Now that's what I call future proofing. IBM makes world's first quantum computing-safe tape drive

By **Chris Mellor** - August 23, 2019

IBM is developing cryptographic security measures to protect archived data against attacks by quantum computers.

You can't be too careful, IBM says: "While years away, data can be harvested today, stored and decrypted in the future with a powerful enough quantum computer."

In a press statement this week, Vadim Lyubashevsky, a cryptographer at IBM Research, said: "IBM Research has been developing cryptographic algorithms that are designed to be resistant to the potential security concerns posed by quantum computers."

IBM Research is working with IBM's tape development teams to implement new encryption algorithms in a TS1160 tape drive's firmware. It seems a long technology journey between the far shores of quantum computing and the humble tape drive. Why the fuss?

Big Blue is developing quantum computers and envisages these becoming enormously powerful, and advancing bio-informatics, chemistry, and AI. Our sister publication The Register recently described quantum computers as forever-nearly-here.

Nevertheless IBM research scientists say that they could arrive in 10 to 30 year's time and could be used to defeat encryption methods used today. Therefore, banks and other organisations with lots of sensitive archived information need to prepare now and deploy new encryption algorithms designed to defeat quantum computer attacks.

Up the Khyber and into Star Trek

IIBM has designed a couple of algorithms based on two cryptographic primitives – Kyber, a secure key encapsulation mechanism, and Dilithium, a secure digital signature concept.

Lyubashevsky said these are "based on the hardness of mathematical problems that have been studied since the 1980s and have not succumbed to any algorithmic attacks, either classical or quantum."

Cyber and Dilithium are included in the CRYSTALS (Cryptographic Suite for Algebraic Lattices), developed by IBM in collaboration with several academic and commercial partners including ENS Lyon, Ruhr-Universität Bochum, Centrum Wiskunde & Informatica and Radboud University.

IBM has made CRYSTALS open source and submitted it to NIST for standardisation. It is also donating algorithms and support to a number of open source projects such as OpenQuantumSafe.org.

IBM TS1160 tape drive getting entangled in quantum computing.

The company said it has tested CRYSTALS successfully on a prototype IBM TS1160 tape drive using both Kyber and Dilithium in combination with symmetric AES-256 encryption, enabling what it calls the world's first quantum computing-safe tape drive.

Air gaps, attacks and cloud marketing

This is all very well but there are no attack-capable quantum computers and so the drive cannot be fully tested. Also since archive tapes are stored offline they are air gap-protected against malicious access attack.

Because of this, the idea of tape as a possible attack target seems odd – until we realise that the IBM mainframes used by banks will have IBM tape drives. Also, the IBM Cloud organisation is involved and tape is used for archiving data in its public cloud.

IBM will begin to provide quantum-safe cryptography services on the IBM public cloud in 2020. It will safeguard data in transit by enhancing TLS/SSL (Transport Layer Security/Secure Sockets Layer) implementations in its Cloud services using the CRYSTALS algorithms.

It is offering a 'Quantum Risk Assessmen't from IBM Security straight away. Read more in an IBM blog.