SNIA STORAGE SECURITY SUMMIT

Wednesday, May 11, 2022 • Virtual

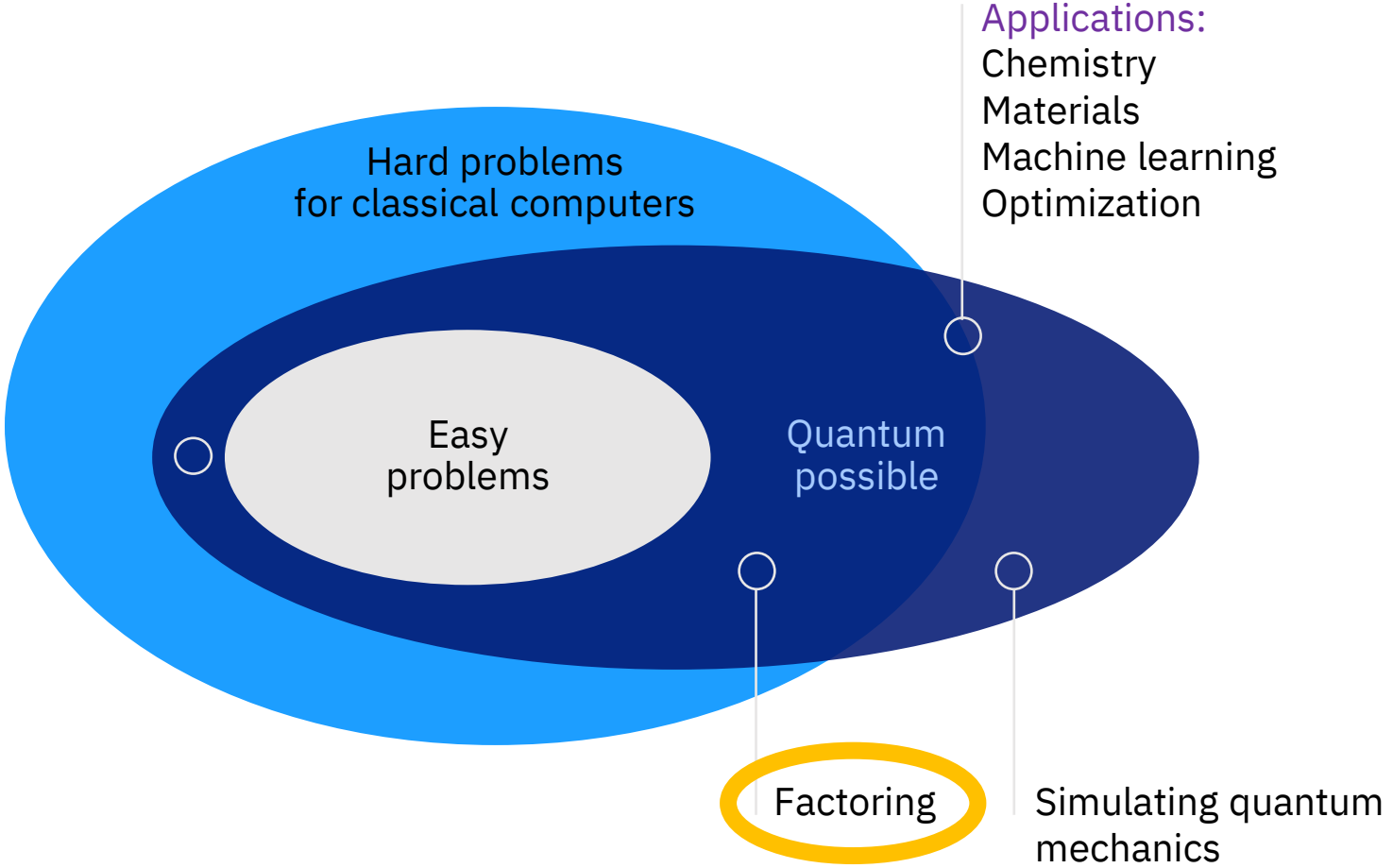
Quantum Safe Cryptography for Long Term Security

Basil Hess, IBM Research

A SNIA Event

Quantum Computing

Applications and risk



Quantum Risk

Quantum algorithms and impact on cryptography

- **Shor's** algorithm breaks many asymmetric Public Key Cryptography schemes based on factoring and DLP:
  - RSA, ECC, ECDH, ECDSA, EdDSA
- **Grover's** algorithm halves the security of symmetric algorithms:
  - AES, SHA 2, SHA 3

Factoring Algorithm (RSA)		EC Discrete logarithm (ECC)	
N bits	Approx #qubits	N bits	Approx #qubits
	2n		F'(n)
512	1024	110	700 (800)
1024	2048	163	1000 (1200)
2048	4096	224	1300 (1800)
3072	6144	256	2800 (3600)

- Quantum roadmaps become tangible
  - IBM Quantum Eagle with 127 qubit introduced in 2021
  - Roadmap: IBM Quantum Condor with 1121 qubit in 2023
- Significant progress on quantum algorithm efficiency

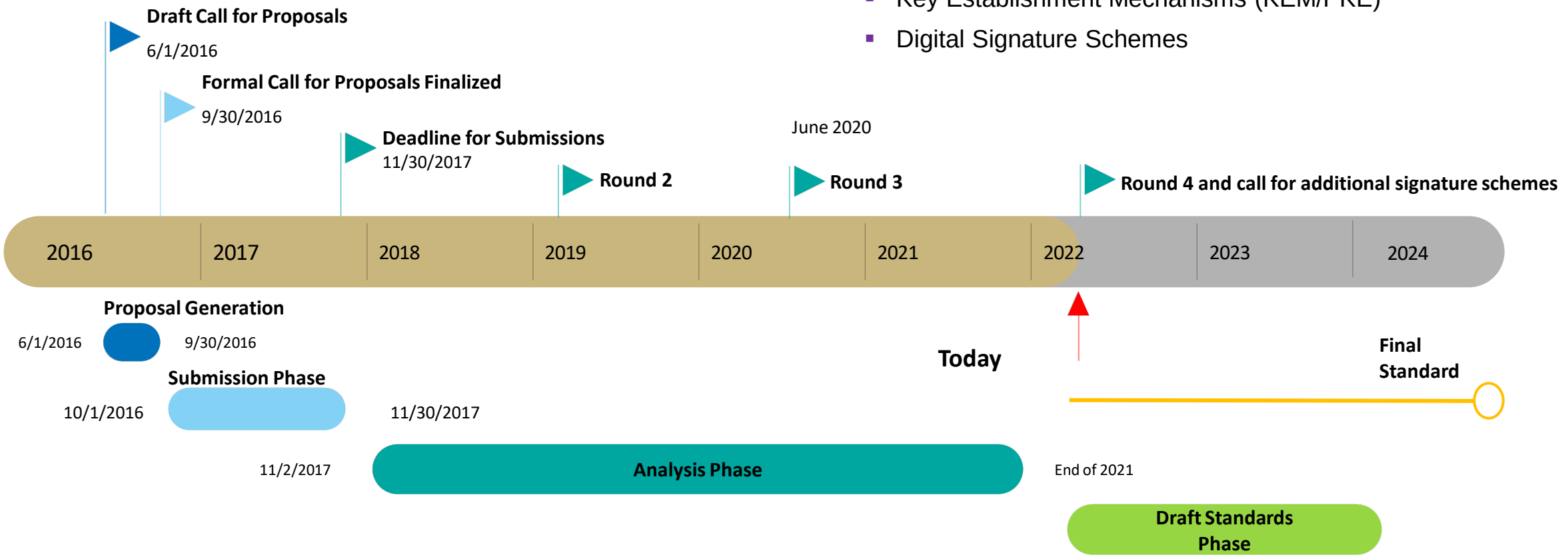
Quantum Safe Cryptography

NIST PQC Standardization

Cryptography based mathematical problems difficult for classical and quantum computers to solve efficiently.

Types of schemes to be standardized:

- Key Establishment Mechanisms (KEM/PKE)
- Digital Signature Schemes



https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization

Quantum Safe Cryptography

Standardization candidates (NIST PQC Round 3)

Finalists: some will be standardized after Round 3

KEMs
1. CRYSTALS–Kyber (Lattice)
2. Classic McEliece (Code)
3. NTRU (Lattice)
4. SABER (Lattice)

Signatures
1. CRYSTALS–Dilithium (Lattice)
2. FALCON (Lattice)
3. Rainbow (Multivariate)

Alternates: some may be standardized as backup or after a further round

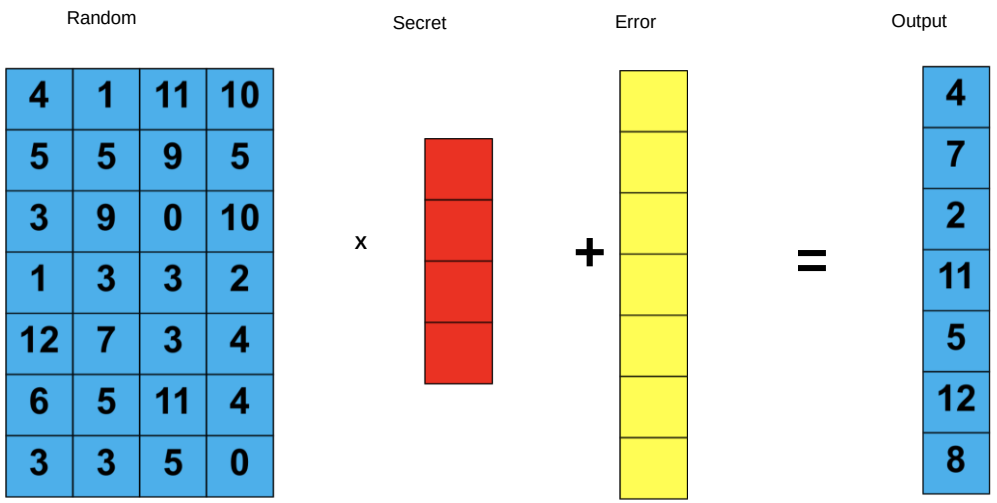
KEMs
1. BIKE (Code)
2. Frodo (Unstructured Lattice)
3. HQC (Code)
4. NTRU Prime (Lattice)
5. SIKE (Isogenies)

Signatures
1. GeMSS (Multivariate)
2. Picnic (Hash functions)
3. Sphincs+ (Hash functions)

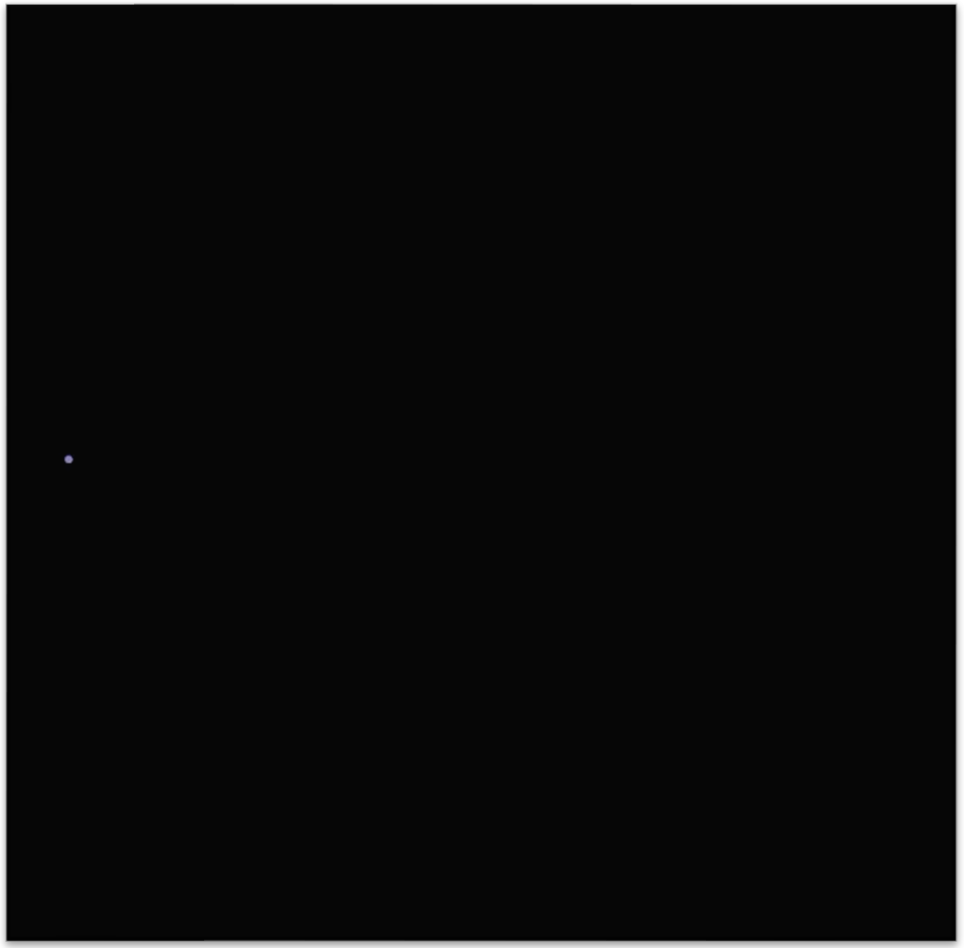
Quantum Safe Cryptography

Lattice cryptography

1 Allows us to formulate problems such as “given the blue matrix/vector find the red secret”



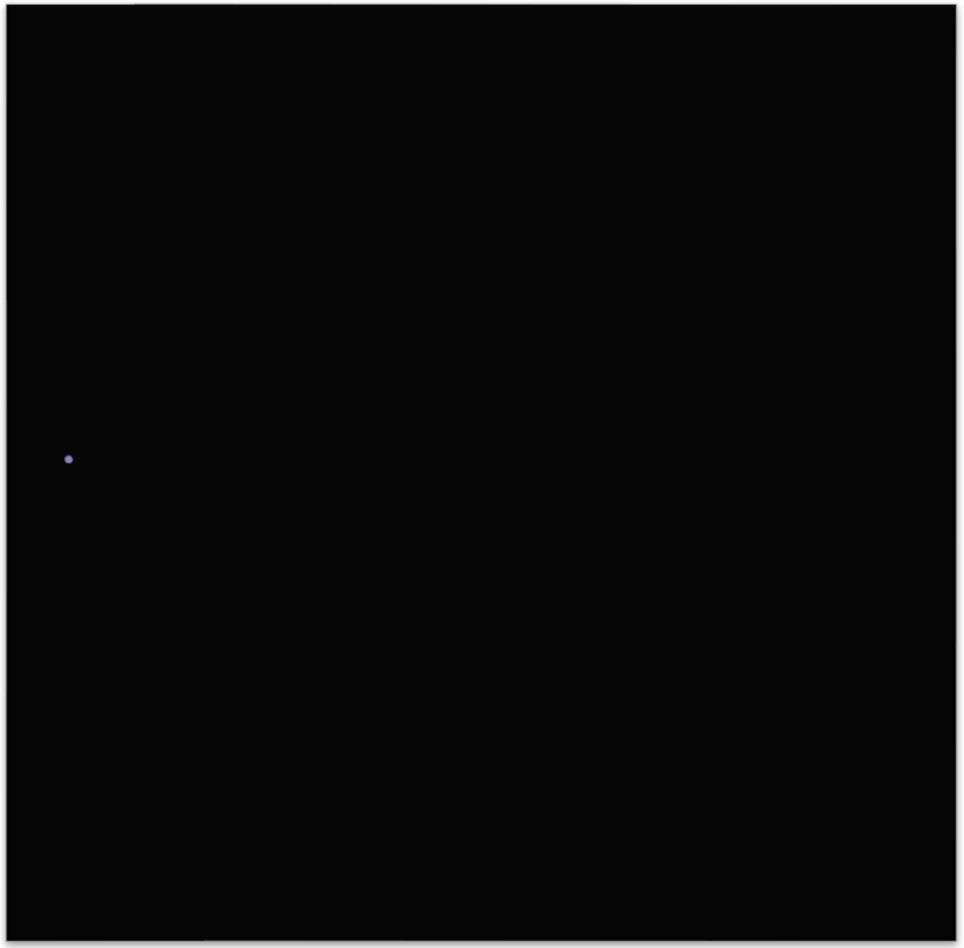
Learning with Errors (LWE) problem



Quantum Safe Cryptography

Lattice cryptography

1 Allows us to formulate problems such as “given the blue matrix/vector find the red secret”



Lattice cryptography combines many advantages for quantum safe cryptography:

- Very efficient and fast implementations
- Keys and Signatures larger than with classical cryptography – but not massively
- The least impact on protocols and applications that need to migrate
- A versatile building block for more complex cryptographic schemes, e.g. FHE

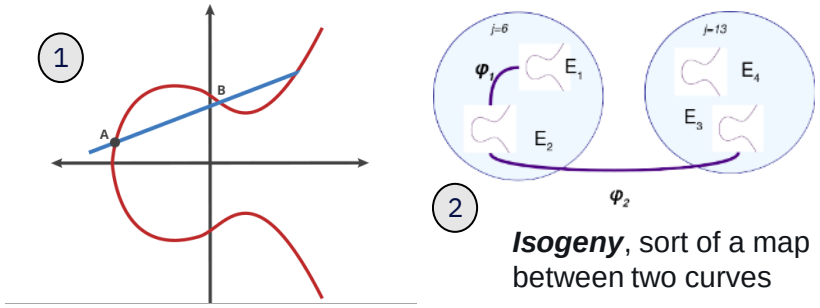
Quantum Safe Cryptography

Isogeny-based cryptography

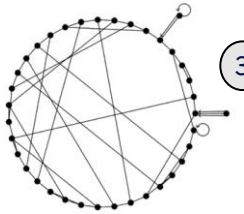
SIDH cryptography is interesting for several reasons:

- One of the few quantum safe schemes that allows a Diffie-Hellman type key exchange
- Operation based on well known elliptic curve functions
- Public keys are very small (but the performance is still relatively slow)
- KEM Submitted to NIST PQC, recent research shows feasibility to construct signature scheme
- Interesting for certain networks – for example high latency

The set of points on the elliptic curve is closed under addition (Groups) ($E: y^2 = x^3 + ax + b$)

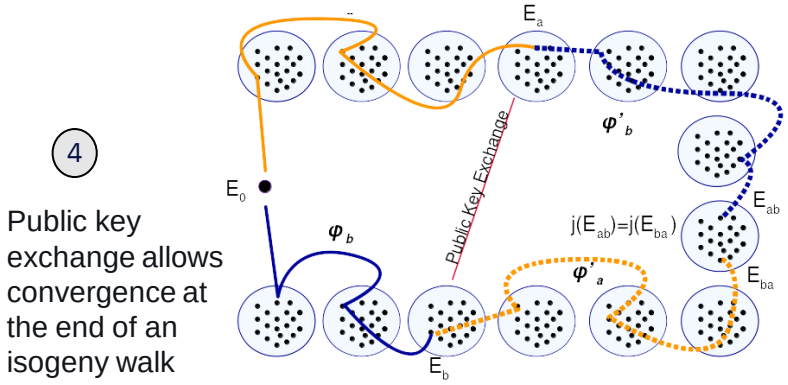


Isogeny, sort of a map between two curves



3

Supersingular isogeny: fully connected vertices but with variable number of isogenies. (Allows random walks between vertices)



Public key exchange allows convergence at the end of an isogeny walk

Quantum Safe Cryptography

Summary and outlook

- Final phase of the NIST PQC Standardization: Standards expected in 2022-2024
- We will see more than one algorithm standardized, based on different hard mathematical problems

Quantum safe research beyond NIST PQC:

- Non-interactive key exchange (NIKE)
- Password-authenticated key exchange (PAKE)
- Zero Knowledge Proofs (ZKP)
- Threshold Signatures
- Blind Signatures
- Fully Homomorphic Encryption (FHE)

Quantum Safe Migration

Overview and Examples

Quantum Safe Migration

Milestones

1	2	3	4
Discover and classify data	Inventory of cryptography	Crypto agility	Quantum safe

Increasing focus on QSC migration:

- **White house memo from Jan 2022 requires US federal agencies to begin quantum-safe modernization planning.**
- **SP 800-56C Rev. 2 (2020) allows the use of hybrid key-establishment with FIPS modules.**
- **BSI (Germany) and ANSSI (France) recommend the use of hybrid cryptography for high security applications.**

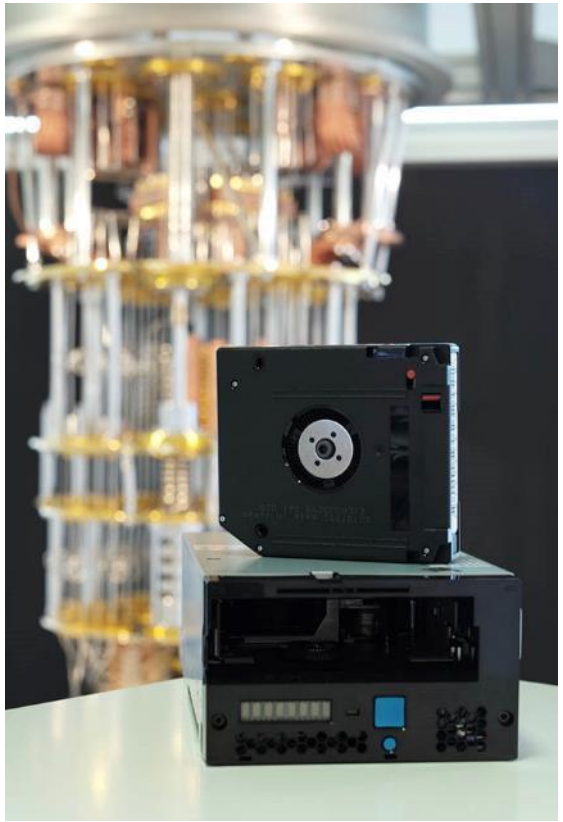
Quantum Safe Migration Example: Tape

Data: Tape systems used to store data of periods up to decades

Crypto inventory: Combination of asymmetric and symmetric cryptography

- Asymmetric cryptography for key establishment, e.g. with KMIP, and for firmware verification
- Symmetric cryptography for data encryption

Quantum safe cryptography allows to security for long-term confidential data

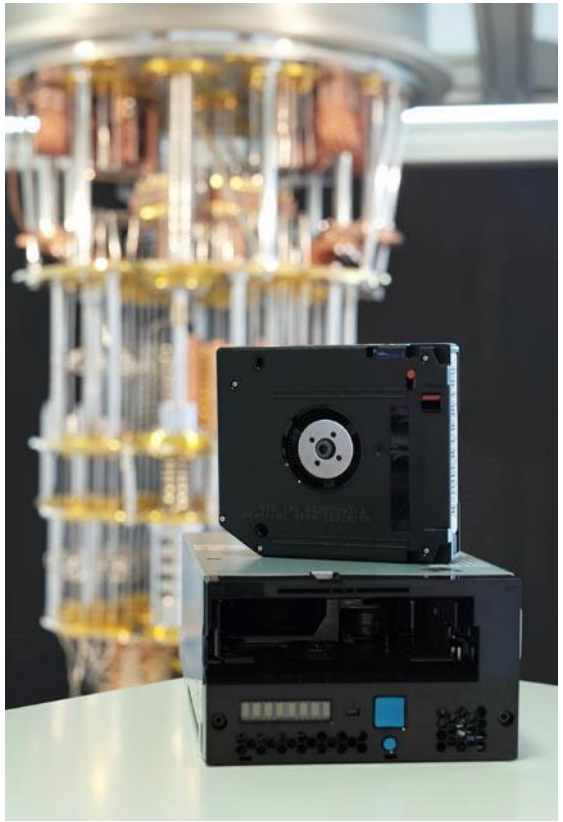


Quantum Safe Migration Example: Tape

In 2019, IBM announced a prototype of the world's first quantum safe tape drive. Implemented in firmware of TS1160 tape drive.

Uses lattice-based cryptography:

- CRYSTALS-Kyber for secure key transport between tape drive and key manager
- CRYSTALS-Dilithium signatures for authentication and firmware verification
- Data encryption on tape with AES256



Thank you!

