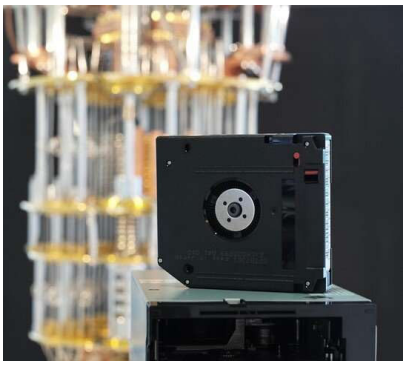
AUGUST 29, 2019 WEBLOG

Quantum safe tape drive: IBM team eyes encryption future

by Nancy Cohen , Tech Xplore



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

This week a collaborative effort among computer scientists and academics to safeguard data is winning attention and it has quantum computing written all over it.

The Netherlands' Centrum Wiskunde & Informatica (CWI), national research institute for mathematics and computer science, had the story: IBM Research developed "quantum-safe algorithms" for securing data. They have done so by working with international partners including CWI and Radboud University in the Netherlands.

IBM and partners share concerns that data protected by current encryption methods may become insecure within the next 10 to 30 years.

What's the concept? The algorithms are based on the hardness of mathematical problems that have not succumbed to any algorithmic attacks, either classical or quantum, according to CWI.

CWI said that "Although the industry is still finalizing post-quantum cryptography standards, businesses and other organizations already can start preparing today. IBM will begin to offer quantum-safe cryptography services on its public cloud in 2020."

The algorithms are part of the CRYSTAL (CRYptographic Suite for Algebraic latticeS) suite.

Further to the algorithms announcement, it was revealed that IBM cryptographers have prototyped the world's first quantum computing safe enterprise class tape, and this is seen as an important step before commercialization.

Mark Lantz, Manager Advanced Tape Technologies, IBM Research and Mark Hill, IBM Systems, trumpeted IBM's cryptography advancements earlier this month in a blog titled "World's First Quantum Computing Safe Tape Drive."

They said the story began 10 months ago when a team got together "to try to build something which has never been built before to address a risk that may not materialize for another decade or more."

They were concerned about the future of encryption methods and insecure data.

"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 IBM collaboration with academic and commercial partners resulted in (1) Kyber, a secure key encapsulation mechanism and (2) Dilithium, a secure digital signature algorithm. The two algorithms make up the Cryptographic Suite for Algebraic Lattices. The quantum computing-safe tape drive prototype uses both Kyber and Dilithium in combination with symmetric AES-256 encryption to enable what Lantz and Hill said was "the world's first quantum computing-safe tape drive."

This is where *Security Boulevard* helped with clarity. "IBM has tested CRYSTALS on a prototype of an IBM TS1160 tape drive using Kyber and Dilithium in combination with symmetric AES-256 encryption. The algorithms are implemented as part of the tape drive's firmware, which IBM hopes eventually will mean support for those algorithms will be provided as part of a software upgrade."

That IBM Research blog post noted magnetic tape's history in storage security as a technology for protecting and preserving data. IBM tape drives were a storage technology providing built-in encryption starting with the TS1120 Enterprise Tape Drive.

Writing in *ZME Science*, Tibi Puiu discussed tape for keeping data secure:

"While hard drives and SSDs are much more suited for accessing databases and reading small files, tape is ideal for storing large amounts of data over a long time. That's because it's incredibly cheap and dense. The current theoretical limit is about 29.5 billion bits per square inch, which would mean a magnetic tape the size of a traditional hard drive could store about 35 terabytes of information."

Also, IBM is donating algorithms and support to a number of open source projects such as OpenQuantumSafe.org. "As an industry, we can only become secure if new quantum-safe algorithms are tested, interoperable and easily consumable in common security standards," said an IBM release.

The goal of the Open Quantum Safe (OQS) project is to support development and prototyping of quantum-resistant cryptography.

As for IBM advancements vis a vis quantum computing, *Security Boulevard* shared its own assessment of how concerned one should be. "Outside of potentially a few nation-states, most cybercriminals are not likely to have access to a quantum computing platform anytime soon. But, in terms of the perennial cybersecurity arms race organizations find themselves in, quantum computing represents an advance that at this point can no longer be ignored."