Best practices Cloud security
7 min read

Starting your journey to become quantum-safe

By Michal Braverman-Blumenstyk, Corporate Vice President, Microsoft Security Division CTO, Israel R&D Center Managing Director

November 1, 2023

Information protection and governance

Threat trends

There's no doubt we are living through a time of rapid technological change. Advances in ubiquitous computing and ambient intelligence transform nearly every aspect of work and life. As the world moves forward with new advancements and distributed technologies, so too does the need to understand the potential security risks. At Microsoft, our mission has always been focused on keeping our customers' and partners' information and data safe and secure, and this is why we're committed to advancing encryption solutions, in order to enable responsible use of new technologies such as AI and quantum computing. As one important example, while scaled quantum computing will help solve some of our toughest problems, like helping us discover new ways of addressing climate change and food scarcity, its development may also create a new set of security challenges and in turn require new encryption standards. As this future quickly approaches, how can we ensure that we reap the benefits of quantum computing while remaining safe in a post-quantum world?

Start your journey with Microsoft towards quantum-safety.

View the questionnaire >

We believe the first step every organization should take toward quantum safety is to be aware of the need to organize, plan, and begin an impact assessment. We recommend prioritizing symmetric encryption where applicable and subsequently adopting post-quantum cryptography (PQC) for asymmetric encryption once standardized and approved by relevant setting bodies and governments, as recommended by cybersecurity agencies globally. Furthermore, we are exploring and experimenting with additional classical and quantum security solution layers through internal experiments, POCs, and collaborations with partners.

Given that preparing for such an objective will be a multi-year and iterative process that requires strategic foresight, it's crucial for organizations to start investing time in their planning and execution efforts today. Thanks to our extensive experience in quantum engineering and expertise as a service and security provider, we can serve as a trusted partner to navigate this process across industry and government.

Tomorrow's quantum computers threaten today's data

In our previous blog post, we discussed the limitations of current quantum computers in terms of breaking today's encryption technology. In parallel, the emergence of scaled quantum computers with specific algorithms—such as Shor's algorithm—could put public key encryption at risk and compromise sensitive information.

While it may take at least 1 million qubits for a quantum computer to break certain encryption algorithms using Shor's algorithm, today's long-term and sensitive data could already be at risk: bad actors could carry out a "Harvest Now, Decrypt Later" scenario by recording data today and decrypting it later when cryptographically relevant quantum computers become available. **Therefore, knowing which data to secure now is a first step on the path to a quantum-safe future.**

Microsoft's commitment to keeping our customers and partners secure

Putting our recommendations into practice, we have taken a comprehensive approach to quantum safety. Because quantum will have a material impact on today's classical encryption of both hardware and software, we've invested time and efforts to set cross-company goals and establish accountability at the most senior levels of our organization. This led to the establishment of the Microsoft Quantum Safe Program, which aims to accelerate and advance all quantum-safe efforts across Microsoft from both technical and business perspectives. The program focuses on Microsoft's transition to quantum safety and the adoption of PQC algorithms across our products, services, and datacenters. Additionally, it aims to assist and empower our customers and partners on their own journey to quantum safety across their processes, priorities, and requirements.

As the first step and highest priority, we are ensuring the compliance of our existing symmetric key encryption and hash function algorithms. Symmetric algorithms, such as Advanced Encryption Standard (AES), and hash functions, such as Secure Hash Algorithm (SHA), are resilient to quantum attacks, and can therefore still be used in deployed systems. At Microsoft, we are already using protocols based on symmetric encryption, such as Media Access Control Security (MACsec) point-to-point protocol.

On top of symmetric encryption, we will prioritize PQC algorithms—still in the process of being standardized by global bodies such as the National Institute of Standards and Technology (NIST), International Standards Organization (ISO), and Internet Engineering Task Force (IETF)—to handle future threats where asymmetric encryption is currently used. Today, much of the internet's data, from e-commerce to Wi-Fi access, is kept secure by public key, or asymmetric key cryptography. Currently used public key algorithms rely on complex mathematical problems considered infeasible for classical computers to break, but that are a perfect task for quantum computers running Shor's algorithm. This undermines the effectiveness of public key algorithms like RSA and Elliptic Curve Cryptography (ECC), and means that PQC algorithms will need to be deployed quickly once standardized, starting with hybrid encryption schemes in tandem with classical algorithms to accelerate adoption.

Empowering and collaborating with the global community

We see the effort to achieve quantum safety as a collaborative effort, and this is why we invest heavily in our ecosystems, global partnerships, and close collaborations with standards-setting bodies, academia, and industry partners alike to foster continuous innovation in the quantum security landscape. The standardization of PQC algorithms, driven by NIST's efforts, is a key step to achieving PQC compliance.

Because we believe that PQC adoption is the ideal path to follow, we're collaborating with standard-setting bodies while conducting experiments and assessments to facilitate the adoption of these algorithms across our services and products as needed. As an example, we are participating in the NIST/NCCoE Migration to PQC to demonstrate vulnerable cryptography detection and drive PQC experiments and integration capabilities. Those efforts, along with our participation in the Open Quantum Safe project, will allow the members to implement and test PQC candidates together, so we can be ready for adoption once the final specs are out.

Furthermore, as part of our investment to empower and collaborate with the global security community, we co-authored FrodoKEM, a quantum-safe key encapsulation mechanism that has been selected, together with Kyber and Classic McEliece, to be part of the first international ISO standard for PQC (in addition, we are participating as co-editors of the standard). We also recently submitted SQISign, a new quantum-safe signature scheme that we co-authored with several industry and academia partners, to NIST's call for additional signature schemes. Lastly, we continue to actively participate as founding members of the new post-quantum cryptography coalition by MITRE and will help to drive progress toward a broader understanding of the public adoption of PQC and NIST's recommendations.

While we continue to conduct research to further develop state-of-the-art security solutions, we are also exploring the potential of other classical and quantum technologies, such as Quantum Key Distribution (QKD). Holistically, at the core of our mission is a commitment to achieving quantum-safety and ensuring the security of our customers.

Getting started with your PQC transition today

To support our customers in preparing for and navigating their quantum-safe journey, we offer assistance and guidance: we invite you to start your path with us by filling out this questionnaire. Based on your responses, we can understand your status and

priorities, and provide the necessary support, including access to experts.

As a first step, we recommend starting with a comprehensive planning process and a definition of your organization's criteria for what constitutes your critical areas and sensitive information, alongside a cryptography inventory and impact assessment of your essential data, code, cryptographic technologies, and the critical services of your organization. This will help you to identify any asymmetric encryption in use that will need to be replaced with the latest PQC standardized algorithms. This process is especially important to identify critical areas and systems that involve or protect sensitive data with a value that extends beyond 10 years and should be prioritized in migrating to PQC.

By considering which data and code need to be secured now, and which may become less relevant over time, as well as uncovering specific instances where cryptography could be used inappropriately or not ideally, your organization will have a better understanding of where to best mitigate potential risks as a quantum future approaches. This will enable you to confidently make the switch to the latest PQC standardized algorithms and safeguard your sensitive data for years to come.

Explore CodeQL

To help, we are contributing to CodeQL: a next-generation program code analysis tool provided by GitHub in collaboration with organizations including NIST and NCCoE. With CodeQL, we are building out a comprehensive set of detections that can empower users to create a complete inventory of all encryption usage within the application layer, helping to produce a cryptographic bill of materials and identify legacy cryptography that requires remediation. This tool can thus help create a cryptography inventory and impact assessment that will drive operational planning and create understanding and clarity around the timeline, resources, and level of risk for which to account.

Try now the Crypto Experience for Resource Estimator

Furthermore, we recently launched the Crypto Experience for Azure Quantum Resource Estimator. Drawing on published research from Microsoft, this new interactive cryptography experience will show you why a symmetric key could remain safe from quantum attacks, but the current public key is vulnerable. And because it is integrated with Copilot in Azure Quantum, you can use the universal user interface of natural language to ask, learn, and explore more topics within the intersection of quantum computing and cryptography.

The opportunity to usher in a quantum, and quantum-safe, future is immense. We see how the collective genius of scientists and businesses will revolutionize the building blocks of everyday products to usher in a new era of innovation and growth in many fields. That's what motivates us at Microsoft to drive new breakthroughs and empower every person and every organization on the planet. Our commitment to our customers, partners, and ecosystem to become quantum-safe and remain secure has never been stronger. We are accountable for having our products and services quantum-resistant and safe and will support and guide our customers through this journey to quantum safety.

Learn more

- Start your journey with Microsoft towards quantum-safety by filling out this questionnaire.
- Learn more about our vision of quantum networking.
- Explore the Open Quantum Safe project for prototyping and evaluating quantum-resistant cryptography.
- Visit the Azure Quantum website and check out the Microsoft Quantum Innovator Series webinars.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (formerly known as "Twitter") (@MSFTSecurity) for the latest news and updates on cybersecurity.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365