Prepare for the next era of computing with quantum-safe cryptography on IBM z16

The security impact of quantum computing

Quantum computing is being referred to as the next technology revolution. When a sufficiently powerful quantum computer is available, it will open up new possibilities to solve challenging problems that classical computers can't address. There are many exciting applications in industries including pharmaceuticals, finance, and manufacturing.

The problem is, quantum computers will also be able to solve the math problems that give many cryptographic algorithms their strength, which will have a significant impact on the classical encryption, hashing and public key algorithms we use today.

Quantum algorithms running on sufficiently powerful quantum computers have the potential to weaken or break core cryptographic primitives that we use to secure systems and communications. The fact that these algorithms can be broken leaves the foundation for global digital security at risk. Organizations relying on weak algorithms will be at risk of major data breaches. Temporary solutions like increasing RSA or ECC key size, will only buy a little time — like extra months, not extra years[1].

Keep a step ahead with quantum-safe cryptography

Organizations and standards bodies are taking action to address the threat. The National Institute of Standards and Technology (NIST) initiated a process to solicit, evaluate and standardize new public-key cryptographic algorithms that can resist threats posed by both the classical computers we have today and quantum computers that will be available in the future. Following three rounds of evaluation, NIST plans to select a small number of new quantum-safe algorithms this year and have new quantum-safe standards in place by 2024. As part of this program, IBM researchers have been involved in the development of three quantum-safe cryptographic algorithms based on lattice cryptography which are in the final round of consideration: CRYSTALS-Kyber, CRYSTALS-Dilithium and Falcon.

Fortunately, we have time to implement quantum-safe solutions before the advent of large-scale quantum computers — but not much time. We don't know when a large-scale quantum computer capable of breaking public key cryptographic algorithms will be available, but experts predict that this could be possible by the end of the decade. And, sensitive data with a long lifespan is already vulnerable to "harvest now, decrypt later" attacks: hackers can harvest encrypted data today and store it for later when they can decrypt it using a quantum computer. Organizations in the United States and Germany have already issued requirements for government agencies to begin quantum-safe modernization planning and start using hybrid schemes for protection in high-security applications by using a combination of both classical algorithm and quantum-safe algorithm.

Based on past experience, NIST expects most organizations will need between 5 to 15 years to implement new public-key standards once they are available, so they advise beginning the transition as soon as possible[2]. NIST advises taking action now, as it will help make the transition process less expensive, less disruptive, and reduce the likelihood of mistakes.

Future proof your business with IBM z16™

As we prepare for a quantum world, IBM is committed to developing and deploying new quantum-safe cryptographic technology. IBM z16 is the industry's first quantum-safe system, protected by quantum-safe technologies across multiple layers of firmware, to help protect your business-critical infrastructure and data from quantum attacks[3].

IBM z16 quantum-safe secure boot technology protects system integrity by using quantum-safe and classical digital signatures to perform a hardware-protected verification of the IML firmware components. This protection is anchored in a hardware-based Root of Trust for the firmware chain of trust. This quantum-safe technology is designed to provide a double layer of protection by using a dual signature scheme which employs classical and quantum-safe cryptographic algorithms to ensure the server starts safely and securely by keeping unauthorized firmware (malware) from taking over your server during system start-up.

Leverage Pervasive Encryption for IBM Z®, a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify Quantum Safe encryption, reduce costs associated with protecting data and aid with mitigation of risks associated with Quantum threats.

Now is the time to start planning for the replacement of hardware, software and services that use public-key and weak symmetric key cryptography. IBM z16 positions you to begin using quantum-safe cryptography along with classical cryptography as you begin modernizing existing applications and building new applications. IBM z16, with Integrated Cryptographic Service Facility (ICSF HCR77D1), the Crypto Express 8S, TKE 10.0 and other security features provide the vehicle to take advantage of these quantum-safe capabilities.

IBM z16 will enable a number of critical client use cases across many industries with the following capabilities:

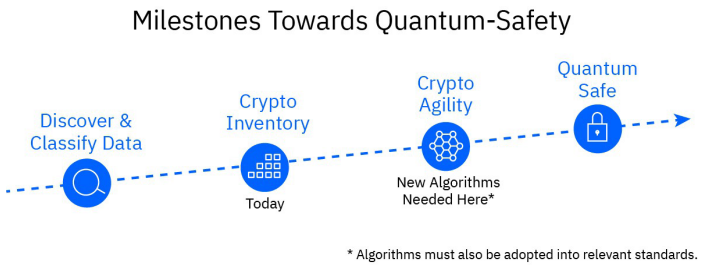
- Quantum-safe key generation
- Quantum-safe encryption
- Quantum-safe hybrid key exchange schemes
- Quantum-safe dual digital signature schemes

Tools and services to help accelerate your journey to quantum-safe security

As you prepare to adopt new quantum-safe standards, there are several key milestones to follow:

- Discover and classify data: Start by classifying the value of your data and understanding compliance requirements. This helps you create a data inventory.
- Create a crypto inventory: Once you have classified your data, you will need to identify how your data is encrypted, as well as other uses of cryptography to create a crypto inventory that will help you during your migration planning. Your crypto inventory will include information like encryption protocols, symmetric and asymmetric algorithms, key lengths, crypto providers, etc.
- Embrace crypto agility: The transition to quantum-safe standards will be a multi-year journey as standards evolve and vendors move to adopt quantum-safe technology. Use a flexible approach and be prepared to make replacements. Implement a hybrid approach as recommended by industry experts by using both classical and quantum-safe cryptographic algorithms. This maintains compliance with current standards while adding quantum-safe protection.

IBM z16 offers several tools to help you discover how cryptography is used in applications to aid in developing a crypto inventory for migration and modernization planning. As you create your crypto inventory, IBM z16 provides new instrumentation that can be used to track cryptographic instruction execution in the CP Assist for Cryptographic



Functions (CPACF). Additionally, IBM Application Discovery and Delivery Intelligence (ADDI) software has been enhanced with capabilities to discover where and what crypto is used in applications. Other tools that aid in crypto discovery on the platform include IBM ICSF Crypto Usage Tracking, the IBM Crypto Analytics Tool (CAT), and z/OS® Encryption Readiness Technology (zERT).

IBM Z Lab Services offers a Quantum Safe Risk Assessment to help you discern how your technology may fare against quantum threats, and review steps you can take today to prepare. This assessment will help you discover and map your critical services relying on encryption, inventory your encrypted data and encryption artifacts (keys, certificates), evaluate risks in the pre- and post-quantum era and develop a transition roadmap including the latest quantum-safe technologies.

For more information

IBM z16 is designed to help you stay ahead of quantum threats and accelerate your transition to a quantum-safe future. Explore quantum-safe technologies, crypto discovery tools and services available on IBM z16, the powerful and secure platform for business:

- IBM z16: https://www.ibm.com/products/z16
- IBM z16 Crypto Express 8S (CEX8S) Hardware Security Module (HSM): https://www.ibm.com/security/cryptocards/hsms
- IBM Z Pervasive Encryption https://www.ibm.com/support/z-content-solutions/pervasive-encryption/
- IBM Application Discovery and Delivery Intelligence (ADDI) software with crypto discovery: https://www.ibm.com/products/app-discovery-and-delivery-intelligence
- IBM Z Quantum Safe Risk Assessment: https://www.ibm.com/downloads/cas/ON6K9KWA
- IBM ICSF Crypto Usage Tracking: https://www.ibm.com/docs/en/zos/3.1.0?topic=guide monitoring-users-jobs-that-perform-cryptographic-operations
- Unified Key Orchestrator for IBM z/OS® https://www.ibm.com/products/unified-key-orchestrator-for-zos
- IBM z/OS Encryption Readiness Technology: https://www.ibm.com/docs/en/zos/3.1.0?topic=zert-using-zos-encryption-readiness-technology
- z/OS Cryptographic Services: https://www.ibm.com/docs/en/zos/3.1.0?topic=zos-cryptographic-services

IBM Corporation
New Orchard Road
Armonk, NY 10504

1. *The Top Security Technology Trends to Watch, Forrester, 2021*
2. *Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms, NIST, 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf*
3. *IBM z16 with the Crypto Express 8S card provides quantum- safe APIs providing access to quantum-safe algorithms which have been selected by NIST to become part of its post-quantum cryptographic standard. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms Quantum-safe cryptography refers to efforts to identify algorithms that are resistant to attacks by both classical and quantum computers, to keep information assets secure even after a large-scale quantum computer has been built. Source: https://www.etsi.org/technologies/quantum-safe-cryptography ." These algorithms are used to help ensure the integrity of a number of the firmware and boot processes. IBM z16 is the Industry-first system protected by quantum-safe technology across multiple layers of firmware. According to Peter Rutten, Research Vice-President IDC, "z16 is the industry's first quantum-safe computing platform."*