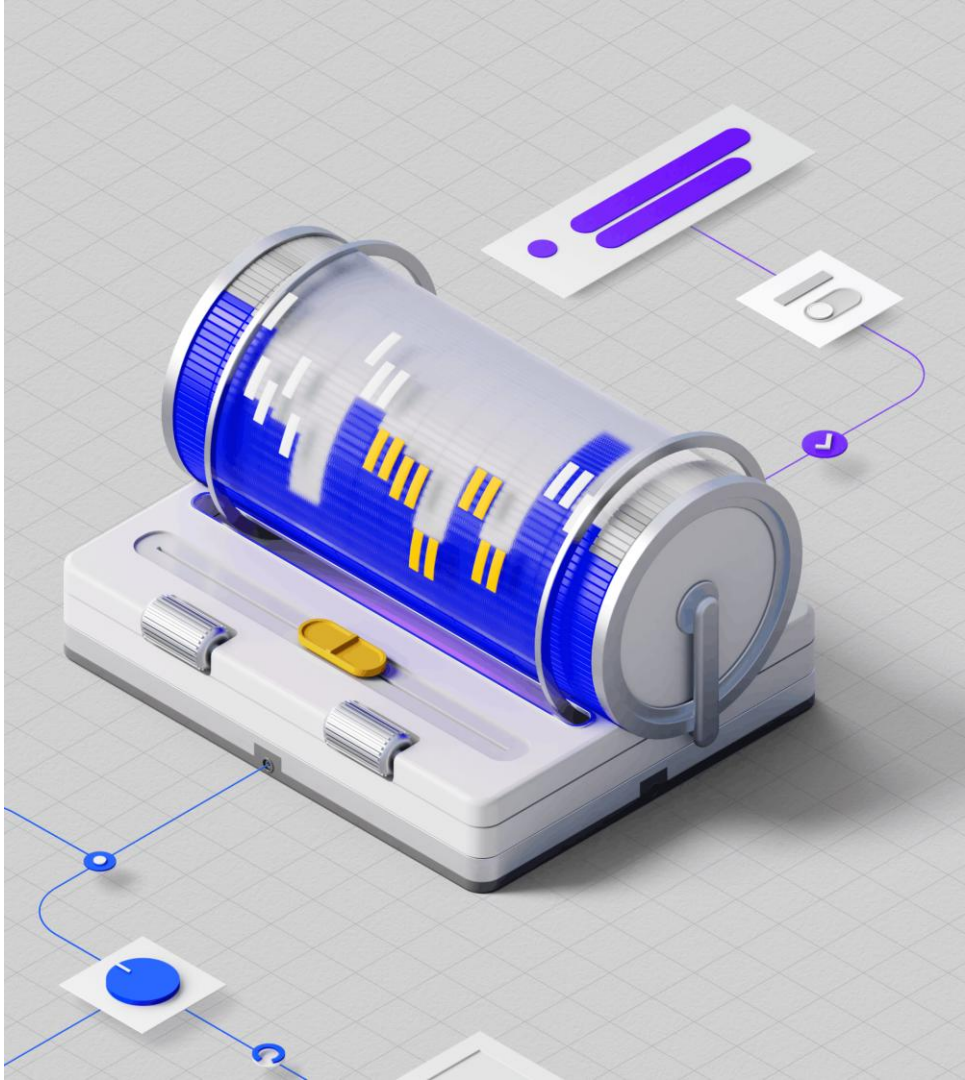
Achieving Quantum-Safe Readiness



Name: Michael Sigmund, msigmund@de.ibm.com
Title: IBM SW Architect

IBM



Bring useful quantum computing to the world

Make the world quantum safe

Cryptography impacts everything

Cryptography touches every corner of the digital world

Internet Protocols



Domain Name Service (DNS), Secure Hyper-text Transfer Protocol (HTTPS), Telnet, SFTP

Critical Infrastructure



Code updates; Control systems- Oil pipelines, Electric grids; Car systems,...

Blockchain Applications



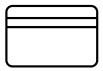
Coin wallets, Transactions, Authentication

Digital Signature Laws



Eelectronic IDentification, Authentication and Trust Services eIDAS (EU Nr. 910/2014)- PDF Advanced Electronic Signature – (PAdES), Advanced Electronic Signatures (AES), ...

Financial Systems



Payment Systems: Europay, Mastercard, and Visa EMV, Society for Worldwide Interbank Financial Telecommunication SWIFT, Settlement Systems, FinTech, ...)

Enterprise Applications



EMAIL – PGP Pretty Good Privacy, Identity Management PKI/LDAP/.., Virus scanning patterns, PKI Services

Much of today's cryptography relies on hard mathematical problems

Public key encryption

Digital signatures

Key exchange algorithms

RSA-2048
(Rivest–Shamir–Adleman)

DSA
(Digital Service Act;
EU Feb. 2024)

ECC
(Elliptic Curve Cryptography)

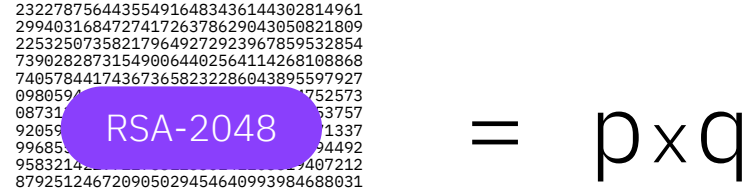
ECDSA
(Elliptic Curve Digital Signature Algorithm)

DH
(Diffie-Hellman; key exchange)

IBM Quantum Safe / © 2025 IBM Corporation

Factorization

Challenge:
Find prime factors



Difficulty

The most powerful computer today
would take millions of years to find the solution

Much of today's cryptography
~~relies on hard mathematical problems~~
can be broken with a cryptographically relevant quantum computer (CRQC)

~~Public key encryption~~	~~RSA~~
~~Digital signatures~~	~~DSA~~
~~Key exchange algorithms~~	~~ECC~~
	~~ECDSA~~
	~~DH~~

Factorization

Challenge:
Find prime factors



$= p \times q$

Difficulty

The most powerful computer today
would take millions of years to find the solution

Shor's quantum algorithm is anticipated to possibly break RSA in **hours** using hardware available soon.

IBM Quantum Safe / © 2025 IBM Corporation

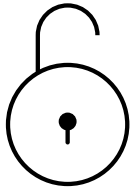
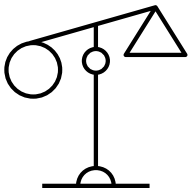
What will a cyber criminal be able to do?

Government organizations assume that “cryptographically relevant” quantum computers will exist from 2029-2035.
(NIST, BSI, ANSSI, Gartner, u.a.)

Availability of “cryptographically relevant” quantum computer

...before

...after

Harvest confidential data	Decrypt lost or harvested confidential data	Disrupt business with manipulation	Manipulate digitally signed contracts and legal history
			
in order to decrypt them later	by breaking encryption	through fraudulent authentication	by forging digital signatures

Urgency

Complexity

IBM Quantum Safe / © 2025 IBM Corporation

IBM proactively manages quantum-era risk

Tackling challenges of discovery, visibility, remediation and modernization in managing cryptography — and staying ahead of the "harvest now, decrypt later" threat

Challenge

IBM recognized a risk that most enterprises are starting to confront: today's cryptography could be tomorrow's liability.
IBM's CIO Office needed a way to discover cryptographic artifacts with near-zero manual effort, generate an actionable Cryptography Bill of Materials (CBOM) for full visibility, identify and remediate crypto-agility anti-patterns before they reach production, and proactively manage quantum-era cryptographic risk with measurable outcomes.

Solution

IBM watsonx.data integration
IBM Databand

Read the full story



Impact

IBM deployed Quantum Safe Explorer:

- Scanned nearly 6000 repositories and over 47 million lines of code
- Identified 3900+ vulnerabilities
- Generated CBOMs for audit and compliance
- Enabled dashboards for leadership to track risk and remediation

"By embedding Quantum Safe Explorer into their DevSecOps pipeline, IBM's CIO Office set a foundation for crypto-agility, quantum-era preparedness, and resilient cyber-hygiene. This early test case helped shape IBM's mission to help enable customers transition towards crypto-agility and quantum-resilience, as enterprises globally begin their quantum-safe transformations."

vodafone

Promoting the adoption of post-quantum cryptography standards and other security best practices in a future of advanced quantum computing

Challenge

Vodafone is proactively protecting its customers and their data from future risks related to quantum computers when browsing the Internet on their smartphones.
In order to do so, Vodafone was looking to introduce new, attack-resistant cryptographic algorithms across its networks, as well as business and consumer products.

Solution

IBM Quantum Safe technologies

Read the full story



Impact

IBM and Vodafone have developed a proof of concept to enhance Vodafone Secure Net against anticipated quantum security risks

Vodafone became one of the first companies to successfully test IBM Quantum Safe technology to identify and inventory cryptography in its network infrastructure and systems

“ We want our customers to enjoy the internet without worry, now and in the future. On the one hand quantum computing could have many societal benefits such as modeling new medicines and optimizing advanced digital networks. But on the other hand, it could be used to undermine the cryptographic principles that the Internet relies on today. That is why Vodafone and IBM are working together with other partners to get ahead of the curve.”

Luke Ibbetson
Head of Research & Development
Vodafone

Whether or not we believe quantum computing's impact on data security strategies, action needs to be taken

Global standards bodies have decided on the need for new, quantum-resilient cryptography.



US Federal Agencies

US National Security Memorandum 10 directs agencies to migrate to quantum-resistant technology[1].



EU Members

Guidance from 18 EU member states requires preparation for quantum threats be integrated into cybersecurity risk management[2].



NIST

By 2030, NIST will deprecate the first set of quantum-vulnerable algorithms. By 2035, NIST will disallow traditional cryptography algorithms[3].

1.National Security Memorandum 10, Young, 2022
2.Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography, BSI, 2024
3.Transition to PQC Standards, NIST, 2024

Organizations face challenges in managing cryptography

Quantum Threats

By **2030**, NIST will deprecate the first quantum-vulnerable algorithms[1], and “Harvest Now, Decrypt Later” attacks put data at risk today

Lack of Visibility

Only 30% of organizations have their apps, data, and services inventoried to understand how cryptography is used across the organization[2]

Lifecycle Complexity

The lifespan of a TLS certificate is set to be reduced from 398 days to just **47 days**

Tool Sprawl

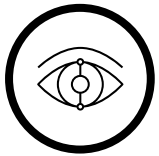
Fragmented tools increase friction, complicating risk management and **making compliance harder**

IBM © 2025 IBM Corporation

1. Transition to PQC Standards, NIST, 2024
2. Quantum-Safe Readiness, IBM Institute for Business Value, 2025

IBM’s approach to achieving crypto-agility

Protecting today. Preparing for tomorrow.



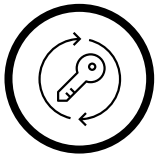
Discover and Inventory

Automatically and continuously discover and inventory your cryptographic landscape



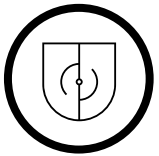
Assess and Comply

Assess your cryptographic posture to prioritize vulnerabilities and maintain compliance



Manage Lifecycle

Simplify and automate cryptographic object management



Protect and Adapt

Encrypt data and adopt a crypto-agile architecture

IBM © 2025 IBM Corporation

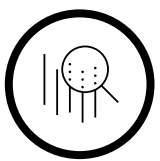
IBM Guardium Cryptography Manager Enterprise

Protecting today. Preparing for tomorrow.



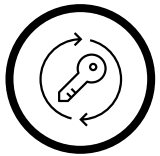
Discover and Inventory

- Identify cryptographic objects and IT assets
- Detect unknown or shadow cryptography
- Map dependencies, ownership, and usage



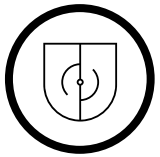
Assess and Comply

- Assess post-quantum cryptography risk
- Flag outdated or vulnerable algorithms
- Generate audit-ready reports



Manage Lifecycle

- Centralize lifecycle operations in one tool
- Automate key generation and certificate renewal
- Enforce consistent policies across the organization



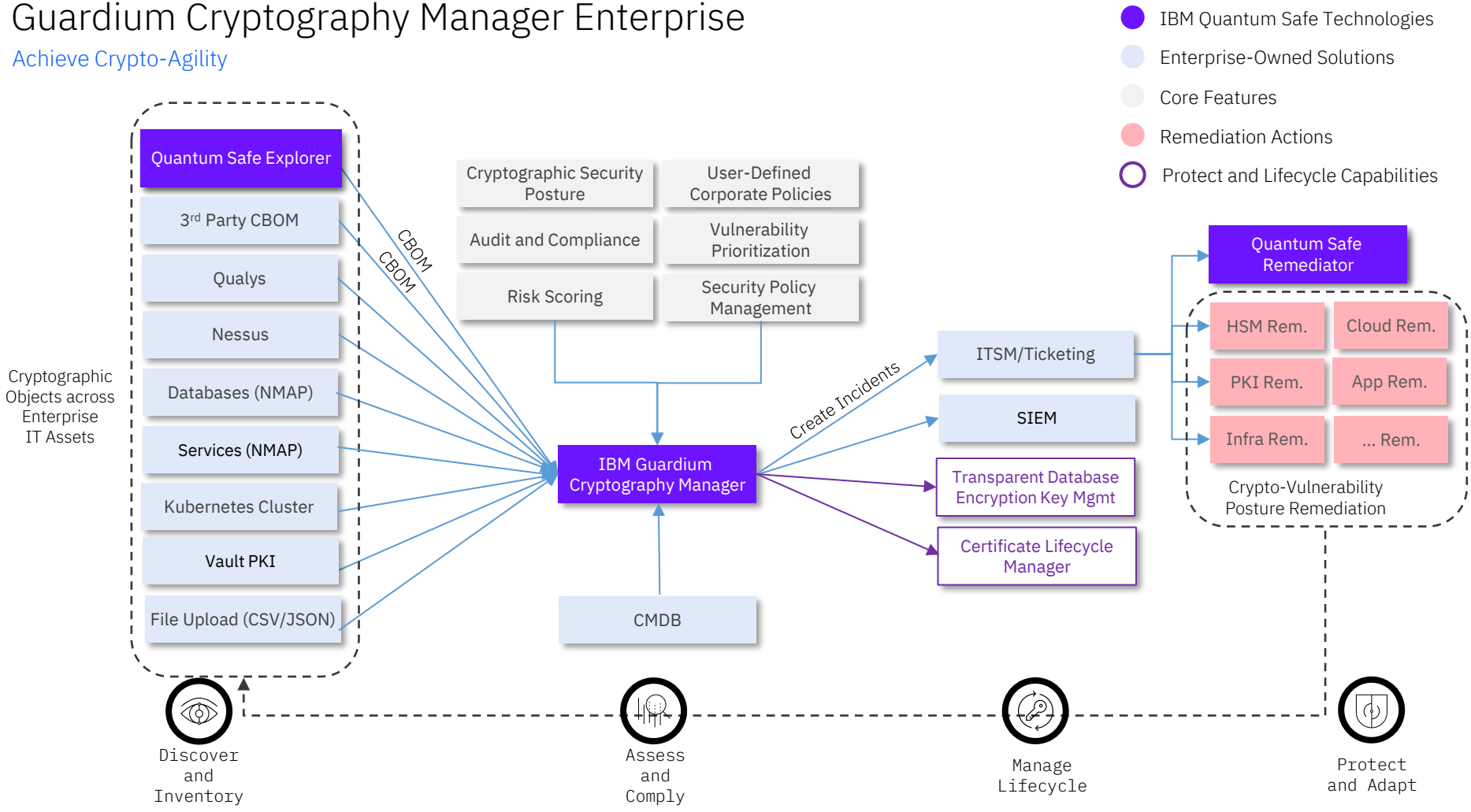
Protect and Adapt

- Utilize encryption to protect sensitive data
- Assess the efficiency and feasibility of PQC algorithms
- Protect against “harvest now, decrypt later” attacks

IBM © 2025 IBM Corporation

Guardium Cryptography Manager Enterprise

Achieve Crypto-Agility



#1 Achieve Quantum-Safe Readiness

Guardium Cryptography Manager

The solution to embrace crypto-agility: protect data today, and prepare for tomorrow's threats

Sales Assets: Seismic
Techzone Demo: All-in-One
Demo Lab Guide: Box Link
IBM Client Zero: URL

Discovery and Inventory

Build a live inventory of cryptographic objects and protocols across hybrid environments, mapped to systems and owners with expiry and strength context.

Assess and Comply

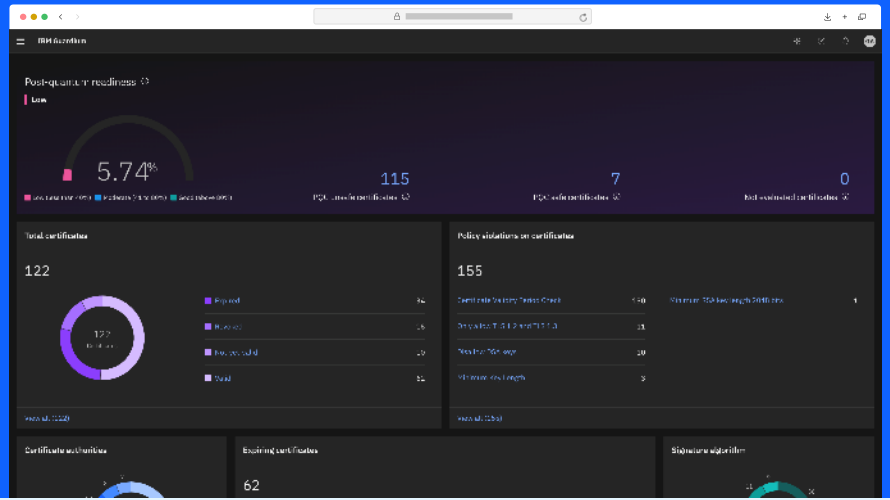
Assess post-quantum readiness across your environment, flag outdated or vulnerable algorithms, and generate audit-ready reports to expedite compliance.

Manage Lifecycle

Centralize cryptographic object lifecycle operations, detect weak or expired certificates, automate certificate renewals and manage revocation to streamline management.

Protect and Adapt

Orchestrate agentless transparent database encryption to protect sensitive data and support migration to NIST-approved quantum safe algorithms.



Only 30%

of organizations have their apps, data, and services inventoried to understand how cryptography is used across the organization[1]

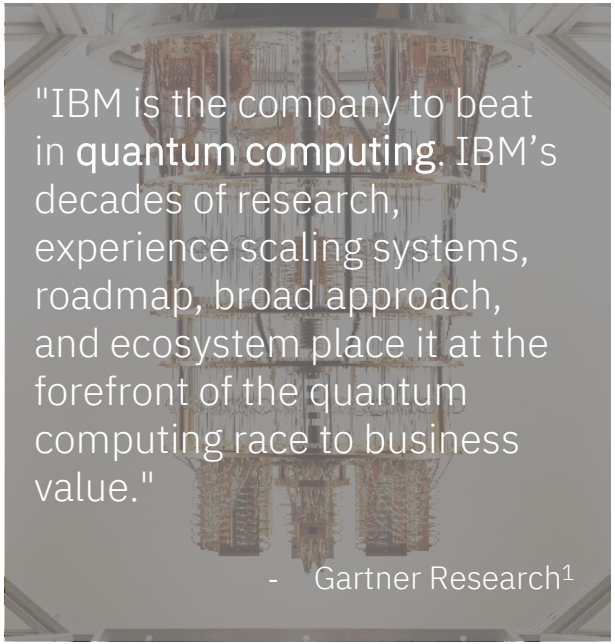
Vodafone, UK/Global

Vodafone aimed to protect their mobile customers from future quantum threats. They partnered with IBM to pilot post-quantum cryptography in Vodafone Secure Net, their digital security service used by millions of customers to protect against phishing, malware and identity theft. This POC demonstrated how new cryptography standards could be integrated into existing customer-facing services, and protect against existing risks of "harvest now, decrypt later".[2]

1. Quantum-Safe Readiness, IBM Institute for Business Value, 2025

IBM is the leader in quantum solutions

IBM leads in bringing useful quantum to the world...



... and leads in making the world quantum safe

2024: IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards[2]

2025: IBM's quantum-safe signature schemes advance in NIST's PQC process[3]

IBM Guardium protects[4]

4 of 5	8 of 10	7 of 10	5 of 5
Top Global Businesses	Top US Insurers	Top Global Banks	Top US Retailers

1. AI Vendor Race: IBM Is the Company to Beat in Quantum Computing, Gartner, 2025
2. IBM-Developed Algorithms Announced as NIST's First Published Post-Quantum Cryptography Standards, IBM Newsroom, 2024
3. IBM's quantum-safe signature schemes advance in NIST's PQC process, IBM Research, 2025
4. 2 Based on IBM client data and The Global 2000, Forbes, 2025

IBM © 2025 IBM Corporation

NIST National Institute of Standards and Technology publish
FIPS Federal Information Processing Standards

ML-KEM: FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard
ML-DSA: FIPS 204, Module-Lattice-Based Digital Signature Standard
SLAH-DSAS: FIPS 205, Stateless Hash-Based Digital Signature Standard
FN-DSA: FIPS 206, FALCON
HQC: Hamming Quasi-Cyclic (under review)
…
At least three more standards from IBM to come

IBM developed
IBM influenced
SandboxAQ (Alphabet/Google)

- - - - -

FIPS 206 specifies FN-DSA based on the selected NIST PQC submission FALCON
- A lattice-based signature scheme
- In the Hash-Then-Sign paradigm
  - Signature is a lattice point close to target point $\boldsymbol{t}$ derived from a randomized message hash
- Uses NTRU Lattice over the NTT-friendly ring $\mathbb{Z}q\ X\ /\ Xn + 1$, where $n = 2\ell$
- Uses FFT, LDL tree (FALCON Tree) to approximate discrete Gaussian sampling

IBM Quantum Safe / © 2025 IBM Corporation

Further Readings ?



