Secure Archives for the Quantum Era

Next generation algorithms set the stage for quantum-safe infrastructure, protecting data in-flight and at-rest.

Highlights

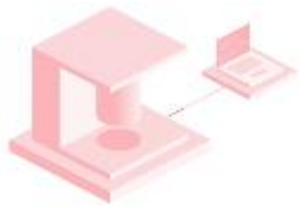
NIST announces Post-Quantum Cryptography Standard

IBM Tape demonstrates quantum-safe algorithm integration

IBM tape committed to secure data storage

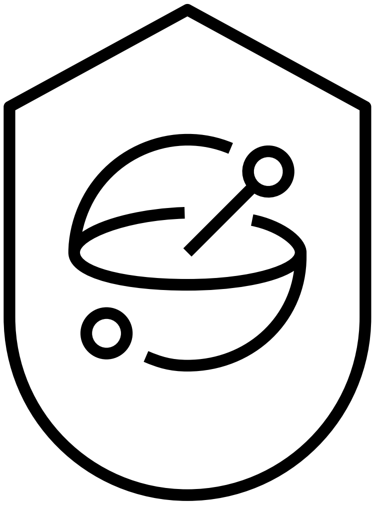
Quantum computers represent a significant threat to existing cryptographic algorithms. This quantum risk is encapsulated in Shor's Algorithm[1], which would allow a large-scale quantum computer to break all existing commonly used encryption protecting data transmissions over the internet. While quantum computers are nowhere near large enough to execute Shor's algorithm, the pace of advancement in qubits put quantum computers on track to be cryptanalytically relevant by the early 2030s.

IBM tape technology integrated hardware-based encryptions in 2004 based on NIST standards for strong encryption using AES-256 algorithm strength. AES-256 encryption technology is still relevant and cryptographically quantum-safe according to calculations made with Grovers algorithm[2]. IBM has been a key contributor to the next generation of encryption standards, developing two quantum resistant cryptographic primitives based on this work: KML-KEM[3], a secure key encapsulation mechanism and ML-DSA[4], a secure digital signature algorithm. These two algorithms make up the "Cryptographic Suite for Algebraic Lattices" we call "CRYSTALS"[5].



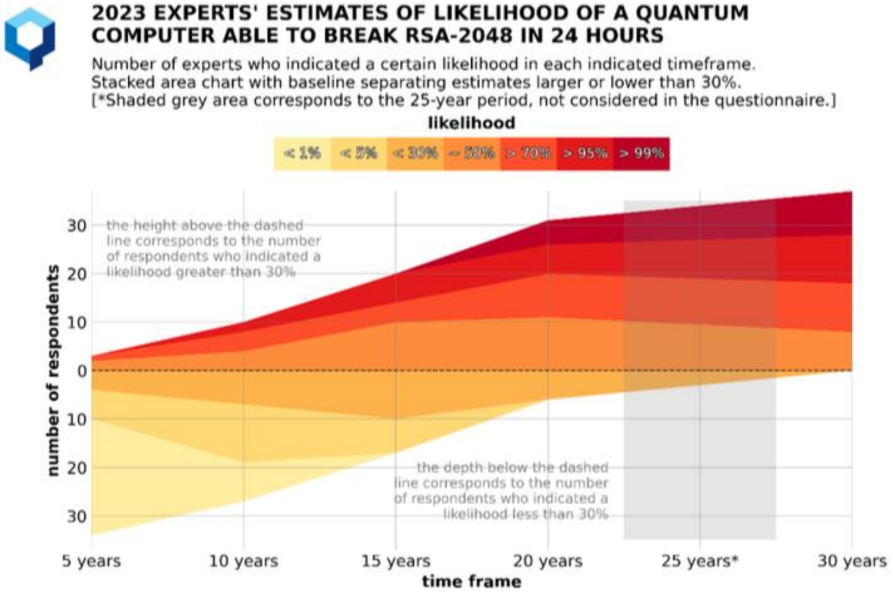
Next generation cryptography standardizes global data protection

On August 13th, 2024, NIST released the first 3 finalized post-quantum encryption standards[6]. The NIST announcement standardizes all qualified post-quantum cryptographic algorithms, setting the stage for implementation in modern IT infrastructure.



Quantum safe

While NIST has stated that post quantum cryptography (PQC) is not an immediate risk[7], IBM tape has taken significant steps to ensure the ability of the tape drive to utilize PQC algorithms.



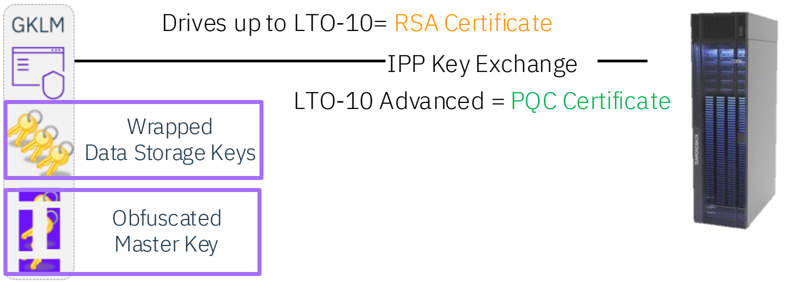
Quantum threat timeline[9]

In 2019, IBM published research on the IBM quantum computing-safe tape[8] drive prototype based on the IBM TS1160 tape drive and utilizing both ML-KEM and ML-DSA in combination with symmetric AES-256 encryption to enable the world's first quantum computing-safe tape drive. IBM tape drives have planned for the NIST standardization announcement of PQC algorithms and will implement the capability in future tape drives and firmware.

IBM tape continues to use the quantum safe AES-256 for encrypting all data on tape media. IBM tape is implementing PQC certificates for advanced security key exchange. IBM Proprietary Protocol is enabled using IBM tape library managed encryption and the IBM Guardium Key lifecycle Manager (GKLM) to securely conduct key exchange for data encryption on tape. This process involves ethernet connectivity of the IBM tape libraries to IBM GKLM using secure TLS creating a VPN like connection between the tape drive and GKLM. The Key exchange handshake requires certificate verification to create the trusted connection and packetization of the key exchange packets. PQC certificates protect the data from bad actors capturing packets and attempting to decrypt the packets using next generation quantum computers. This is part of advancing key lifecycle management and exchange in the larger security framework.

Key Exchange Process

- Unique Master Key per GKLM
- Master Key stored in GKLM Application
- Obfuscation hides Master Key
- All other keys encrypted (wrapped) under Master Key
- GKLM communicates with tape storage via IPP



Drives up to LTO-10= RSA Certificate

IPP Key Exchange

LTO-10 Advanced = PQC Certificate

Wrapped Data Storage Keys

Obfuscated Master Key

Implementation of PQC certificates for key exchange mechanisms is being implemented in LTO-10. To take advantage of the advanced security, clients will be required to update to a supporting version of LTO-10 tape drive code and a supporting GKLM version. Planning this upgrade must start with GKLM.

With the implementation 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 infrastructure.

For more information

To learn more about quantum safe infrastructure, contact your IBM representative or IBM Business Partner, or visit

https://www.ibm.com/quantum/quantum-safe

https://www.ibm.com/tape-storage

[1] https://epubs.siam.org/doi/10.1137/S0097539795293172

[2] https://en.wikipedia.org/wiki/Grover's_algorithm

[3] https://pq-crystals.org/kyber/index.shtml

[4] https://pq-crystals.org/dilithium/index.shtml

[5] https://pq-crystals.org/index.shtml

[6] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[7] https://www.youtube.com/watch?v=uE_Y1C4QPU8&t=72s

[8] https://research.ibm.com/blog/crystals-quantum-safe

[9] https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
June 2025

This document is current as of the initial date of publication and may be changed by IBM at any time.
Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.