Cryptography

World's First Quantum Computing Safe Tape Drive

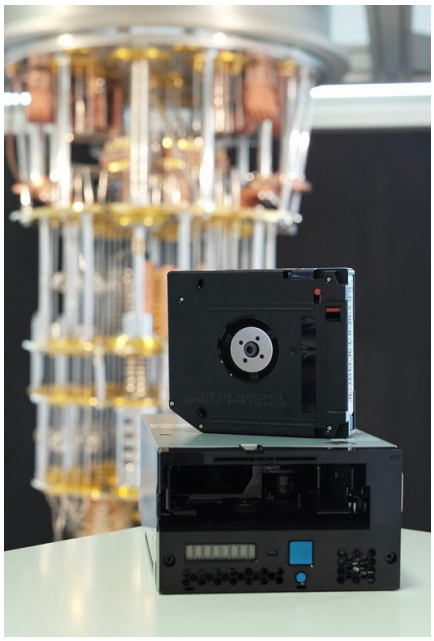
August 23, 2019 | Written by:Mark Lantz and Mark Hill

Categorized: Cryptography | IBM Research-Zurich | Quantum Computing | Security | Storage | Systems

Share this post:

Ten months ago we assembled a team from IBM Research in Switzerland and IBM tape developers based in Tucson, Arizona, to try to build something which has never been built before to address a risk that may not materialize for another decade or more. As you can tell, we love a good challenge.

The risk comes from quantum advantage, the point when a quantum computer can perform some particular computation significantly faster than a classical computer. The challenge we faced, develop a quantum computing safe tape drive, because 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.



The new IBM quantum computing-safe tape drive prototype is based on a state of the art IBM TS1160 tape drive.

Preparing Cybersecurity for a Quantum World

Quantum computingis an emerging form of computing that takes advantage of quantum mechanical phenomena to solve certain types of problem that are effectively impossible to solve on classical computers. Quantum Advantage will occur when quantum computers surpass today's classical computers at which point they are expected to enable dramatic advances in areas such as chemistry, bioinformatics and artificial intelligence, but at the same time they will impact information security.

State of the art storage technologies, such as magnetic tape drives, use a combination of symmetric and asymmetric encryption to ensure that the data they store remains secure. However, in the future, the security of today's asymmetric encryption techniques will very likely be broken by advances in quantum computing.

At the current rate of progress in quantum computing, it is expected that asymmetric encryption may become insecure within the next 10-30 years. While this seems rather far in the future, tape systems are often used to archive data for many years which is why it's important to begin implementing quantum computing-safe solutions now to provide clients sufficient time to migrate to this new technology before their data becomes vulnerable.

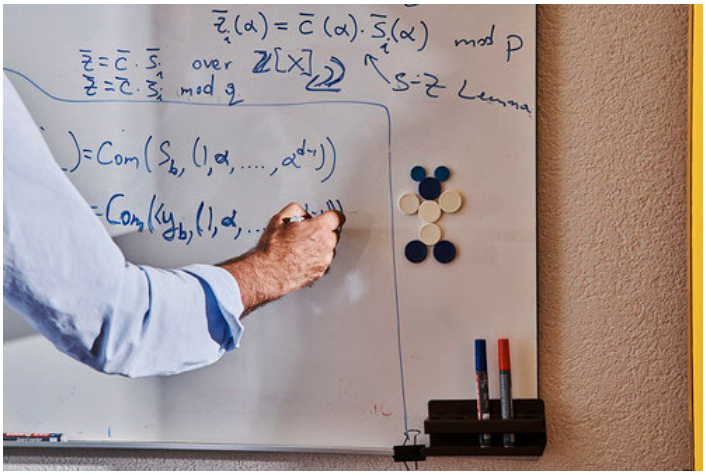
Making Tape Quantum Computing Safe

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 resistant to potential security concerns posed by quantum compute.

These algorithms are based on Lattice Cryptography, which is in turn related to a set of mathematical problems that have been studied since the 1980's and have not succumbed to any algorithmic attacks, either classical or quantum

In collaboration with several academic and commercial partners including: ENS Lyon, Ruhr-Universität Bochum, Centrum Wiskunde &

Informatica and Radboud University, IBM researchers have developed two quantum resistant cryptographic primitives based this work: Kyber, a secure key encapsulation mechanism and Dilithium, a secure digital signature algorithm. These two algorithms make up the "Cryptographic Suite for Algebraic Lattices" we call "CRYSTALS" .



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.

Both of these algorithms are candidates in the second round of the National Institute of Standards and Technology (NIST) Post Quantum Cryptography standardization process and will be presented today at the Second PQC Standardization Conference at the University of Santa Barbara, Aug 22-24, 2019.

The new IBM quantum computing-safe tape drive prototype is based on a state-of-the-art IBM TS1160 tape drive and uses 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 th 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.

Magnetic tape has a long history of leadership in storage security and is an essential technology for protecting and preserving data. For example, IBM tape drives were the first storage technology to provide built-in encryption starting with the TS1120 Enterprise Tape Driv

In addition, tape provides an additional layer of security via an airgap between the data stored on a cartridge and the outside world, i.e data stored on a cartridge cannot be read or modified unless it is mounted in a tape drive. The security and reliability provided by tape systems combined with their low total cost of ownership have resulted in tape becoming the technology of choice for archiving data in the cloud as well as in commercial and scientific data centers

With the development of quantum computing-safe tape encryption technology, IBM Tape continues the legacy of tape leadership in security and encryption and reaffirms its long term commitment to this critical part of modern storage infrastructu

---

The authors also wish to acknowledge the expertise and support of Paul Greco and Glen Jaquette from IBM Systems and Tamas Visegrady and Silvio Dragone, IBM Research.

Mark Lantz
Manager Advanced Tape Technologies, IBM Research

Mark Hill
Program Director, Development, Data Protection & Retention and DCS3xxx Disk, IBM Systems

CRYSTALS | Magnetic Tape Storage | quantum computing | Quantum Safe Cryptography

Previous Post
Making and Imaging Cyclocarbon

Next Post
Meet the "Quantum Undergraduate Research at IBM and Princeton" Interns