IBM Newsroom

IBM Developing New Cloud Services and Technology to Help Keep Data Secured from Future Fault-Tolerant Quantum Computers

- New quantum risk assessment and subscription services available to clients

- IBM Cloud will begin to provide quantum-safe cryptography services on the public cloud in 2020

- IBM Research demonstrates world's first quantum computing safe tape drive prototype

- IBM donates quantum-safe cryptographic algorithms to open source community

ARMONK, N.Y., Aug. 23, 2019 /PRNewswire/ -- Today at the Second Post-Quantum Cryptography Standardization Conference organized by the National Institute of Standards and Technology (NIST), IBM (NYSE: IBM) took a major step towards maintaining the highest level of security of its client's data and privacy in the future from fault-tolerant quantum computers.

With today's news, IBM is announcing that it will begin to provide, what the industry would call, quantum-safe cryptography services on the IBM public cloud in 2020 and is now offering a Quantum Risk Assessment from IBM Security to help customers assess their risk in the quantum world. Additionally, IBM cryptographers have prototyped the world's first quantum computing safe enterprise class tape, an important step before commercialization.

IBM is also committed to making quantum-safe algorithms available through the open source community. As an industry, we can only become secure if new quantum-safe algorithms are tested, interoperable and easily consumable in common security standards. To this end, IBM is donating algorithms and support to a number of open source projects such as OpenQuantumSafe.org.

These new services and technologies are building on IBM's leading position in quantum computing and leverage decades of research in cryptography to protect data at rest and in motion.

IBM first made quantum computers available through its public cloud in May 2016 with the IBM Q Experience platform. As of today, users have executed more than 28 million experiments and simulations on the quantum cloud platform and published over 180 third-party research papers.

Preparing Cybersecurity for a Quantum World

Quantum computing is an emerging form of technology that takes advantage of quantum mechanical phenomena to solve certain types of problems that are effectively impossible to solve on classical computers. As quantum systems become more powerful, they will also impact information security and will create new opportunities for improving security for data both on-premises and in the cloud.

At the current rate of progress in quantum computing, it is expected that data protected by the asymmetric encryption methods used today may become insecure within the next 10-30 years. While years away, data can

be harvested today, stored and decrypted in the future with a powerful enough quantum computer. While the industry is still finalizing post-quantum cryptography standards, businesses and other organizations can start preparing today.

IBM Takes Steps to Help Clients Maintain Security in the Future World of Quantum Computing

With more enterprises turning to the cloud for their mission-critical data, IBM is bringing together its hybrid cloud leadership with quantum and security research expertise to stay at the forefront of future quantum cybersecurity threats.

IBM will begin to unveil quantum-safe cryptography services on its public cloud in 2020. To help clients achieve quantum-safe protection of their data while it is in-transit within IBM Cloud, IBM will enhance its TLS/SSL implementations in IBM Cloud services using algorithms designed to be quantum-safe leveraging open standards and open source technology. IBM is also evaluating approaches to provide services that render quantum-safe digital signatures.

"IBM Cloud is taking the critical steps needed to help enterprises ensure their data stays secure in a quantum future," said Harish Grama, general manager, IBM Cloud. "Starting in 2020, IBM Cloud will roll out new services that will help keep data secured and private from the emerging cybersecurity challenges presented by future quantum computers."

IBM Research Donating Cryptographic Algorithms to Open Community, Demonstrates First Quantum-Safe Tape Storage Prototype

"In order to prepare for the impact that quantum computers are expected to have on data security, IBM Research has been developing cryptographic algorithms that are designed to be resistant to the potential security concerns posed by quantum computers," said Vadim Lyubashevsky, cryptographer, IBM Research. "Our jointly developed quantum-safe algorithms, part of a lattice cryptography suite called CRYSTALS, are based on the hardness of mathematical problems that have been studied since the 1980's and have not succumbed to any algorithmic attacks, either classical or quantum. This is why we have made our algorithms open source and have submitted them to NIST for standardization."

IBM has actively supported NIST on its journey to standardize quantum safe cryptography with preparatory input, algorithm submissions, analysis of submitted algorithms and feedback to the process. We will continue this commitment by contributing our learning as we migrate IBM's own systems and services to become quantum-safe based on the NIST standards, which are expected to be available between 2022-2024.

CRYSTALS (Cryptographic Suite for Algebraic Lattices) is developed jointly in collaboration with several academic and commercial partners including ENS Lyon, Ruhr-Universität Bochum, Centrum Wiskunde & Informatica and Radboud University. It's based on two quantum resistant cryptographic primitives - Kyber, a secure key encapsulation mechanism, and Dilithium, a secure digital signature algorithm. CRYSTALS has been donated to OpenQuantumSafe.org, to further develop open standards.

IBM has tested CRYSTALS successfully on a prototype IBM TS1160 tape drive using both Kyber and Dilithium in combination with symmetric AES-256 encryption to enable the world's first quantum computing safe tape drive.

The new algorithms are implemented as part of the tape drive's firmware and could be provided to customers as a firmware upgrade for existing tape drives and/or included in the firmware of future generations of tape drives.

To help clients assess their potential risks and begin the quantum-safe journey, IBM Security is also offering a quantum data risk assessment service to help clients develop a quantum-safe cryptography implementation strategy.

To educate security professionals and executives on migrating to the next generation of quantum-safe cryptography, IBM Research has recently launched a Security Subscription service which provides quarterly reports and seminars. The next seminar is currently planned for October 2, 2019 in Zurich, Switzerland.

To learn more about quantum computing and its impact on information security, download the IBM Institute for Business Value report: Wielding a double-edged sword: Preparing cybersecurity now for a quantum world

MEDIA CONTACTS:

Sarah Murphy
IBM Cloud
+1 336-337-7584
srmurphy@us.ibm.com

Chris Sciacca
IBM Research
+41 44 724 8443
cia@zurich.ibm.com

SOURCE IBM Research
