Quantum computing and key impacts on digital security

Marco Brenner
IBM Research

IBM **Quantum**

IBM Research Europe-Zurich

130+
H2020 Collaborations

500+
Collaborations with SMEs, Enterprises and Universities

26
Swiss National Science Foundation Projects

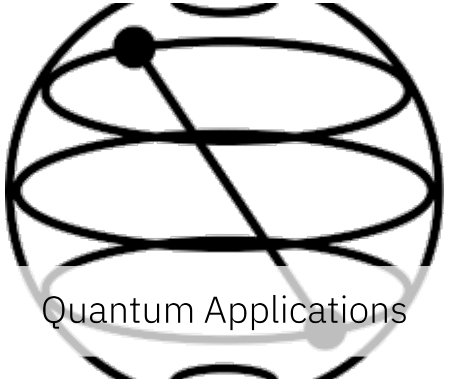
45+
Nationalities

12
European Research Council Grants

4
Nobel Laureates

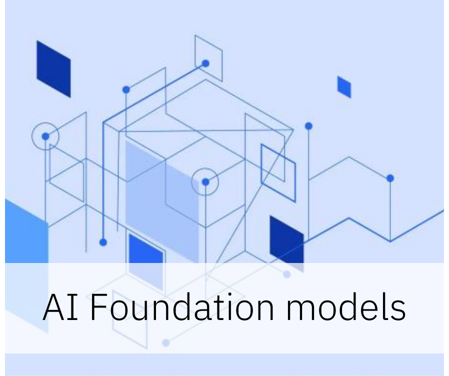
With a focused research on AI, Hybrid Cloud, Quantum, Science

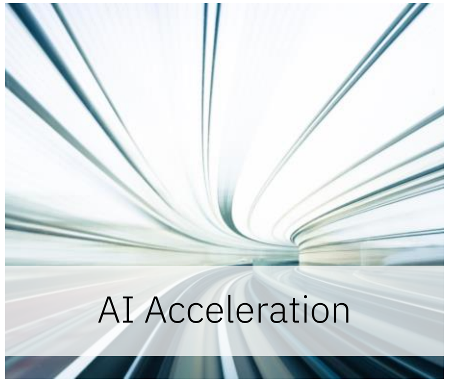

Accelerated Discovery

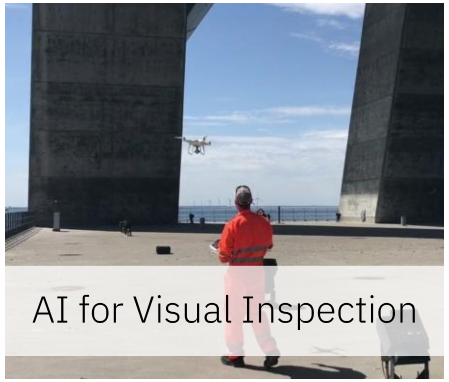

Quantum Applications


Quantum-Safe Crypto


Exploratory Science


AI Foundation models


AI Acceleration


AI for Visual Inspection


AI for Security


AI Hardware


Quantum Technology


Next-Generation Storage

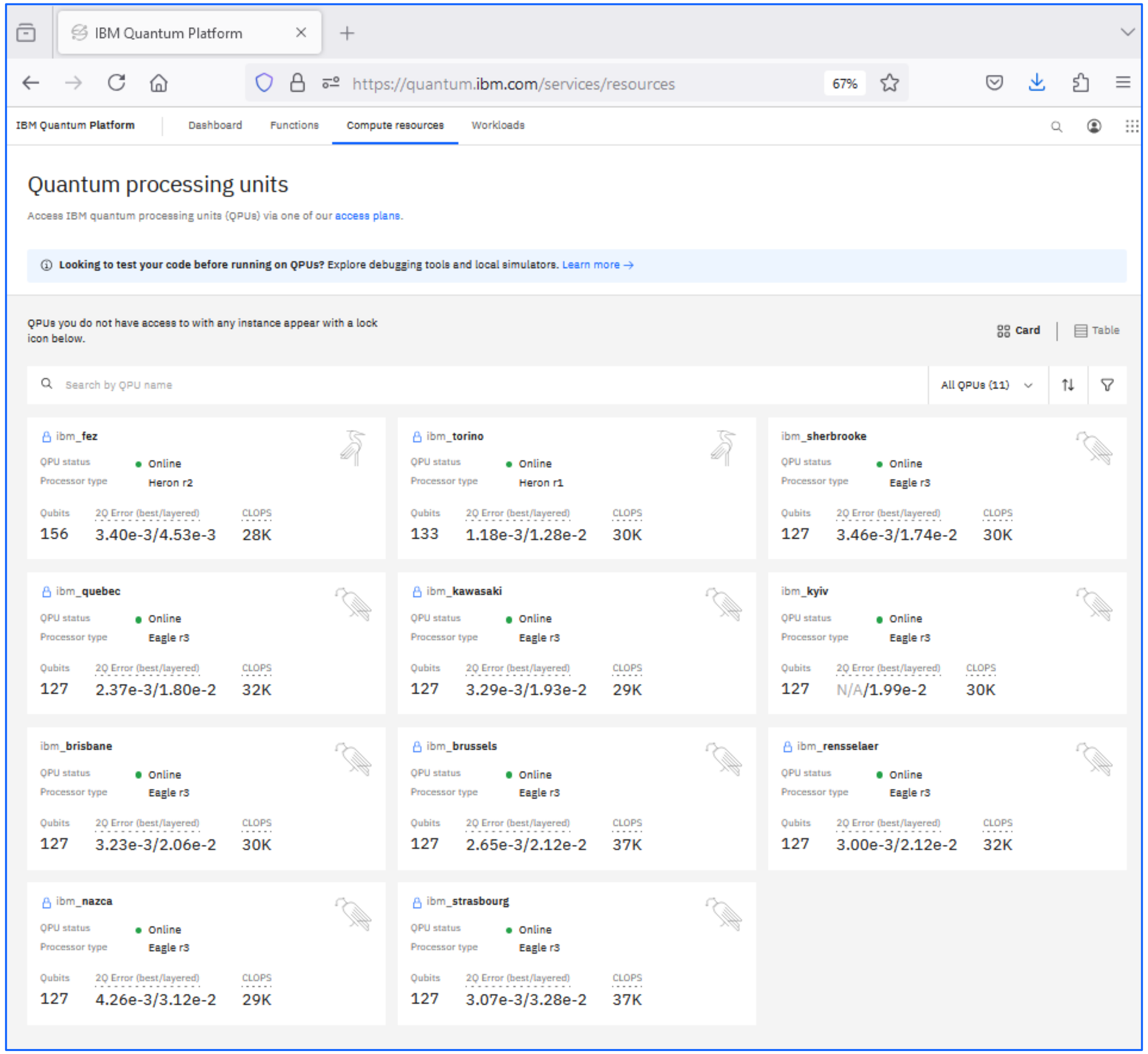

Hybrid Data Fabric

Our mission

Bring useful quantum computing to the world

Make the world quantum safe

IBM Cloud quantum services




Forbes

FORBES > INNOVATION > CLOUD

IBM Opens Its First Quantum Data Center In Europe

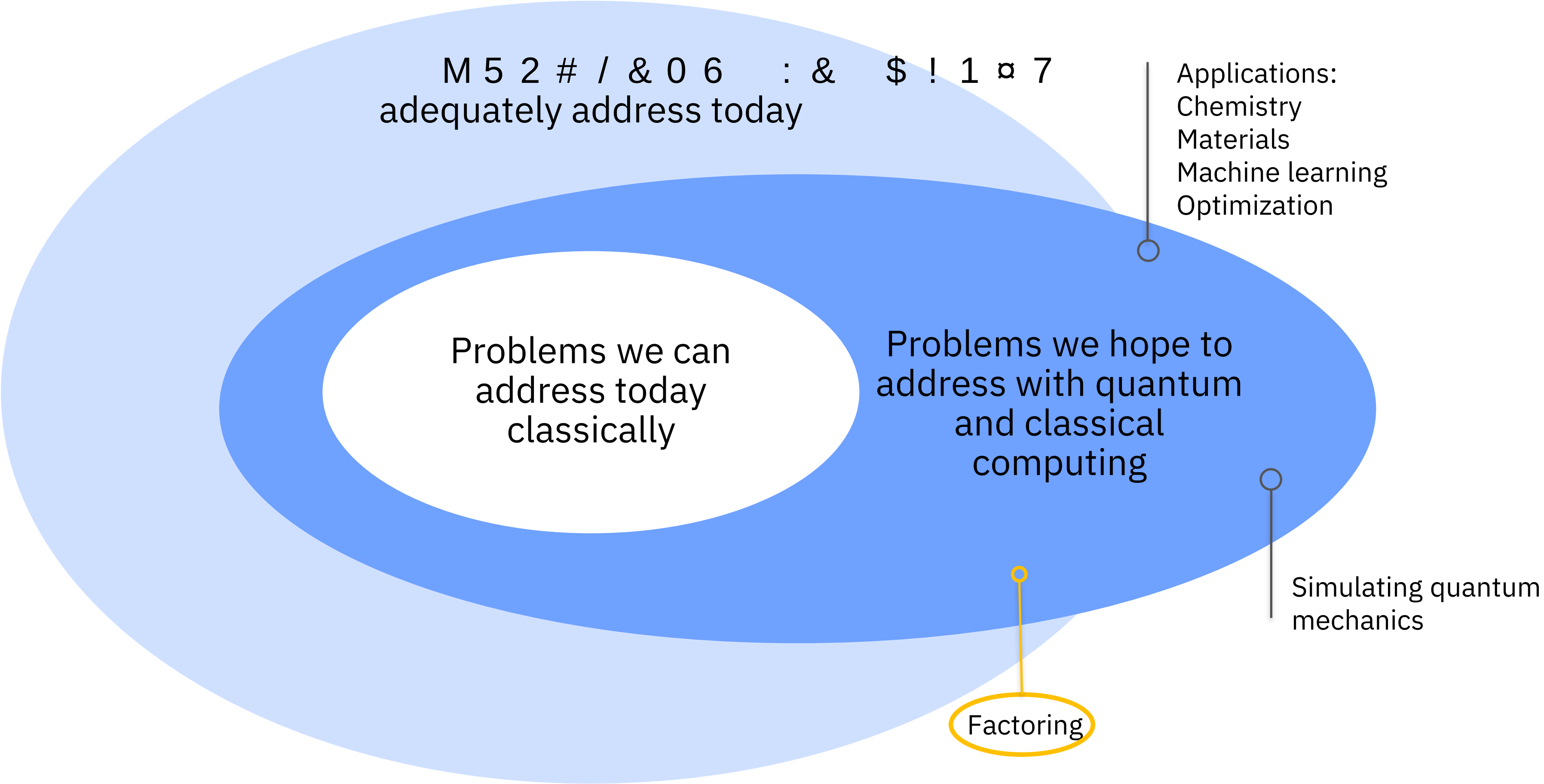
Paul Smith-Goodson Contributor
Moor Insights and Strategy Contributor Group

Follow

Oct 21, 2024, 04:43pm EDT

German Chancellor Olaf Scholz at the opening of the IBM Quantum Data Center in Ehningen, Germany IBM

Why Quantum ?



A & 6 3 , 7 & + 2 : 6 2 3 + , 6 7 , $! 7 & % % , (, 7 ! / ¥ $ / ! 6 6 , $! / ¦ $ 2 0 3 8
8 6 , 1 & 6 6 3 5 2 # / & 0 6 ' 2 5 : + , $ + : & ¤ 9 & # ! 5 & / < 6 $ 5 !

Digital security is based on mathematical problems

Current popular cryptographic algorithms rely on one of three hard mathematical problems:

Åthe integer factorization problem,

Åthe discrete logarithm problem

Åthe elliptic-curve discrete logarithm problem

Used mainly for:

Å Digital signatures

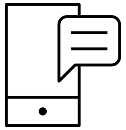
Å Key exchange (establishment of a common symmetric key)

Factorization	Challenge: find prime factors	Computation time
2322787564435549164834361443028149612994031684727417263786290430508218092253250735821796492729239678595328547390282873154900644025641142681088687405784417436736582322860438955979270980594463654064631679[illegible]57308731326921590012233642611076405375792059[illegible]7346037133799685553462443743658643499508[illegible]631233014110351940721287925124672090502945[illegible]4585674072483168497062280397019458840452229853555457804905221526364397187245486217526051159916514049067262683351832309929798930626982884352880228081343661786676287332222814070049377025100824571915521143930659330865829 30373 (RSA2048)	= p ∗ q	Most powerful computer today: millions of years
		P + 2 5 ∗ 6 Quantum Algorithm: Some hours

What do we need asymmetric cryptography for?

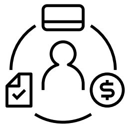
Confidentiality

To protect information from being disclosed to unauthorized entities.



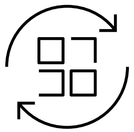
Authentication

To identify the entities involved in a communication or transaction.



Integrity

To ensure communication is not changed between entities.



Nonrepudiation

To ensure that authorship can not be disputed.

Our digital infrastructure depends on cryptography to provide the foundation for trusting digital ecosystems.

What will attackers be able to do?

availability of
¦ $ 5 < 3 7 2 (5 ! 3 + , $! / / < 5 & / & 9 ! 1 7 §
Quantum Computer

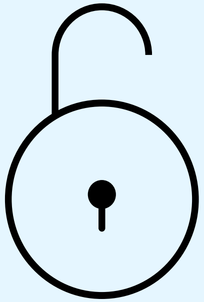
| # & '

| ! ' 7 & 5

Harvest
confidential data

in order to decrypt them later

Decrypt
lost or harvested confidential historical data

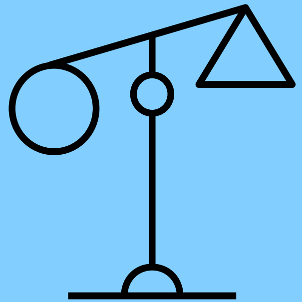


through stealing encryption keys

Disrupt
daily business by manipulating updates, malware detection & forging transactions

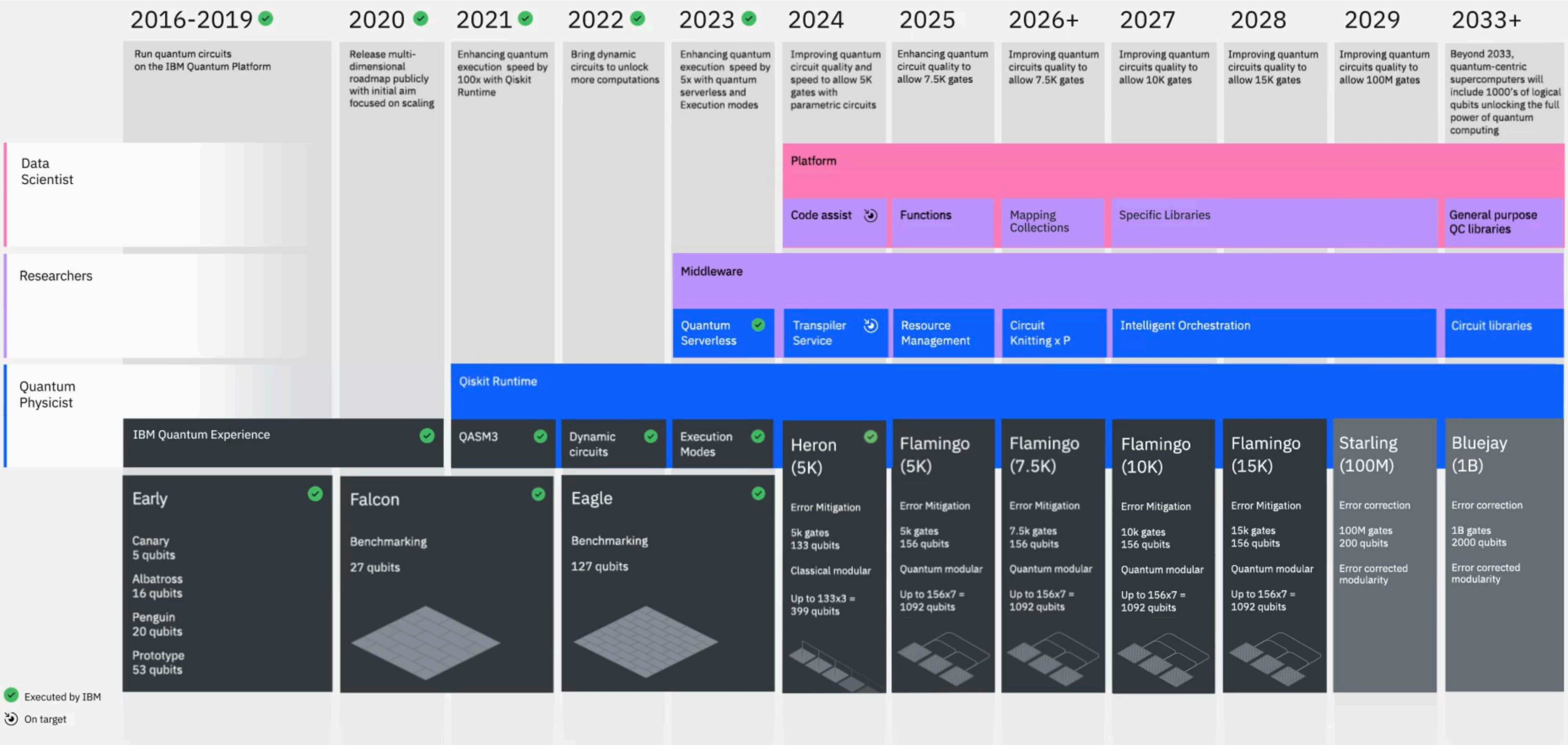
through fraudulent authentication

Manipulate
digitally signed contracts retrospectively& legal history



by forging digital signatures

Development Roadmap

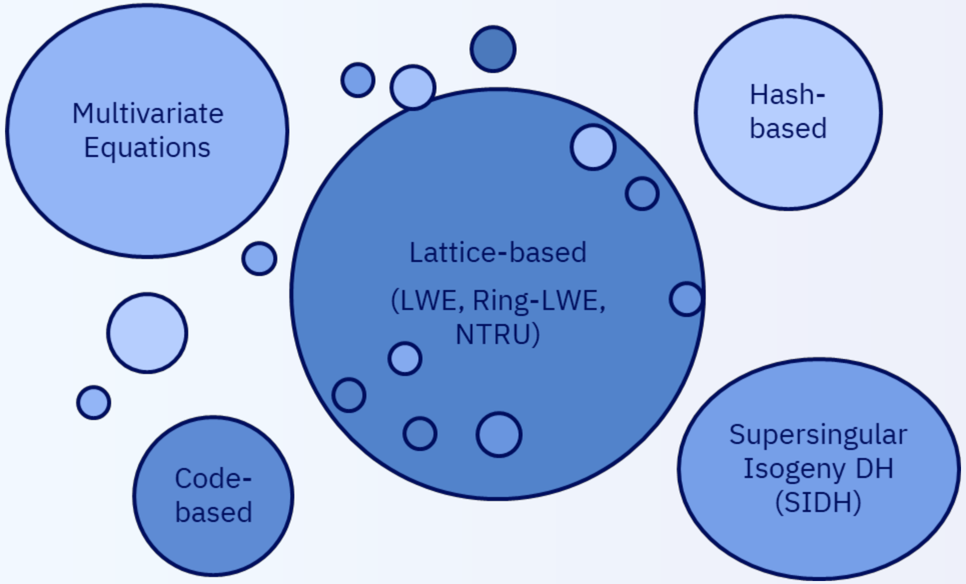


https://www.ibm.com/quantum/technology#roadmap

Quantum Safe Algorithms

Standardization for cryptographic algorithms are usually driven by the US National Institute for Standards and Technology (NIST).

After three rounds of evaluation of Quantum Safe algorithms, NIST identified seven finalists. In July 2022 NIST selected a small number of new quantum-safe algorithms for standardization by 2024.



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

Algorithms selected for standardization after round 3:

Digital Signatures
(document signatures & network certificates)
1. ML-DSA wCRYSTALS-Dilithium* (lattices)
2. FALCON * (lattices)
3. SLH-DSA wSphincs+ (hash-based)

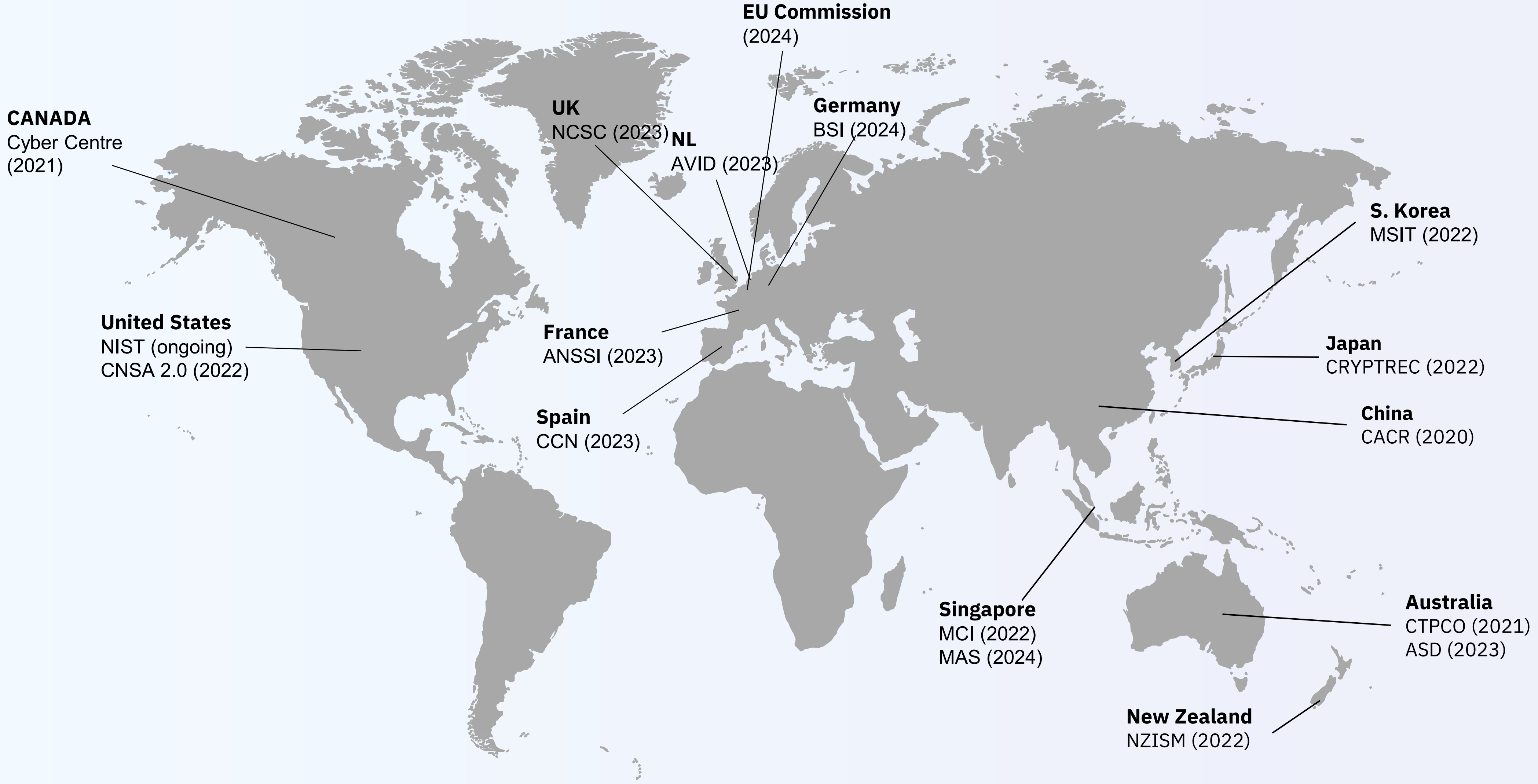
Key Encapsulation mechanisms
(session key establishment)
1. ML-KEM wCRYSTALS-Kyber * (lattices)

A 4th round for non-lattice based KEM submissions is going on, and an evaluation process for non-lattice-
! 6 & % 6 , (1-5 7 ! 8 0 5 3 & 6 3 + 2 ! 6 L 1 6 7 ! 5 7 &

ML-KEM, ML-DSA and SLH-DSA standards have been issued in August 2024 as FIPS-203/4/5

* CRYSTALS-Dilithium, CRYSTALS-Kyber and Falcon developed by IBM Research team, in collaboration with industry and academic partners.

Globally, several recommendations for Post Quantum Cryptography are emerging

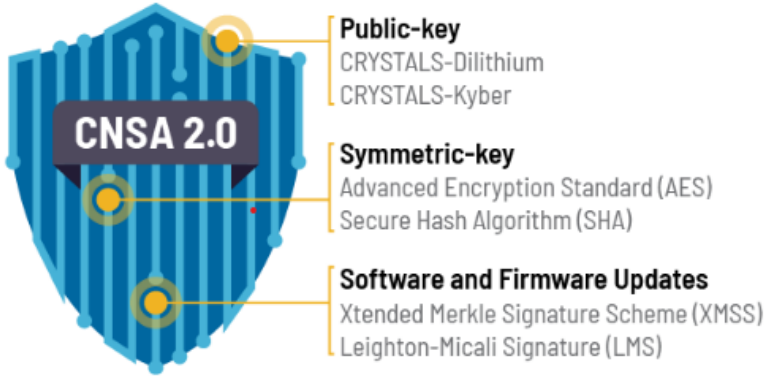


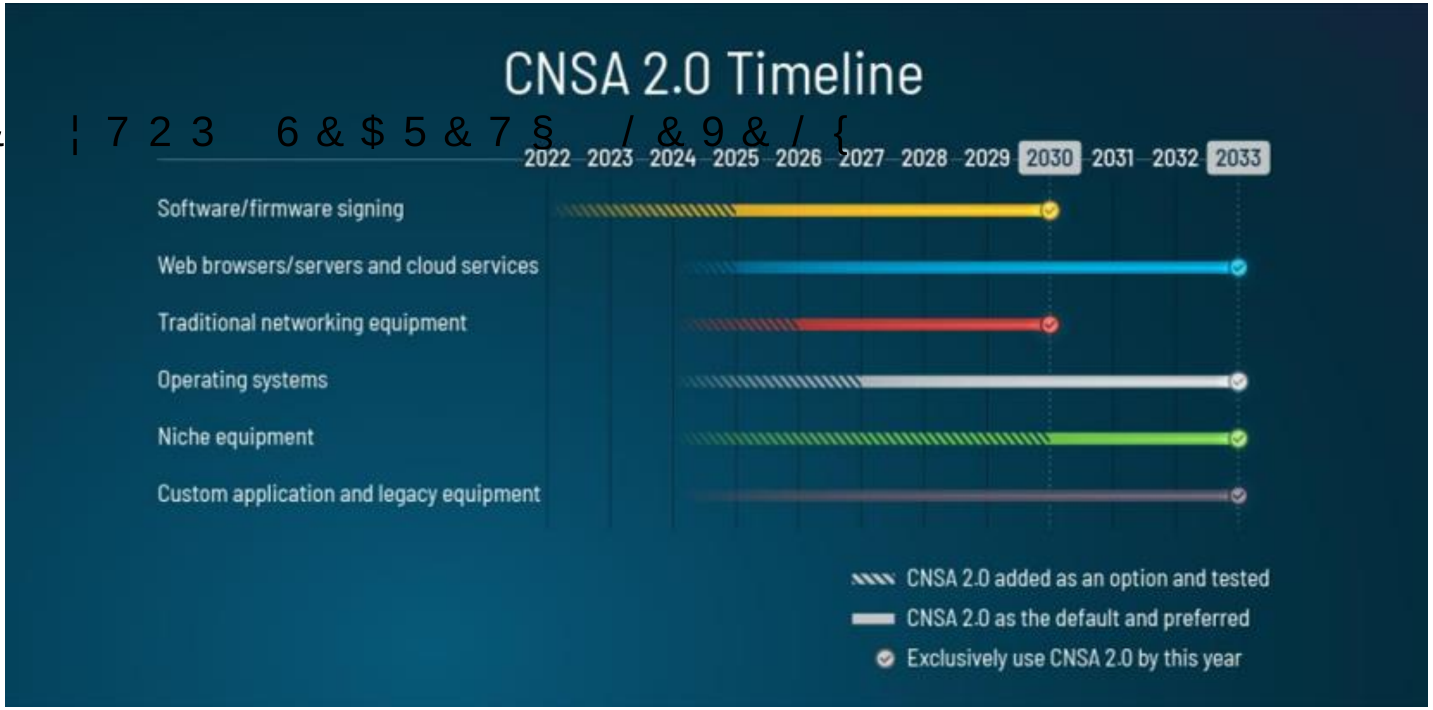
US government mandate for technology suppliers

National Security Agency (NSA): Commercial National Security Algorithm Suite (CNSA) 2.0 [1)]

Å The CNSA provides the cryptographic base to protect US National Security
, 1 ' 2 5 0 ! 7 , 2 1 8 3 7 2 7 + & ¦ 7 2 3 6 & $ 5 & 7 § / & 9 & / {

Å A timeline has been set for mandatory replacement of algorithms by 2025 and later.



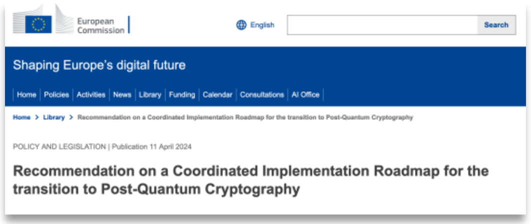


1) https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

Relevant European Recommendations

European Commission

- Member states to define -Quantum Cryptography Coordinated
- Available two years following the publication of Recommendation
- Roadmap with list of actions, including timeline for different phases and milestones



ANSSI (France)

- Hybridization to be used whenever mitigation is needed in the short and medium term
- Encourages all industries to define progressive transition strategy towards quantum-safe for relevant cryptographic products

ANSSI views on the Post-Quantum Cryptography transition
(2023 follow up)

December 21, 2023

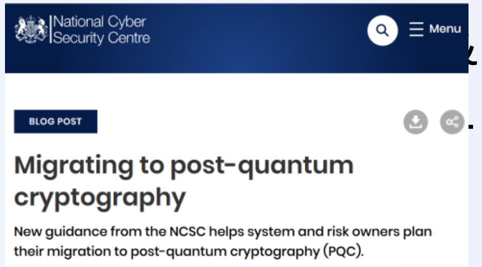
BSI (Germany)

- BSI has published a report in 2021, with a more detailed discussion about quantum-safe algorithms.
- Recommends the usage of hybrid modes with quantum-safe algorithms.
- BSI acts on the hypothesis that cryptographically relevant quantum computers will be available in the early 2030s.

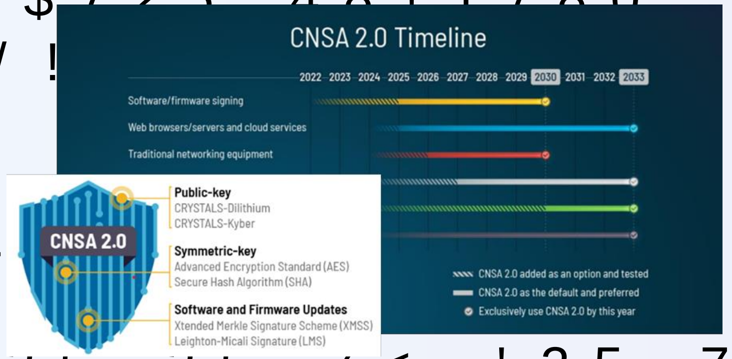
NCSC, AIVD (Netherlands)

- Published a PQC Migration Handbook that defines which organizations need to take action now with mitigation measures.
- The NCSC recommends organizations to draft a plan of action.

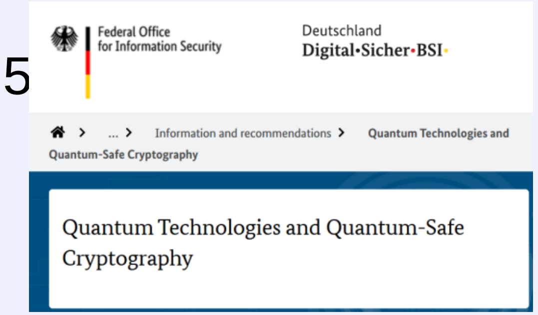
´ | µ ¦ L 5 (! 1 , = ! 7 , 2 1 6 $! 1 ! 1 % (, 1 7 2
3 / ! 1 ! 1 % 3 5 & 3 ! 5 & ' 2 5 7 + , 6 7 . 1 2 : § ´ | µ



Organisations ´ | µ 6 + 2 8 / % '- ! $ 7 2 5 4 8 ! 1 7 8 0
safe transition into their long- 7 & 5 0 3 / !



´ | µ Organisations ´ | µ 6 + 2 8 / % $ 2
investigatory work to identify which of their
6 < 6 7 & 0 6 : , / / # & + , (+ 3 5 , 2 5 , 7 < ' 2 5 7 5 §



´ | µ Organisations should factor the threat of
quantum computer attacks into their long-term
5 2 ! % 0 ! 3 6 § ´ | µ

Sources: NIST, BSI, UK NCSC

Notices and disclaimers