Post Quantum Cryptography

Quantum Computing ≠ Post Quantum Cryptography

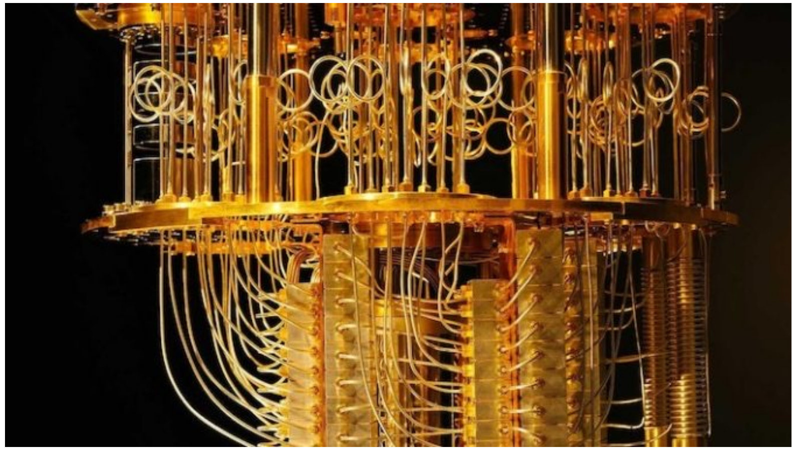
Ing. Miloš Soukup

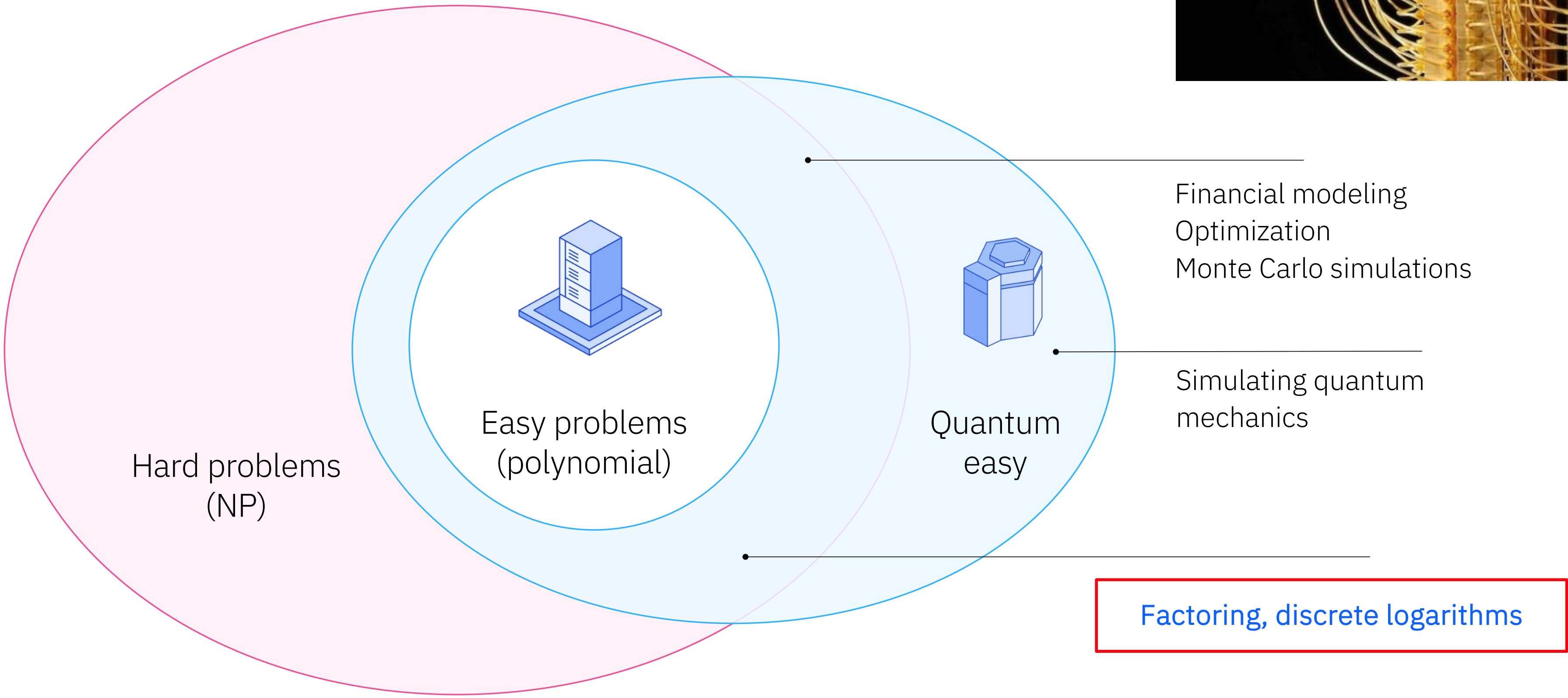
milos.soukup@ibm.com

Quantum Ambassador

Business Technology Leader

What is Quantum able to solve ?





Today's classical security protocols will be obsolete tomorrow

Prime factors	2048-bit composite integer	Expected computation time
= p x q	25195908475657893494027183240048398571429282126204032027777137836043662020707595556264018525880784406918290641249515082189298559149176184502808489120072844992687392807287776735971418347270261896375014971824691165077613379859095700097330459748808428401797429100642458691817195118746121515172654632282216869987549182422433637259085141865462043576798423387184774447920739934236584823824281198163815010674810451660377306056201619676256133844143603833904414952634432190114657544454178424020924616515723350778707749817125772467962926386356373289912154831438167899885040445364023527381951378636564391212010397122822120720357	The most powerful computer today: **Millions of years** Shor's quantum algorithm: **Hours**

Public key encryption • Digital signatures • Key exchange algorithms

RSA • DSA • ECC • ECDSA • DH

Improvements in last 5 years

Quantum Computers
1000 x QPU

2000x Speed (40k CLOPS)

Error Correction
1000x improved

Qiskit 1.x – 5x quicker running
16x quicker transpiling

Shor Algorithm
R&D

1000x less Qbits

Dramatic speed up from Shor

	Abstract Qubits	Measurement Depth	Toffoli+T/2 Count	Toffoli+T/2 Count (billions)			Min Volume (megaqubitdays)		
Factoring RSA integers	Asymptotic			$n = 1024$	$n = 2048$	$n = 3072$	$n = 1024$	$n = 2048$	$n = 3072$
Vedral et al. 1996 [87]	$7n + 1$	$80n^3 + O(n^2)$	$80n^3 + O(n^2)$	86	690	2300	240	4100	23000
Zalka 1998 (basic) [90]	$3n + O(1)$	$12n^3 + O(n)$	$12n^3 + O(n^2)$	13	100	350	16	250	1400
Zalka 1998 (log add) [90]	$5n + O(1)$	$600n^2 + O(n)$	$52n^3 + O(n^2)$	56	450	1500	16	160	540
Zalka 1998 (fft mult) [90]	$\approx 96n$	$\approx 2^{17}n^{1.2}$	$\approx 2^{17}n^2$	140	550	1200	62	260	710
Beauregard 2002 [6]	$2n + 3$	$144n^3 \lg n + O(n^2 \lg n)$	$576n^3 \lg^2 n + O(n^3 \lg n)$	62000	600000	2200000	32000	380000	1700000
Fowler et al. 2012 [28]	$3n + O(1)$	$40n^3 + O(n^2)$	$40n^3 + O(n^2)$	43	340	1200	53	850	4600
Häner et al. 2016 [42]	$2n + 2$	$52n^3 + O(n^2)$	$64n^3 \lg n + O(n^3)$	580	5200	19000	230	2800	13000
(ours) 2019	$\mathbf{3n + 0.002n \lg n}$	$\mathbf{500n^2 + n^2 \lg n}$	$\mathbf{0.3n^3 + 0.0005n^3 \lg n}$	**0.4**	**2.7**	**9.9**	**0.5**	**5.9**	**21**
Solving elliptic curve DLPs	Asymptotic			$n = 160$	$n = 224$	$n = 256$	$n = 160$	$n = 224$	$n = 256$
Roetteler et al. 2017 [74]	$9n + O(\lg n)$	$448n^3 \lg n + 4090n^3$	$448n^3 \lg n + 4090n^3$	30	84	130	13	52	83

Table 1: Expected costs of factoring n bit RSA integers using various constructions proposed in the literature.

https://quantum-journal.org/papers/q-2021-04-15-433/pdf/

10.1.2023

Forbes

FORBES > BUSINESS > POLICY

Did China Break The Quantum Barrier?

Arthur Herman Former Contributor

I comment on quantum computing and AI, and American national security.

Jan 10, 2023, 09:01am EST

BEIJING, Dec. 4, 2020 — A research team including Chinese quantum physicist Pan Jianwei established ...

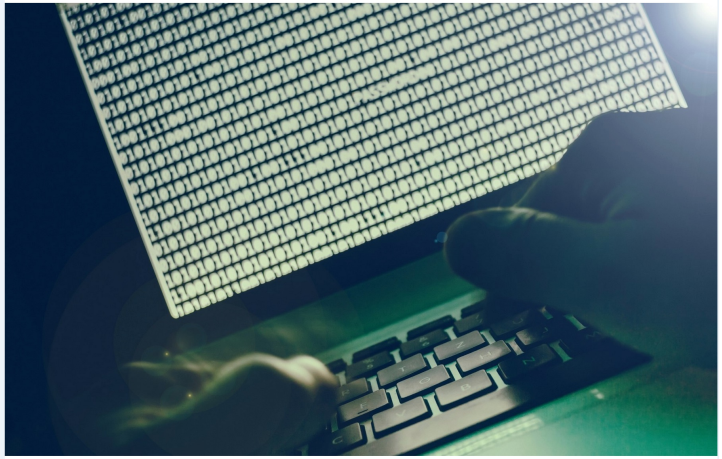
[+] XINHUA NEWS AGENCY/GETTY IMAGES

https://www.forbes.com/sites/arthurherman/2023/01/10/did-china-break-the-quantum-barrier/

11.10.2024

Chinese Scientists Report Using Quantum Computer To Hack Military-Grade Encryption

National, Quantum Computing Business, Research   Matt Swayne • October 11, 2024



Insider Brief

- Chinese researchers, using a D-Wave quantum computer, claim to have executed what they are calling the first successful quantum attack on widely used encryption algorithms, posing a "real and substantial threat" to sectors like banking and the military, as reported by SCMP.
- The D-Wave Advantage, initially designed for non-cryptographic applications, was used to breach SPN-structured algorithms but has not yet cracked specific passcodes, highlighting the early-stage nature of this threat.
- Despite the advance, the researchers acknowledge limitations such as environmental interference, underdeveloped hardware and the inability to develop a single attack method for multiple encryption systems still hinder quantum computing's full cryptographic potential.

https://thequantuminsider.com/2024/10/11/chinese-scientists-report-using-quantum-computer-to-hack-military-grade-encryption/

The Quantum Risk is real

Don’t panic but act

AI Generated 15.10.2024 Martin Svik

What can a cybercriminal do TODAY ?

Harvest now, decrypt later

Availability of “cryptographically relevant” quantum computers

Before

After

Harvest confidential data to decrypt later

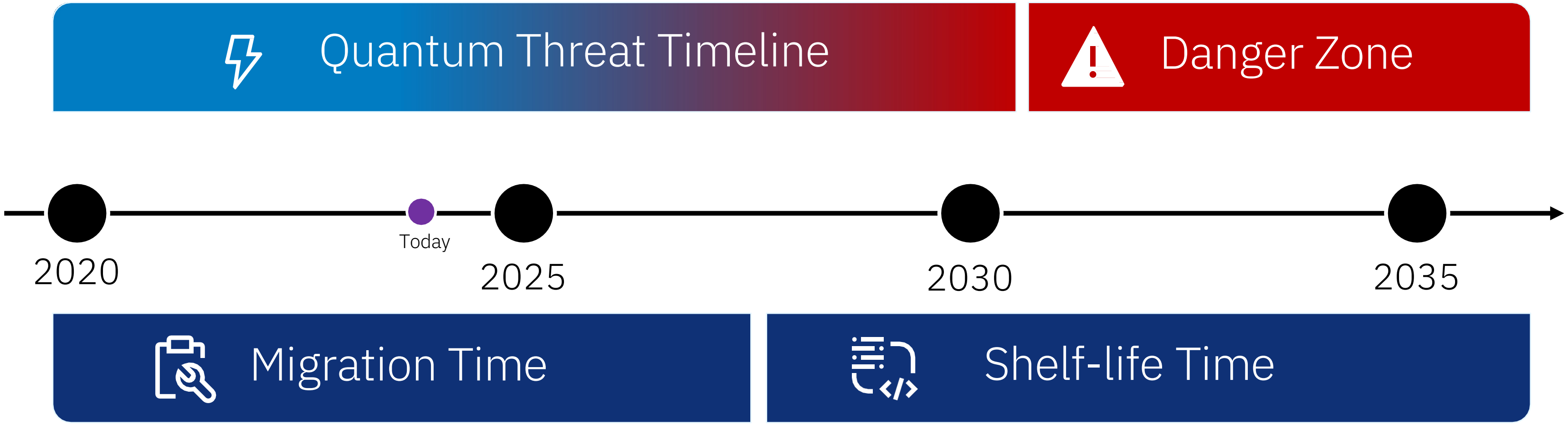
Decrypt lost or harvested confidential data by breaking encryption

Disrupt business with manipulation through fraudulent authentication

Manipulate digitally signed contracts and legal history by forging digital signatures

When will the quantum threat materialize?

For data that will requires long term protection, the threat is today. The impact is in the future



"The precise threat timeline you should focus on depends on your risk tolerance. For very critical systems and assets, the likelihood of quantum attacks in five years is becoming material and for most critical systems and assets I believe the 10-year likelihood needs to be addressed assertively."
Dr. Michele Mosca, University of Waterloo,Canada

"Experience has shown that, in the best case, *5 to 15 or more years* following the publication of quantum-resistant public-key cryptographic standards *will still be required to implement those standards*"
National Cybersecurity Center of Excellence (NCCoE)

Types of cryptography

Symmetric

Encryption key =

Decryption key =

- Alice and Bob share a **single secret key**
- The same key is used to encrypt and decrypt messages
- Needs a way to share keys securely—an N^2 problem
- Enigma, Data Encryption Standard (DES), Advanced Encryption Standard (AES)

Asymmetric

Private key =

Public key =

- Alice has a **public key** that Bob uses to encrypt messages
- Alice uses her **private key** to decrypt Bob's messages
- Allows digital **signature**
- Solves key **exchange**
- Relies on a **trapdoor** function
- The basis of internet security
- Non-Secret Encryption, RSA, Diffie-Hellman, elliptic curve, digital signature algorithm (DSA), Kyber

One-time pad

Encryption key =

Decryption key =

- Basis of Shannon's theory of secrecy
- Perfect secrecy
- **Private key** is same length as message; must **never** be reused
- Used for diplomatic communications
- Needs a way to create and distribute keys
- Couriers hand-carry KEYMAT
- SIGSALY, Floradora, Venona

Hashing

No encryption or decryption key

- Bob wants to verify the **integrity** of a sent message
- Alice uses a hash function (a **one-way** function) to create a fixed **fingerprint** of the message
- Bob can recalculate the fingerprint; the slightest change to the message would change the fingerprint
- No encryption key is used when applying a hash function (but see 'stateful' hash)
- MD5, SHA-1, SHA-2, SHA-3, XMSS/LMS

The Challenge

Modern **financial services world depends on cryptography**

Various Crypto Schemes in FSS depending on Public Key Cryptography

Online Transactions:

Public key cryptography ensures the confidentiality and integrity of sensitive data, such as credit card information and personal identification numbers (PINs).

Digital Signatures:

Public key cryptography enables the use of digital signatures in financial services. Digital signatures provide a way to verify the authenticity and integrity of digital documents, such as contracts and financial statements, ensuring they have not been tampered with during transmission.

Communication Channels:

Public key cryptography ensures that data exchanged between parties, such as account information and transaction details, is protected from eavesdropping and tampering.

Mobile Banking:

Public key cryptography enables secure communication between mobile devices and banking servers, ensuring that sensitive financial data transmitted over mobile networks is encrypted and protected.

Two-Factor Authentication (2FA):

Public key cryptography enhances security by requiring users to provide two different types of authentication factors, such as a password and a digital certificate, to access their accounts.

Secure Key Exchange:

Public key cryptography enable two parties to establish a shared secret key over an insecure channel, ensuring that subsequent communication is encrypted and secure.

ATM Transactions:

Public key cryptography ensures that data exchanged between the ATM and the banking network is encrypted, protecting users' PINs and transaction details from unauthorized access.

Fund Transfers:

Public key cryptography ensures that sensitive financial information, such as account numbers and transaction details, is encrypted and protected during transit.

Financial Data Storage:

Public key cryptography is employed in securing financial data stored in databases and servers. It enables encryption and decryption of sensitive data, protecting it from unauthorized access in case of a data breach

The Challenge

Modern **telco world depends on cryptography**

Various Crypto Schemes in Telcos depending on Public Key Cryptography

5G Network Access:

Public key cryptography ensures the confidentiality and integrity of data transmitted over the network, protecting against unauthorized access and tampering.

Subscriber Authentication:

Public key cryptography enables secure authentication of subscribers, ensuring that only authorized users can access the network and services.

Network Slicing:

Public key cryptography helps establish secure communication channels between network slices, ensuring isolation and confidentiality of data transmitted between different slices.

IoT Connectivity:

Public key cryptography enables the authentication and secure communication between IoT devices and the network, protecting against unauthorized access and data breaches.

Network Function Virtualization (NFV):

Public key cryptography helps establish secure connections between virtualized network functions, ensuring the integrity and confidentiality of data transmitted between them.

Mobile Edge Computing (MEC):

Public key cryptography enables secure communication between edge computing nodes, ensuring the confidentiality and integrity of data processed at the network edge.

Network Management:

Public key cryptography ensures that network management operations and communications are encrypted and protected from unauthorized access.

Over-the-Air (OTA) Updates:

Public key cryptography enables secure and authenticated updates, ensuring that only authorized updates are installed, and protecting against tampering and unauthorized modifications.

Billing and Payment Systems:

Public key cryptography ensures the integrity and confidentiality of billing information and protects against fraudulent transactions.

Roaming and Interconnection:

Public key cryptography helps establish secure connections between networks, ensuring the confidentiality and integrity of data exchanged during roaming and interconnection.

Launching the era of quantum safe

We are here

2016

Submission to NIST

Lattice-based cryptography
Code-based cryptography
Isogeny-based cryptography

2019

IBM Infrastructure

Quantum-safe
tape announcement

2020

IBM open source announcement: Open Quantum Safe (OQS)

2021

IBM Cloud

Availability of quantum-safe algorithms and communication

2022

NIST algorithm announcement

→ CRYSTALS-Kyber
→ CRYSTALS-Dilithium

→ Falcon
→ SPHINCS+

GSMA, IBM, and Vodafone establish Post-Quantum Telco Network Taskforce

→ NGMN, 6G, ODIN

IBM z16

First quantum-safe platform

2023

IBM Quantum Safe

Roadmap, technology, and services announced

NIST "on-ramps" digital signatures submission

→ UOV
→ MAYO
→ SQIsign

2024

NIST quantum-safe standards

→ 203 ML-KEM
→ 204 ML-DSA
→ 205 SLH-DSA
206 FN-DSA (Draft)

2024+ Round 4:
→ BIKE, Classic McEliece, HQC

NIST Post Quantum Cryptography Process

ML-KEM, FIPS 203

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Designed for encrypting the keys used to set up secure communication (e.g. website). Based on the CRYSTALS-Kyber submission.

NIST recommends as **key encapsulation** algorithm.

ML-DSA, FIPS 204

Module-Lattice-Based Digital Signature Standard

Designed to protect the digital signatures used when signing documents remotely. Based on the CRYSTALS-Dilithium submission.

NIST recommends as **primary signature** algorithm.

SLH-DSA, FIPS 205

Stateless Hash-Based Digital Signature Standard

(Also) designed to protect the digital signatures used when signing documents remotely. Different performance characteristics. Based on the SPHINCS+ submission.

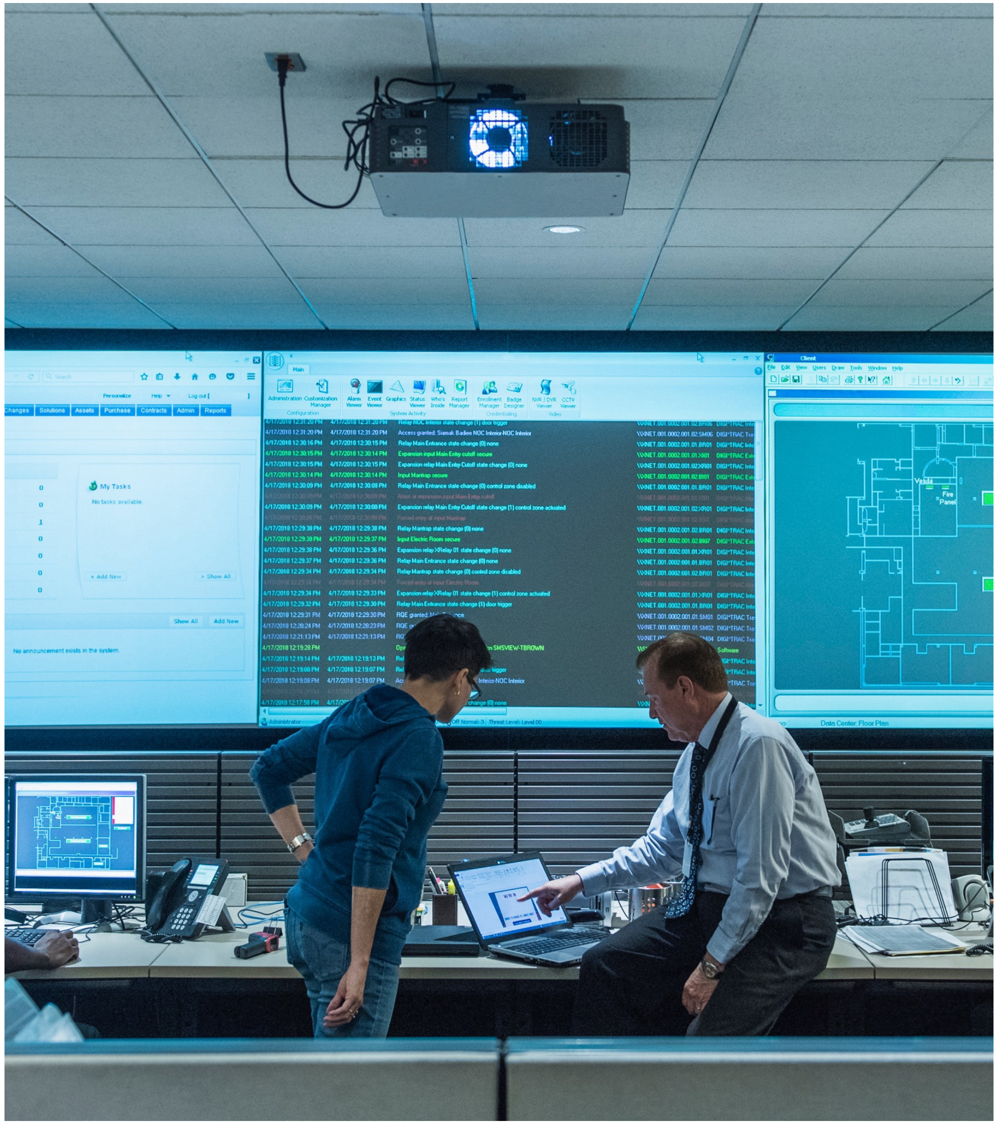
FN-DSA, Draft FIPS 206

FFT over NTRU Lattice based Digital Signature

(Also) designed to protect the digital signatures used when signing documents remotely. Different performance characteristics. Based on the FALCON submission

Later timeline for standardization than FIPS 203/4/5

Cryptography in the enterprise



IBM **Quantum** Safe Roadmap

First generation available · On target · Planned

	2022	2023	2024	2025	2026+
Regulatory milestones	NIST selects algorithms for standardization	Federal agencies plan for PQC adoption	NIST publishes PQC standards	CNSA 2.0: preference to PQC-compliant vendors	Vendors complete transition to PQC
Consortia	Open Quantum Safe (OQS) Post-Quantum Telco Network	NCCoE PQC Coalition (MITRE)	Payments (EPAA, NACHA) PQC Alliance (Linux Foundation)	Critical Infrastructure Protection Coalition	
IBM services		Quantum-safe preparation & advisory	Application modernization Platform modernization	Security platform modernization	Quantum-safe talent transformation
IBM Quantum Safe technology: **IBM Quantum Safe Remediator** — *Transform*			Adaptive Proxy Performance benchmarking TLS, VPN, SSH	Crypto-agility framework Encryption Key/certificate management	Automated remediation LLM-based recommendation
IBM Quantum Safe technology: **IBM Guardium Quantum Safe** — *Observe*			Dynamic scan Cryptographic inventory Cryptographic posture mgmt	Risk-based prioritization Enriched metadata	AI-driven risk analysis
IBM Quantum Safe technology: **IBM Quantum Safe Explorer** — *Discover*		Static scan CBOM generation CI/CD integration	Custom library support Remediation recommendation	LLM-assisted scanning	
Algorithms, protocols, standards, libraries	Key encryption: CRYSTALS - Kyber Digital signature: CRYSTALS - Dilithium, FALCON	Cryptography Bill of Materials (CBOM)	MAYO, UOV, SQISign OpenSSL		
IBM infrastructure		IBM z16, IBM Hyper Protect Crypto Services, IBM Tape Storage, Hardware Security Modules (HSM)	IBM Cloud, IBM Software, Red Hat, IBM Storage, IBM Power		

IBM is ahead of competition and dominating in Quantum

- Quantum safe consultancy
  - Quantum Safe Assessment (Expert Labs D partn number to ELA, Research, Consulting)
- Quantum Safe Software
  - Quantum Safe Explorer
  - Quantum Safe Remediator
  - Quantum Safe Posture Management
  - Guardium Quantum Safe
  - Datapower PQC Gateway / appliance

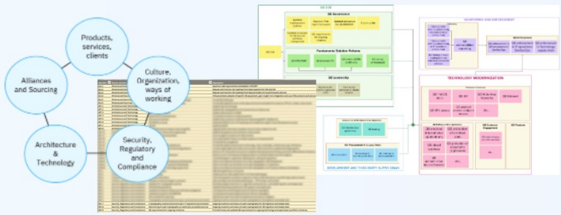
- Quantum Safe Hardware
  - Z16 + CX8 cryptocard 4770 – Linux ONE – First full end to end Quant safe system – 11/2023
  - Power 10/11 + 4770 CX8 – Tech Preview - NCEE only
  - Quantum Safe Storage – Flash FCM4
  - Quantum Safe Cloud – Bring your own key – Crypto services

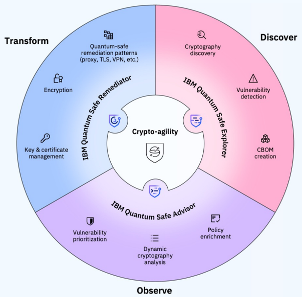
- Quantum Safe – Cryptoagility – best practices – How to develop crypto agile apps
  - Automation Brand – Application Server, Team Concert

Quantum Safe Assessment - Approach

IBM **Quantum**

Understand the situation → Define the target state & Plan QS Journey → Execute transformation





PoC → MVPs → Deploy at Scale

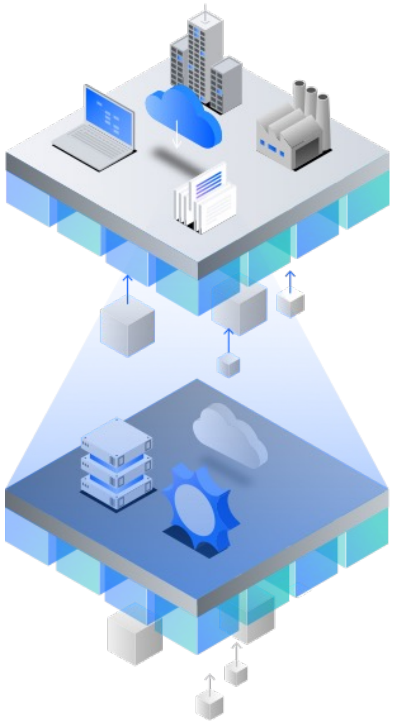
Quantum safe: enterprise baseline

Observe cryptography across the network

Operational cryptographic posture

Key/certificate management (PKI, CA)

Software development Cryptographic posture



Remediate cryptography

Discover cryptography in source repos

New capabilities

- Cryptographic agility
- Observability
- Automation
- Skills
- Maturity

Ecosystem impact

- Customers
- Technology suppliers
- Service providers

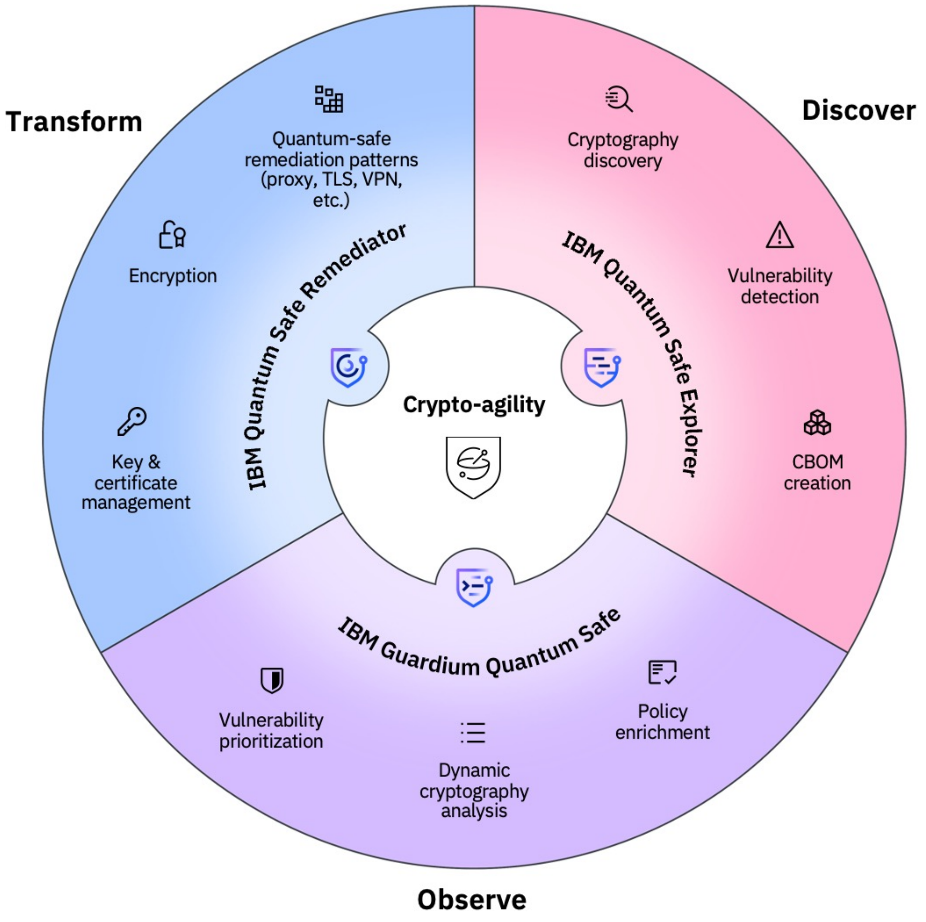
- Regulators
- Industry groups
- Standardization bodies
- Open-source community

IBM Quantum Safe technology

Explorer: Scan applications to locate cryptographic artifacts and vulnerabilities. Create various cryptographic inventory reports, including a cryptography bill of materials (CBOM).

Guardium Quantum Safe: Perform dynamic cryptography analysis to evaluate cryptographic posture and compliance. Leverage risk assessment to prioritize vulnerabilities for quantum-safe transformation.

Remediator: Learn and apply best practices for quantum-safe remediation patterns. Implement scalable and automated quantum-safe solutions to establish cryptographic agility



Quantum-safe technology and key management services were developed to help protect data and keys against a potential future quantum attack like harvest now, decrypt later

IBM z16 and Power 11/10 (NCEE Quantum iLAB NCEE prepared Tech preview)

Quantum-Safe System

Industry first quantum-safe system protected by quantum-safe technologies through multiple layers of firmware

Helps protect IBM z16 firmware from quantum attacks through a built-in dual signature scheme with no changes required

Crypto Express 8s

Protect Sensitive Data

New Crypto Express card with quantum-safe APIs to modernize existing and build new applications leveraging quantum-safe cryptography along with classical cryptography

Create Crypto Inventory

Discover where and what crypto is used in applications to aid in developing a crypto inventory for migration and modernization planning

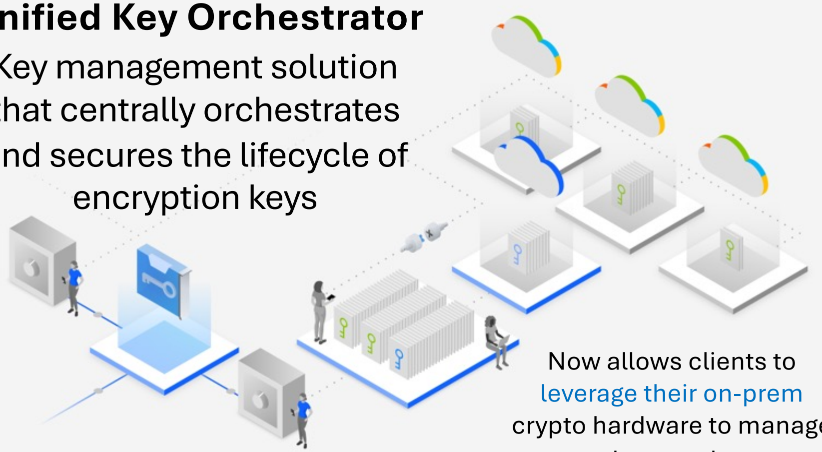
New crypto discovery features in IBM Application Discovery and Delivery Intelligence (ADDI) to analyze COBOL source code and discover crypto usage in applications.

Unified Key Orchestrator for Containers

After z/OS and IBM Cloud, now available on LinuxONE & Linux on Z

Unified Key Orchestrator

Key management solution that centrally orchestrates and secures the lifecycle of encryption keys



Now allows clients to leverage their on-prem crypto hardware to manage and secure keys.

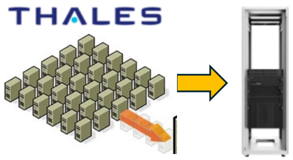
Starter Bundle

UKO for Containers	4 VPCs ($10K OTC + $2.5K S&S list price / VPC)
OCP	Single node clusters for 4 IFLs
LinuxONE 4 Express*	4 IFLs and 384 GB Memory
Security Leader Package	2 Crypto Express8S, TKE, cards and card readers

* Alternatively, can add 4 IFLs to existing Z / LinuxONE

Use cases

- Multicloud Key Management
  (serving AWS, Azure, GCP, IBM Cloud)
- z/OS Key Management
  (combined with UKO for z/OS)
- Enterprise Encryption Consolidation with ACSP (e.g. serving x86 and IBM Power on-prem)



all leveraging on-prem keys for data sovereignty

ACSP "Bridge" from aaS to Product

- ACSP is currently offered as a service
- Plan to add ACSP as priced feature of UKO in 1H25
- Can sell now and offer clients a "bridge" to convert from service to product
  - Term license at same S&S ($2.5K per VPC)
  - Unlimited license at $10K OTC + $2.5K S&S per VPC

IBM DataPower as PQC Gateway

IBM DataPower Gateway at a glance:

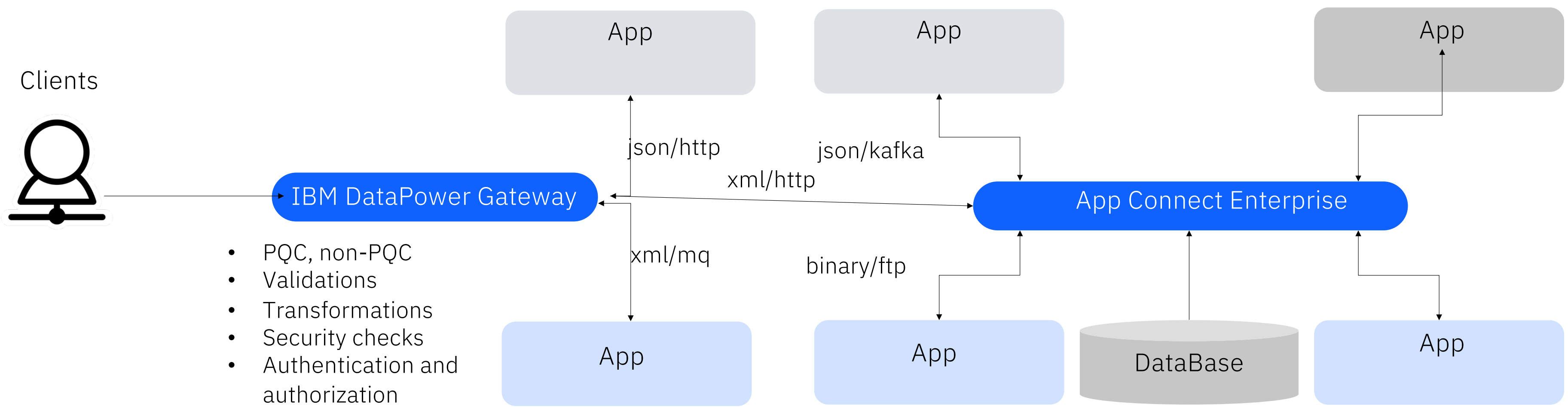
- Leading API, Application and Security gateway
- 2000+ clients
- Extremely reliable, performant and secure (specialized OS, no java, advanced security features, etc.)
- Container, virtual machine or physical appliance **(Security people love it!)**

Key use-cases:

- API Gateway (API Management)
- Application protection (eg. OWASP Top 10)
- Multi-protocol Gateway
- XMl/JSON offloading

DataPower as PQC Gateway:

- Single gateway for classical and PQC crypto algorithms
- Support PQC algorithms such as ML-KEM-512, ML-KEM-768 and ML-KEM-1024
- Encryption/decryption for both client (client to DataPower) and server (DataPower to backend) connections



- PQC, non-PQC
- Validations
- Transformations
- Security checks
- Authentication and authorization
- SLA

Read more: https://community.ibm.com/community/user/integration/blogs/matt-roberts1/2025/02/13/ibm-datapower-pqc

Infrastructure as Code for Quantum Safe applications

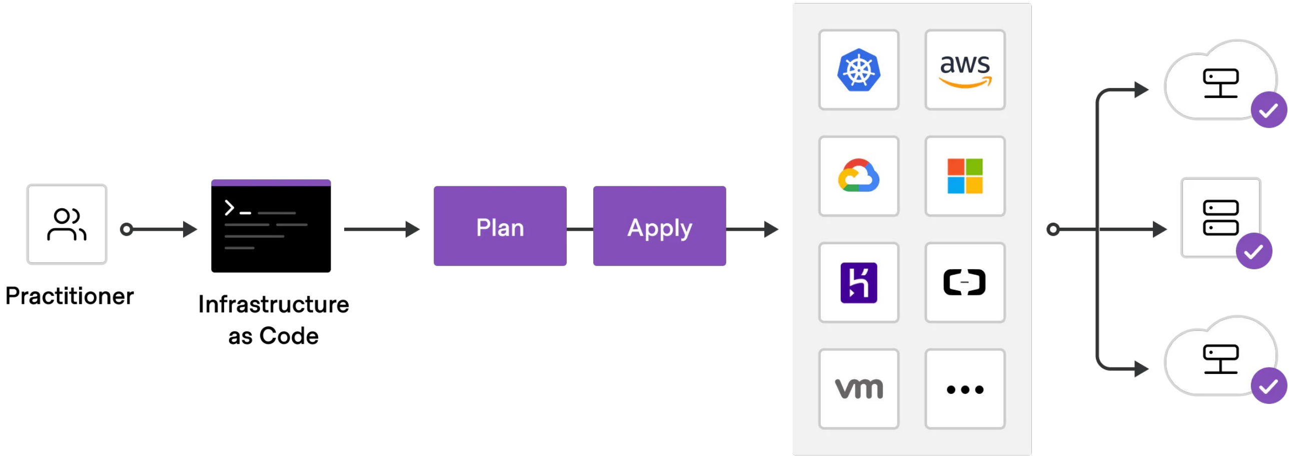
Infrastructure as Code for Quantum Safe applications is important for:

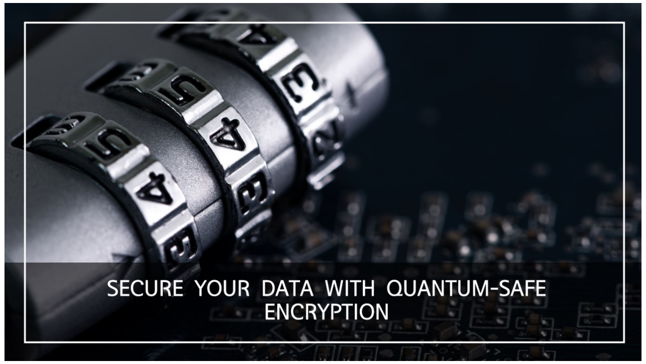
1. Infrastructure Management - Quantum-safe applications may require specialized hardware or cloud environments to operate. Terraform can automate the provisioning of these environments, ensuring consistency, repeatability, and scalability.

2. Integration with security tools - as organizations begin to adopt PQC, Terraform can help integrate these new tools and libraries into the infrastructure. This could include setting up secure communication channels or configuring cloud services with quantum-resistant algorithms.

3. Scalability - Quantum-safe applications might need to scale rapidly to handle large datasets or increased computational demands. Terraform allows you to define scalable infrastructure, making it easier to respond to these demands without manual intervention.

4. Consistency across environments - Quantum-safe applications may need to run across multiple environments (development, testing, production). Terraform ensures that these environments are consistent, which is crucial for maintaining the integrity of quantum-safe algorithms.

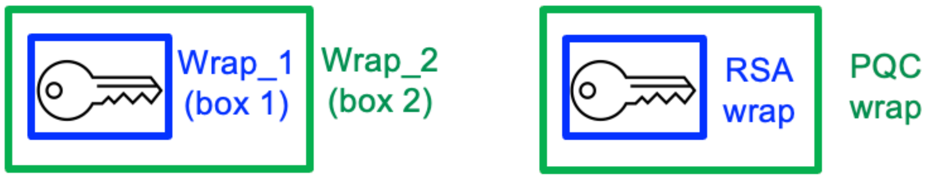


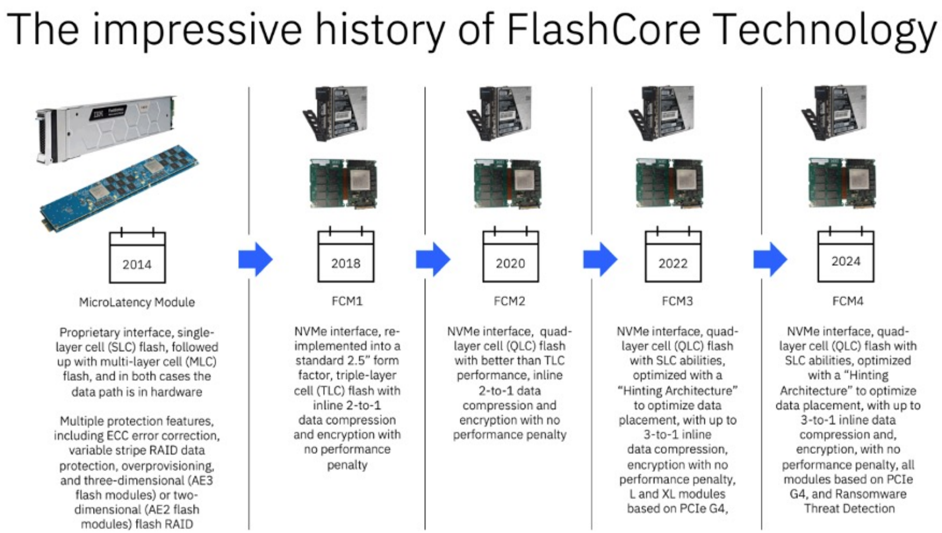


FlashCore FCM4, the world’s first quantum-safe, self-encrypting custom flash module.

As IBM developed its next-generation custom flash module, FCM4, it chose to make it quantum-safe, by replacing all of its conventional asymmetric cryptography with hybrid cryptographic implementations that leverage the post-quantum cryptographic algorithms Dilithium (which NIST is standardizing as ‘ML-DSA’) and Kyber (which NIST is standardizing as ‘ML-KEM’). FCMs will continue to use the XTS-AES-256 algorithm, which remains quantum-safe, for bulk data encryption.

a hybrid key wrap

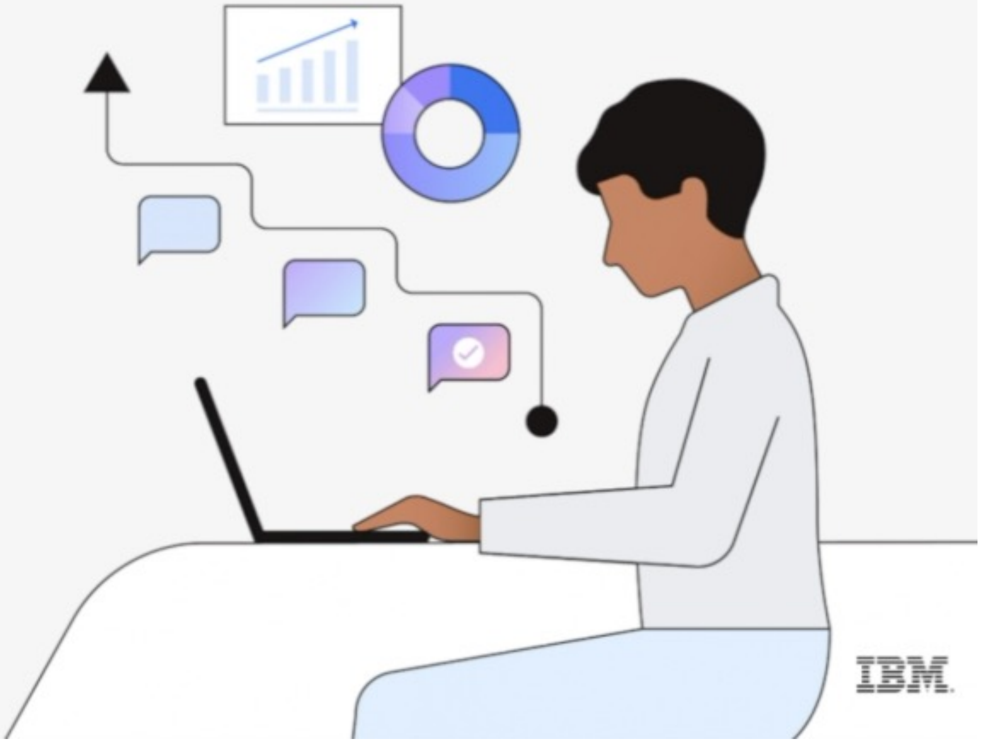




https://www.linkedin.com/pulse/quantum-safe-encryption-storage-amir-zahoor-rerrc/

Making an Online Communications Platform Quantum Safe End-to-End

Quantum Safe Crypto Agility without Application Changes



IBM

IBM **Quantum**