IBM Newsroom

IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards

As quantum computers rapidly advance, U.S. National Institute of Standards and Technology (NIST) publishes new algorithms, including those developed by IBM, in collaboration with industry partners, to secure data against potential quantum attacks

YORKTOWN HEIGHTS, N.Y., Aug. 13, 2024 /PRNewswire/ -- Two IBM-developed algorithms (NYSE: IBM) have been officially published among the first three post-quantum cryptography standards, announced today by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST).

The standards include three post-quantum cryptographic algorithms: two of them, ML-KEM (originally known as CRYSTALS-Kyber) and ML-DSA (originally CRYSTALS-Dilithium) were developed by IBM researchers in collaboration with several industry and academic partners. The third published algorithm, SLH-DSA (initially submitted as SPHINCS+) was co-developed by a researcher who has since joined IBM. Additionally, a fourth IBM-developed algorithm, FN-DSA (originally called FALCON), has been selected for future standardization.

The official publication of these algorithms marks a crucial milestone to advancing the protection of the world's encrypted data from cyberattacks that could be attempted through the unique power of quantum computers, which are rapidly progressing to cryptographic relevancy. This is the point at which quantum computers will harness enough computational power to break the encryption standards underlying most of the world's data and infrastructure today.

"IBM's mission in quantum computing is two-fold: to bring useful quantum computing to the world and to make the world quantum-safe. We are excited about the incredible progress we have made with today's quantum computers, which are being used across global industries to explore problems as we push towards fully error-corrected systems," said Jay Gambetta, Vice President, IBM Quantum. "However, we understand these advancements could herald an upheaval in the security of our most sensitive data and systems. NIST's publication of their first three post-quantum cryptography standards marks a significant step in efforts to build a quantum-safe future alongside quantum computing."

As an entirely new branch of computing, quantum computers are quickly accelerating to useful and large-scale systems, as evidenced by the hardware and software milestones achieved and planned on IBM's Quantum Development Roadmap. For

example, IBM projects it will deliver its first error-corrected quantum system by 2029. This system is anticipated to run hundreds of millions of quantum operations to return accurate results for complex and valuable problems that are currently inaccessible to classical computers. Looking further into the future, IBM's roadmap includes plans to expand this system to run upwards of one billion quantum operations by 2033. As IBM builds towards these goals, the company has already equipped experts across healthcare and life sciences; finance; materials development; logistics; and other fields with utility-scale systems to begin applying and scaling their most pressing challenges to quantum computers as they advance.

However, the advent of more powerful quantum computers could carry risks to today's cybersecurity protocols. As their levels of speed and error correction abilities grow, they are also likely to encompass the ability to break today's most used cryptographic schemes, such as RSA, which has long protected global data. Beginning with work started several decades ago, IBM's team of the world's foremost cryptographic experts continue to lead the industry in the development of algorithms to protect data against future threats, which are now positioned to eventually replace today's encryption schemes.

NIST's newly published standards are designed to safeguard data exchanged across public networks, as well as for digital signatures for identity authentication. Now formalized, they will set the standard as the blueprints for governments and industries worldwide to begin adopting post-quantum cybersecurity strategies.

In 2016, NIST asked cryptographers worldwide to develop and submit new, quantum-safe cryptographic schemes to be considered for future standardization. In 2022, four out of the 69 algorithms that were submitted for review were chosen for future standardization: CRYSTALS-Kyber, CRYSTALS-Dilithium, Falcon, and SPHINCS+.

In addition to continued evaluations to publish Falcon as the fourth official standard, NIST is continuing to identify and evaluate additional algorithms to diversify its toolkit of post-quantum cryptographic algorithms, including several others developed by IBM researchers. IBM cryptographers are among those pioneering the expansion of these tools, including three newly submitted digital signatures schemes that have already been accepted for consideration by NIST and are undergoing the initial round of evaluation.

Toward its mission to make the world quantum-safe, IBM continues to integrate post-quantum cryptography into many of its own products, such as IBM z16 and IBM Cloud. In 2023, the company unveiled the IBM Quantum Safe roadmap, a three-step blueprint to chart the milestones towards increasingly advanced quantum-safe technology, and defined by phases of discovery, observation, and transformation. Alongside this roadmap, the company also introduced IBM Quantum Safe technology and IBM Quantum Safe Transformation Services to support clients in their journeys to becoming quantum safe. These technologies include the introduction of Cryptography Bill of Materials (CBOM), a new standard to capture and exchange information about cryptographic assets in software and systems.

For more information about the IBM Quantum Safe technology and services, visit: https://www.ibm.com/quantum/quantum-safe.

About IBM

IBM is a leading provider of global hybrid cloud and AI, and consulting expertise. We help clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. More than 4,000 government and corporate entities in critical infrastructure areas such as financial services, telecommunications and healthcare rely on IBM's hybrid cloud platform and Red Hat OpenShift to affect their digital transformations quickly, efficiently and securely. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions and consulting deliver open and flexible options to our clients. All of this is backed by IBM's long-standing

commitment to trust, transparency, responsibility, inclusivity and service. Visit ibm.com for more information.

Media contacts:

Erin Angelini, IBM
edlehr@us.ibm.com

Chris Nay, IBM
cnay@us.ibm.com

SOURCE IBM
