, and locations, such as corporate and government venues, for future decryption. Health data, military intelligence, financial records, and more could land in the crosshairs. These scenarios raise questions about the impact of breaches on encrypted data, as well as the evolution of regulations such as GDPR. Data confidentiality breaches could also impact improperly disposed encrypted storage media, including tapes and disk drives, and the copying of encrypted snapshots and backups.

The threat to authentication protocols and digital governance

In this scenario, a recovered private key, which is derived from a public key, can be used through remote control to fraudulently authenticate a critical system. Examples of these systems could include a utility grid or blockchain-dependent financial transactions. Hackers could initiate malicious transactions on long-term blockchains or distributed ledgers.

This escalates concerns related to the design of systems with long life cycles—for example, cars, transport infrastructure, core banking applications, and blockchain applications.

The threat to data integrity

Cybercriminals could use quantum computing technology to recover/decrypt private keys—and from there, create or manipulate digital documents and their digital signatures. This might include audit records; legal documents; attestations of assurance, originality, or provenance; and, more generally, any sensitive communications that rely upon encrypted messaging.

From a legal perspective, schemes could include tampering with digital evidence—for example, creating or manipulating digitally signed documents that have some legal value. Or a future quantum adversary could create a signed document proving ownership with a backdated transaction date. This type of threat poses perplexing questions on the future trustworthiness of digital transactions executed today. In years to come, it may be necessary to distinguish between real and fraudulent documents that both have valid signatures.

FIGURE 2

The keys to the digital realm

Common examples of how cryptography is used in practice*



Data confidentiality

Use combination of private-public keys to agree on a secret key, which is then used for data encryption and decryption.



Identification/authentication

Validate the identity of a user or a machine by using a digital certificate, which contains the public key signed by a trusted authority.



Data integrity

Sender signs data with a private key and receiver verifies the integrity of the data with sender's public key.

A public key is a cryptographic key that can be used by anyone to encrypt data intended for a specific recipient. The encrypted messages can only be decrypted by using the corresponding **private key**, which is unique to that specific recipient.

*The above examples are not definitions but rather a selection of specific use cases, and not intended as an exhaustive list of how these concepts may be applied.

A quantum leap: From threats to opportunities

Organizations looking to migrate applications to the cloud and/or modernize applications on the cloud need to plan for quantum-safe cryptography and crypto-agility.

Yes, the advent of quantum computing poses threats to cybersecurity.

But it's not a time to simply rip and replace existing cryptography. It's a time to regroup, reassess, and revamp. To meet the challenges posed by quantum-safe cryptography, a calculated response is called for.

Quantum-safe roadmaps must address two different needs. First, they need to reinforce digital transformation initiatives based on emerging technologies and new ways of doing business. And second, they need to support remediation efforts associated with making existing data assets and services quantum safe. For some perspective, let's further distinguish between these.

According to the *MIT Sloan Management Review*, digital transformation should be embraced as continually adapting to ever-evolving environments.¹⁴ For all organizations, the transition to quantum-safe encryption creates an opportunity to transform by integrating these capabilities in ways that evolve business transactions and relationships.

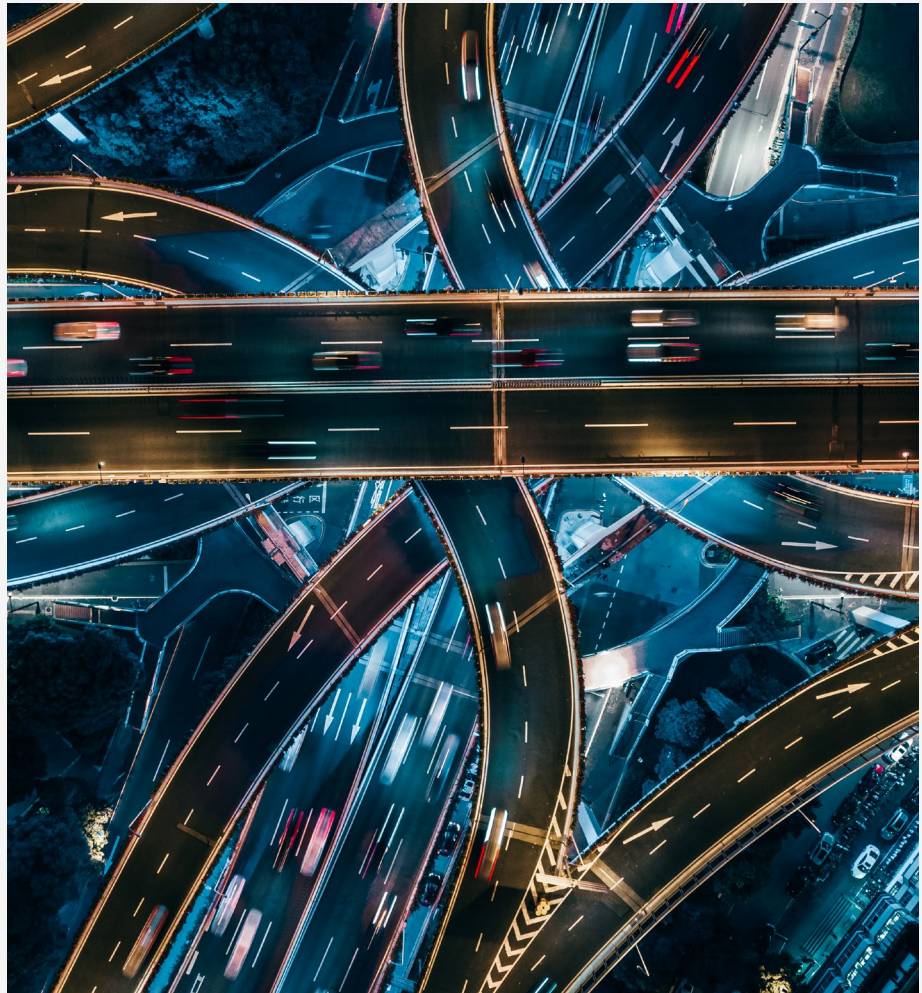
Remediation, on the other hand, is the mitigation of a threat or vulnerability.¹⁵ Current encryption implementations can be remediated to alleviate existing vulnerabilities. For example, crypto-agility can help organizations react faster to cryptographic vulnerabilities and future changes to cryptographic standards. This is essential now—and was essential well before the complexities posed by quantum computing.

Both transformation and remediation are complex, iterative endeavors. Additionally, organizations looking to migrate applications to the cloud and/or modernize applications on the cloud need to plan for quantum-safe cryptography and crypto-agility.

Perspective

What is crypto-agility?

Crypto-agility means just what its name implies. It's a characteristic of a flexible information security system that can pivot to another encryption method without significant disruption. According to the US government's National Institute of Standards and Technology (NIST), maintaining crypto-agility is imperative to preparing for a quantum-safe future.¹⁶



Quantum-safe algorithms within reach: The NIST competition

Concerns related to quantum-safe cryptography are mounting—but they’re not new. Back in December 2016, NIST issued a request for nominations for public-key quantum-safe cryptographic algorithms, kicking off a years-long process of competitive development.¹⁷ Ultimately, NIST received 82 submissions.¹⁸

In July 2022, after extensive evaluation and testing, NIST narrowed its initial selections down to four algorithms (see Figure 3), three of which were created by IBM in collaboration with industry and academic partners. And, in fact, IBM was involved in developing the two primary algorithms to be implemented for most use cases: CRYSTALS-Kyber (key establishment) and CRYSTALS-Dilithium (digital signatures).¹⁹ Four alternate candidates are progressing to additional evaluation.

Both algorithms involve lattice cryptography, which offers substantial advantages, including serving as a building block for ID-based encryption and more.

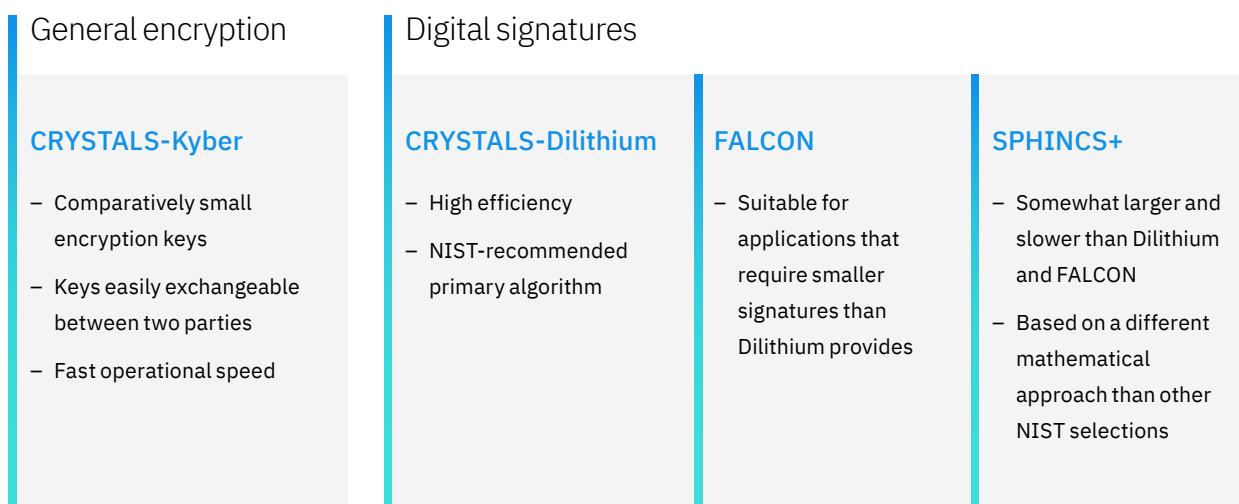
Based on a type of math problem called Learning with Errors (LWE), these algorithms facilitate extremely efficient and fast implementations when compared to RSA encryption. And critically, they can support hybrid cloud and edge use cases. CRYSTALS-Kyber and CRYSTALS-Dilithium also serve as fertile ground for future cryptographic advances. In fact, IBM z16, the industry’s first generally available, quantum-safe high-performance computing solution, uses both algorithms as the underpinnings of its key encapsulation and digital signature capabilities. (See case study, “IBM zSystems: A quantum-safe crypto migration,” on page 11.)

According to the World Economic Forum (WEF), NIST standards are relied upon by most private and public organizations globally. WEF notes, “[These standards] are the basis for today’s secure global communications—be it making a purchase on the web or transferring sensitive data.”²⁰ For additional information, see the IBM report “Transitioning to Quantum-Safe Encryption.”²¹

FIGURE 3

The four NIST finalists*²²

Progressing toward quantum-safe operations



*Four alternate candidates are progressing to additional evaluation.

Case study

IBM zSystems®: Making the migration to quantum safe²³

In 2015, even before IBM put its first quantum computer on the cloud and way before NIST chose its new standards, an IBM cryptographic research team began investigating how to quantum-proof the IBM zSystems platform. By 2018, the cryptographic team expanded its system tests to include NIST's first-round candidates as they were announced. And in the first risk assessment based on its proof of concept and test results, the team collaborated with IBM zSystems to migrate z16 to quantum-safe algorithms.

The first step was to compile a cryptographic inventory of the entire IBM zSystems solution architecture. To do so, the IBM cryptography and IBM zSystems teams developed a questionnaire and sent it to all firmware and product owners. The answers provided the first complete view of cryptographic usage within the IBM zSystems stack, helping to define the critical system components that needed to be updated as part of the migration strategy. The teams also created cryptographic libraries and consulted the development teams on their migration to quantum-safe algorithms.

During this process, the cryptographic team improved the Hardware Security Modules (HSM) to support quantum-safe algorithm capabilities. The HSM provided some quantum-safe cryptographic services, but also the algorithms themselves were accelerated with a dedicated hardware engine that was developed and implemented by the cryptographic team. The new IBM z16™ was launched in April 2022, just weeks before NIST announced the winners of its six-year-long crypto challenge. With IBM z16, companies can build toward a quantum-safe future, today.

The urgency of collaboration and partnership

Infusing crypto-agility into systems as they're modernized and transformed is no small task. It's an ambitious albeit necessary initiative that needs the full support of line of business and senior executives. In effect, it's not simply a CISO-driven initiative, but a strategic outlook shaped by leaders across the organization and partners outside the organization. Partners may include vendors, industry peers, customers and consumers, and standards bodies such as NIST.

Deploying a crypto-agile governance model based on collaboration

Without collaboration around interoperability and standards, quantum-safe bank transactions will simply not be possible.

Governance helps us understand how change should be implemented. Crypto-agility must be responsive to new standards, community guidelines, and design principles that reflect the needs of different industries, organizations, and communities.

Consider that modernization and transformation involve changing the basic building blocks of encryption as well as the numerous standards built on top of those building blocks. Reducing misalignments within any particular industry is a compelling challenge, one that involves understanding its governance, standards, and design principles. That's why many enterprises, working across standards organizations and geographies, collaborate with industry peers, stakeholders, partners, third-party assurance services, and industry regulators to coordinate efforts at a meta level.

For certain industries, these issues literally cannot be solved without collaboration. For example, a large financial services back-end provider works with thousands of banks, all of which need interchangeable bank transactions and consistent governance. Without collaboration around interoperability and standards, quantum-safe bank transactions will simply not be possible.

From our perspective, *financial services* organizations are one of four industries highly incentivized to develop quantum-safe capabilities. For the *government* sector, crypto-agility is a matter of national security, and the US government is leading the way with the NIST competition for quantum-safe algorithms. *Telecommunications* is another frontrunner, with its motivation—and pressure—of being the connective network across all industries. As operators and service providers for critical infrastructure services such as water and power, the *energy and utility* industry rounds out our list.

Because standards and practices are still evolving, the path forward will be discovery-driven. To expedite insights and the development of leading practices, leaders need to understand multiple viewpoints and priorities. Consortiums and standards bodies, ecosystems, and partnerships both across industries and with external service providers are the most efficient ways to engage with subject-matter experts in quantum-safe cryptography.

In line with that thinking, IBM is teaming up with the Global System for Mobile Communications Association (GSMA) and Vodafone in the first taskforce dedicated to global adoption of quantum-safe cryptography protections for telecommunications. This newly formed group will address the crucial step of charting a roadmap to quantum-safe networks and operational criteria.²⁴

Engaging stakeholders via partnerships and communities of practice

Every organization could benefit from a Center of Excellence around quantum computing, data encryption, and cryptography. As pointed out in *The Quantum Decade*, enterprises can develop partnerships and join ecosystems for “deep tech” quantum know-how. What they do need on their teams is literacy in quantum computing potential—a fluency that can help scope out possibilities and define a transformative path forward.²⁵

Also essential is a cybersecurity sub-team. This calls for one or more in-house resources who keep on top of remediation efforts associated with quantum-safe cryptography, in particular establishing priorities, identifying issues, and troubleshooting operational constraints. This person or team should have visibility across application modernization and quantum-safe transformation efforts.

Because quantum capabilities will take time to mature, external resources like communities of knowledge can facilitate sharing insights, shaping leading practices, and influencing the development of quantum-safe governance.

Perspective

Starting your quantum-safe journey

As organizations prepare for the quantum era, they also need to know where and how to protect their data and systems from future cryptographically relevant quantum computers. With so much converging at once—new algorithms, standards, best practices, and guidance from government and standards organizations—the IBM Quantum Safe roadmap (see Figure 4) guides enterprises through the major milestones that can lead to a successful implementation of new quantum-safe cryptographic standards.²⁶

FIGURE 4

IBM Quantum Safe roadmap

Regulatory milestones	2022	2023	2024	2025	2026+					
	NIST selects algorithms for standardization	Federal agencies plan for adoption of PQC	NIST publishes PQC standards	CSNA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC					
IBM services	Helping clients throughout their journey to quantum safe <hr/> <p style="text-align: center;">Scale toward crypto-agility IBM multcloud services, cybersecurity transformation services</p> <p style="text-align: center;">Modernize applications and data security IBM application modernization, data modernization services</p> <p style="text-align: center;">Establish foundation IBM Quantum Safe technical services</p>									
IBM Quantum Safe technology	Empowering clients to discover, observe, and transform their cryptography <hr/> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> Remediation patterns: Proxy, VPN, TLS IBM Quantum Safe Advisor Compliance posture, vulnerabilities, prioritization IBM Quantum Safe Explorer Scanner, dependency analyzer, CBOM generator </td> <td style="width: 50%; vertical-align: top;"> IBM Quantum Safe Remediator Quantum-safe PKI, key and certificate management VMS integration CI/CD integration </td> </tr> </table> <hr/> <table border="0" style="width: 100%;"> <tr> <td style="width: 33%; vertical-align: top;"> Algorithms & protocols Key encryption: CRYSTALS-Kyber Digital signature: CRYSTALS-Dilithium, FALCON </td> <td style="width: 33%; vertical-align: top;"> Interoperability standards CBOM </td> <td style="width: 33%; vertical-align: top;"> Libraries OpenSSL </td> </tr> </table>					Remediation patterns: Proxy, VPN, TLS IBM Quantum Safe Advisor Compliance posture, vulnerabilities, prioritization IBM Quantum Safe Explorer Scanner, dependency analyzer, CBOM generator	IBM Quantum Safe Remediator Quantum-safe PKI, key and certificate management VMS integration CI/CD integration	Algorithms & protocols Key encryption: CRYSTALS-Kyber Digital signature: CRYSTALS-Dilithium, FALCON	Interoperability standards CBOM	Libraries OpenSSL
Remediation patterns: Proxy, VPN, TLS IBM Quantum Safe Advisor Compliance posture, vulnerabilities, prioritization IBM Quantum Safe Explorer Scanner, dependency analyzer, CBOM generator	IBM Quantum Safe Remediator Quantum-safe PKI, key and certificate management VMS integration CI/CD integration									
Algorithms & protocols Key encryption: CRYSTALS-Kyber Digital signature: CRYSTALS-Dilithium, FALCON	Interoperability standards CBOM	Libraries OpenSSL								
IBM infrastructure	Accelerating the client journey to quantum safe <hr/> <table border="0" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM) </td> <td style="width: 50%; vertical-align: top;"> IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power </td> </tr> </table>					IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power			
IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power									

The IBM Quantum Safe roadmap

Sometimes, the journey starts before travelers realize they need a roadmap. In this case, the transition to post-quantum cryptography is well underway. In the US last year, the Biden administration issued a memorandum to the heads of executive departments and agencies declaring that they were required to submit a cryptographic inventory of systems vulnerable to quantum computing-based exploits.²⁷

Looking ahead, in 2025, the National Security Administration (NSA) will require owners and operators of national security systems to prioritize quantum-safe algorithms while configuring their systems.²⁸ Use of these algorithms will be mandatory for commercial products used in these systems.²⁹

This means that, in about two years, organizations engaging with the US federal government will need to begin their quantum-safe transition.

The IBM Quantum Safe roadmap enables organizations to confidently implement new cryptography infrastructure and solutions that adapt to changing circumstances. As a first step, leaders will want to ensure their stakeholders understand how these systems work and how to incorporate risks and associated impacts into their roadmaps.

Given how extensively we rely upon existing data encryption algorithms, this mission may seem daunting. It's helpful to distill major milestones into three focus areas (see Figure 5):

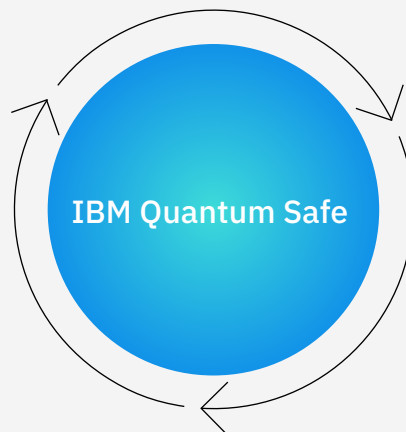
FIGURE 5

IBM Quantum Safe remediation

Recommended methodology

Transform

Remediate by deploying quantum-safe cryptographic patterns best-suited to the organization's operating environment.



Discover

Identify cryptography usage, analyze dependencies, and generate a Cryptography Bill of Materials (CBOM).

Observe

Analyze cryptography posture of compliance and vulnerabilities and prioritize remediation based on risks.

Discover

At the Discover stage, organizations need to scan source code and object code to locate all cryptographically relevant artifacts and dependencies. By producing static code inventory and surfacing the quantum security risks present in dependencies, imports, platforms, and configurations, organizations can manage their application security.

A call graph catalogs cryptographic artifacts, producing a knowledge base that is arranged into a CBOM. Prudent organizations should begin creating their CBOMs this year: in 2024, NIST is expected to publish its post-quantum cryptography (PQC) standards.

Observe

At the Observe stage, leaders gain an operations perspective of their IT environment through an audit of metadata that is collected from network and security scanners and consolidated CBOMs and augmented with policy-based enrichment. This contextual analysis should lead to a comprehensive cryptographic inventory that enables leaders to observe in real time their cryptographic usage and at-risk data flows.

This cryptographic inventory should provide a prioritized list of vulnerabilities based on industry-specific compliance policies, business priorities, and risks, so organizations can update their cryptographic infrastructure and related data solutions accordingly.

Transform

At the Transform stage, one key initiative is to explore remediation patterns and understand the potential impact on business systems and assets. Remediation allows implementing optimal patterns with quantum-safe algorithms, certificates, and key management services.

This also helps organizations achieve crypto-agility—meaning they can quickly adapt to changing policies and threats without significant operational or budgetary implications. This exploration should support a hybrid implementation approach that allows use of *both* classical and quantum-safe cryptography as organizations transition toward Federal Information Processing Standards (FIPS)-certified quantum-safe algorithms.

Making the world quantum safe

While timelines may shift, the broader steps toward quantum-safe computing are expected to remain constant. The IBM Quantum Safe roadmap can help organizations embrace the pace of change required to address new quantum-safe standards and integrate them into existing IT or IS programs. With a roadmap in hand, these changes may also be used to support broader transformation initiatives. To be successful, organizations within and across industries will need

to share best practices and lessons learned. Within the next couple of years, our aspiration is that organizations have a quantum-safe strategy in place and are well along their way toward implementing quantum-safe standards.

Making organizations quantum safe will help secure critical data for the foreseeable future. With that as our foundation, we can truly explore the vast potential of the quantum era.



Gaining quantum-safe momentum

We have outlined, at a high level, the three focus areas of Discover, Observe, and Transform. Here, we go into tactical steps that align with recommendations from the Cybersecurity and Infrastructure Security Agency (CISA), a US federal government organization.³⁰ These recommendations should be adapted to address the unique needs of any particular organization.


Establishing the foundation

- Gain buy-in from senior leaders about the urgency associated with quantum-safe remediation.
- Assess vendors for possible inclusion in your organization’s roadmap. Seek out partners with extensive quantum-safe cryptographic research experience.
- Educate your workforce about the upcoming transition. Develop and deliver relevant training based on roles and responsibilities.
- Gather critical and contextual metadata around data workflows to create better insight-driven recommendations.
- Identify near-term, achievable cryptographic maturity goals, then prioritize initiatives to reduce near-term risks and to lay foundations for long-term crypto-agility.




Discover

- Develop a Cryptographic Bill of Materials (CBOM), including cryptography usage identification and dependency analysis.
- Determine the extent of your exposed data, systems, applications, and services. Visualize key relationships and dependencies.
- Inventory your organization’s systems for applications and understand how cryptography is currently being used. For example, how do you currently manage and implement encryption, signing of data, cryptographic keys, and so forth?
- Create acquisition policies regarding quantum-safe cryptography. This process should include:
 - Establishing service levels and requirements for the transition.
 - Pinpointing required foundational technologies.
 - Working with key vendors on a common approach to quantum-safe governance that is consistent with your organization’s own cryptographic governance and security.



Observe

- Develop an executive dashboard to gain an operational view of enterprise-wide cryptography usage and posture.
- Incorporate IT observability and telemetry capabilities to understand data workflows, vulnerabilities, and compliance and to prioritize data remediation efforts.³¹
- Incorporate AI capabilities to support identification of data assets and services, interpret usage patterns, automate routine hygiene processes, and guide decisioning about data remediation.
- Incorporate common data governance mechanisms to promote visibility and to help ensure consistency of operations.
- Formalize cryptography posture to address operational risk and regulatory compliance requirements.



Transform

- Determine best practices for the new quantum-safe cryptographic algorithms (NIST) and implementations in a development environment to identify best-fit remediation patterns. Organizations should wait until the new standards are officially released to deploy in the production environment.
- Create and execute a plan for transitioning your organization's systems to the new cryptographic standards. This plan should include:
 - Formally adopting new cryptographic design patterns based on an optimal mix of classical and quantum-safe encryption standards.
 - Validating and testing products that incorporate the new standard.
 - Implementing and deploying new crypto-agility processes in the production environment.
 - Monitoring and optimizing performance, based on empirical learning.
 - Decommissioning old technology that will become unsupported upon publication of the new standard.
- Promote the business impact of quantum-safe and crypto-agility investments.

About Expert Insights

Expert Insights represent the opinions of thought leaders on newsworthy business and related technology topics. They are based on conversations with leading subject-matter experts from around the globe. For more information, contact the IBM Institute for Business Value at iibv@us.ibm.com.

IBM Institute for Business Value

For two decades, the IBM Institute for Business Value has served as the thought leadership think tank for IBM. What inspires us is producing research-backed, technology-informed strategic insights that help leaders make smarter business decisions.

From our unique position at the intersection of business, technology, and society, we survey, interview, and engage with thousands of executives, consumers, and experts each year, synthesizing their perspectives into credible, inspiring, and actionable insights.

To stay connected and informed, sign up to receive IBV's email newsletter at ibm.com/ibv. You can also follow @IBMIBV on Twitter or find us on LinkedIn at <https://ibm.co/ibv-linkedin>.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research, and technology to give them a distinct advantage in today's rapidly changing environment.

Notes and sources

- 1 *The Quantum Decade*. IBM Institute for Business Value. November 2022. ibm.co/quantum-decade
- 2 Based on internal IBM experience.
- 3 "How to preserve secrets in a quantum age." *The Economist*. July 13, 2022. <https://www.economist.com/science-and-technology/2022/07/13/how-to-preserve-secrets-in-a-quantum-age>
- 4 Based on internal IBM information.
- 5 Davis, Mel. "Toxic Substance Exposure Requires Record Retention for 30 Years." Alert presented by CalChamber. February 18, 2022. <https://calchamberalert.com/2022/02/18/toxic-substance-exposure-requires-record-retention-for-30-years/>; "Retention and Destruction of Health Information." AHIMA. Accessed November 29, 2022. <https://library.ahima.org/PB/RetentionDestruction#.Y4VxPi2B2fU>; Nakamura, Masahiko. "Current Status of Electronic Medical Recording in Japan and Issues Involved." *JMAJ*. 2006. https://www.med.or.jp/english/pdf/2006_02/070_080.pdf; "HIPAA and Medical Records Retention Requirements by State." Total HIPAA. Accessed November 29, 2022. <https://www.totalhipaa.com/wp-content/uploads/2017/02/StateDocumentRetentionAgencyMedical.pdf>; "How long should I keep records?" Internal Revenue Service. Accessed November 29, 2022. <https://www.irs.gov/businesses/small-businesses-self-employed/how-long-should-i-keep-records>
- 6 Hayat, Zia. "Digital trust: How to unleash the trillion-dollar opportunity for our global economy." World Economic Forum. August 17, 2022. <https://www.weforum.org/agenda/2022/08/digital-trust-how-to-unleash-the-trillion-dollar-opportunity-for-our-global-economy/>
- 7 "Preparing Critical Infrastructure for Post-Quantum Cryptography." CISA Insights. August 2022. https://www.cisa.gov/sites/default/files/publications/cisa_insight_post_quantum_cryptography_508.pdf
- 8 "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." The White House. May 4, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>
- 9 Candelon, François, Maxime Courtaux, Gabriel Nahas, and Jean-François Bobier. "The U.S., China, and Europe are ramping up a quantum computing arms race. Here's what they'll need to do to win." *Fortune*. September 2, 2022. <https://fortune.com/2022/09/02/quantum-computing-cryptography-companies-arms-race/>
- 10 Mosca, Michele, Dr. and Dr. Marco Piani. "2021 Quantum Threat Timeline Report." Global Risk Institute. January 24, 2022. <https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/>
- 11 "Cryptography." Wikipedia. Accessed November 8, 2022. <https://en.wikipedia.org/wiki/Cryptography>

- 12 “Encryption.” Tech Target. Accessed October 6, 2022. <https://www.techtarget.com/searchsecurity/definition/encryption>
- 13 Wise, Jason. “How Much Data is Created Every Day in 2022?” Earthweb. September 22, 2022. <https://earthweb.com/how-much-data-is-created-every-day/>
- 14 Kane, Gerald C. “‘Digital Transformation’ Is a Misnomer.” MIT Sloan Management Review. August 7, 2017. <https://sloanreview.mit.edu/article/digital-transformation-is-a-misnomer/>
- 15 Computer Security Resource Center. “Remediation.” NIST. Accessed October 11, 2022. <https://csrc.nist.gov/glossary/term/remediation>
- 16 Chen, Lily *et al.* “Report on Post-Quantum Cryptography.” NISTIR 8105. April 2016. <https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf>
- 17 “Post-Quantum Cryptography PQC.” Computer Security Resource Center. NIST. Updated September 21, 2022. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- 18 Moody, Dustin. “Let’s Get Ready to Rumble—The NIST PQC ‘Competition.’” NIST. Accessed October 11, 2022. https://csrc.nist.gov/CSRC/media/Presentations/Let-s-Get-Ready-to-Rumble-The-NIST-PQC-Competiti/images-media/PQCrypto-April2018_Moody.pdf
- 19 “IBM scientists help develop NIST’s quantum-safe standards.” IBM Research Blog. July 6, 2022. <https://research.ibm.com/blog/nist-quantum-safe-protocols>
- 20 Curioni, Alessandro. “How quantum-safe cryptography will ensure a secure computing future.” World Economic Forum. July 6, 2022. <https://www.weforum.org/agenda/2022/07/how-quantum-safe-cryptography-will-ensure-a-secure-computing-future/>
- 21 Muppidi, Sridhar and Walid Rjaibi. “Transitioning to Quantum-Safe Encryption.” Security Intelligence. December 8, 2022. <https://securityintelligence.com/posts/transitioning-quantum-safe-encryption>
- 22 “NIST Announces First Four Quantum-Resistant Cryptographic Algorithms.” NIST. July 5, 2022. <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>
- 23 “How we quantum-proofed IBM z16.” IBM Research blog. October 11, 2022. <https://research.ibm.com/blog/z16-quantum-safe-migration>
- 24 “GSMA, IBM and Vodafone Establish Post-Quantum Telco Network Taskforce.” IBM Newsroom. Sep 29, 2022. <https://newsroom.ibm.com/2022-09-29-GSMA,-IBM-and-Vodafone-Establish-Post-Quantum-Telco-Network-Taskforce>
- 25 The Quantum Decade. IBM Institute for Business Value. November 2022. ibm.co/quantum-decade
- 26 Harishankar, Ray, John Buselli, and Jai S. Arun. “How IBM Quantum is bringing organizations along their quantum-safe technology journey.” IBM Reserch blog. May 10, 2023. <https://research.ibm.com/blog/quantum-safe-roadmap>
- 27 “FACT SHEET: President Biden Announces Two Presidential Directives Advancing Quantum Technologies.” The White House. May 4, 2022. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/fact-sheet-president-biden-announces-two-presidential-directives-advancing-quantum-technologies/>; “IBM Statement on the Quantum Computing Cybersecurity Preparedness Act.” IBM. December 13, 2022. <https://www.ibm.com/policy/ibm-statement-on-the-quantum-computing-cybersecurity-preparedness-act/>
- 28 “NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems.” Press release. National Security Agency/Central Security Service. September 7, 2022. <https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/>
- 29 “Cybersecurity Advisory Announcing the Commercial National Security Algorithm Suite 2.0.” National Security Agency. September 2022. https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF
- 30 “Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats.” Cybersecurity & Infrastructure Security Agency (US). July 5, 2022. <https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats>
- 31 “What is observability?” IBM Cloud. Accessed May 3, 2023. <https://www.ibm.com/topics/observability>

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America | May 2023

IBM, the IBM logo, ibm.com and Watson are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at: ibm.com/legal/copytrade.shtml.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This report is intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. IBM shall not be responsible for any loss whatsoever sustained by any organization or person who relies on this publication.

The data used in this report may be derived from third-party sources and IBM does not independently verify, validate or audit such data. The results from the use of such data are provided on an “as is” basis and IBM makes no representations or warranties, express or implied.

