IBM Quantum:

Towards Real-World Applications

(We’re Not There Yet!)

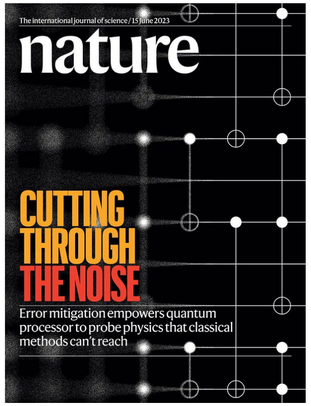
Kevin Roche
IBM Quantum Ambassador

Utility vs. Advantage

Quantum Utility (2023)

Demonstration that a quantum computer can run quantum circuits beyond the ability of a classical computer simulating a quantum computer

Confirmation via research, papers, & theory



IBM's 2023 research paper ("Evidence for the utility of quantum computing before fault tolerance") provided evidence and methods to move the industry into the Utility era

https://www.nature.com/articles/s41586-023-06096-3

Quantum Advantage (TBD)

Demonstration that a quantum computer can run quantum circuits beyond the ability of all known classical methods

Confirmation via real-world usage

Advantage will come at different times in different domains and depends on the continued advancement of quantum algorithm implementations across industries

Quantum computing applications for logistics

Optimizing routing and scheduling and enhancing insights for business strategy

Last mile delivery and multimodal transport

Quantum computers may be capable of supporting global routing optimization and more frequent re-optimization. This may improve decision making and increase revenue.

Vehicle routing and scheduling

Quantum computers could potentially provide better solutions to vehicle routing and scheduling problems with large and complex datasets than classical solvers like CPLEX.

Predictive demand forecasting

Quantum computers may improve demand forecasting by using more efficient machine learning techniques through better customer classification or patterns detection.

Global supply chain optimization

Quantum computing may enable complex, global, and rapid optimization of the global supply chain, leading to more profitable procurement, production, storage, distribution, and transportation operations.

Disruption identification and mitigation

Quantum computers may help reoptimize or simulate the impacts of disruptive events to improve decision making and reduce recovery time.

Disruption identification and mitigation

Business imperative

Managing and recovering from disruptive events quickly and reducing their impact is key to improving operations and reducing unplanned costs.

Current state

Current systems are mainly rule based, and the processes are ad hoc, with little insight to support replanning and arbitrage decisions.

Business value exploration

Quantum computers may help reoptimize or simulate these impacts to improve decision making and reduce recovery time.

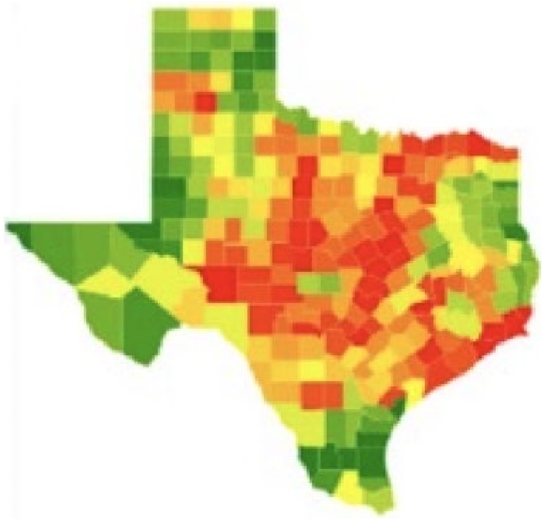
Quantum machine learning for flash flood prediction

A team of classical data scientists, Qiskit developer advocates, QML researchers, and subject matter experts in disaster management studied the application of QML to the prediction of flash flood events.

They built two models—a classic ML model and a quantum-enhanced model—and analyzed the performance of both models on a flash flood dataset from Texas and Kentucky.

Using a quantum kernel training prototype, the team demonstrated small improvements in the performance of the quantum-enhanced model, warranting further exploration for studying complex multi-hazard events.

Note: Accuracy advantages are dataset specific.



# Variables or Qubits	Classical ML Accuracy SVM	Quantum ML Accuracy Kernel Method
2	81.3%	81.9%
3	81.2%	82.7%
5	82.0%	82.9%
7	81.1%	88.8%

https://medium.com/qiskit/exploring-quantum-versus-classical-machine-learning-methods-for-disaster-management-aa58d6a3ee68

ExxonMobil

Routing optimization

In 2021, more than 500 liquified natural gas (LNG) ships were used to transport critical fuel supplies across the oceans. Together, they make thousands of journeys per year to destination ports where the LNG is deployed to power critical infrastructure.

Finding optimal routes for a fleet of such ships can be a mind-bendingly complex optimization problem.

https://www.ibm.com/case-studies/exxonmobil/
https://arxiv.org/abs/2003.02303v2
IEEE Trans Quantum Engineering, vol. 2, p. 1

Quantum computers take a new approach to addressing this sort of complexity, with the potential to find solutions that classical supercomputers alone cannot handle. Industry leaders like ExxonMobil are getting involved now to explore how blending classical and quantum computing techniques might solve big, complex, pressing global challenges.

Quantum routing optimization

Business Story

Need:

- Routing optimization is a critical problem for many industries such as logistics, supply chain, automotive, telecommunications, and manufacturing.

Value:

- Reduces the total cost of delivery:
  - vehicle cost per day,
  - driving cost per hour,
  - and distance cost per mile/km)
- Constrains: 1,200 delivery locations, vehicle capacity, single depot and delivery time windows

Learning asset:

- Last mile delivery modeled by the CVRPTW (Capacitated Vehicle Routing Problem with Time Windows)

Link: https://vrp-demo-ny.4ww07dugj2l.us-south.codeengine.appdomain.cloud/

Last mile delivery and multimodal transportation

Business imperative

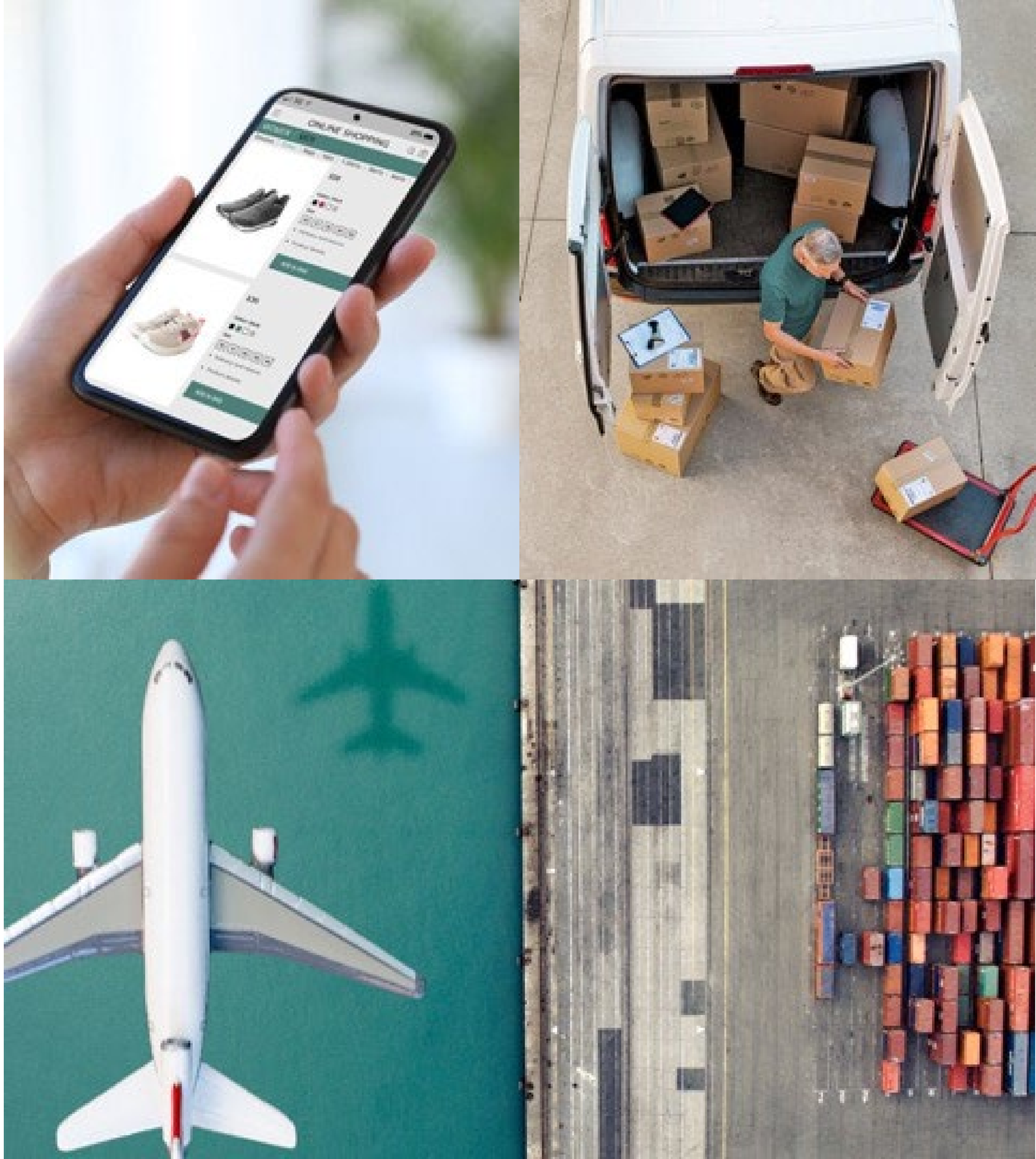
Customers’ expectations for speedy omnichannel fulfillment are growing, making optimization of multimodal transportation and last mile delivery a priority.

Current state

Current logistics optimization systems are fragmented, static, and can conduct only limited optimizations for large-scale logistics networks.

Business value exploration

Quantum computers may be capable of supporting global routing optimization and more frequent re-optimization. This may improve decision making and increase revenue.



Satellite image classification

Business imperative

Earth observation imagery plays numerous crucial roles, such as monitoring agriculture, water management, and climate change.

Current state

Hundreds of terabytes of images are collected daily. Correctly classifying these images is a first step in deriving useful information.

Business value exploration

Quantum computing may enable more accurate satellite image classification, which in turn can allow faster and more accurate management of crucial resources.

Predictive maintenance

Business imperative

Maintenance and health management of complex systems is key to cost reduction and asset availability improvement.

Current state

Most of the predictive/reliability solutions focus on sub-systems due to the inherent complexity of the mathematical models employed in the system of systems analysis and simulation.

Business value exploration

We are exploring the potential to build predictive/reliability models for complex systems by leveraging quantum machine learning and quantum simulation algorithms.

Bring useful quantum computing to the world

Make the world quantum safe

Today’s classical security protocols will be obsolete tomorrow

Prime factors

= p x q

2048-bit composite integer

```
25195908475657893494027183240048398571429282126204032
27777137836043662020707595556264018525880784406918290
41249515082189298559149176184502808489120072844992687
92807287776735971418347270261896375014971824691165077
13379859095700097330459748808428401797429100642458691
17195118746121515172654632282216869987549182422433637
59085141865462043576798423387184774447920739934236584
23824281198163815010674810451660377306056201619676256
33844143603833904414952634432190114657544454178424020
24616515723350778707749817125772467962926386356373289
12154831438167899885040445364023527381951378636564392
201039712282212072035
```

Expected computation time

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

What can a cybercriminal do?

Harvest now, decrypt later

Before

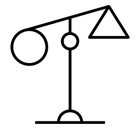
Harvest confidential data to decrypt later

Availability of “cryptographically relevant” quantum computers

After

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

The response: make the world quantum safe

Announcing Issuance of Federal Information Processing Standards (FIPS) FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard, FIPS 204, Module-Lattice- Based Digital Signature Standard, and FIPS 205, Stateless Hash-Based Digital Signature Standard

AGENCY: National Institute of Standards and Technology (NIST), Commerce.
ACTION: Notice.

SUMMARY: This notice announces the Secretary of Commerce's approval of three Federal Information Processing Standards (FIPS): FIPS 203, Module-Lattice-Based Key-Encapsulation Mechanism Standard; FIPS 204, Module-Lattice-Based Digital Signature Standard; and FIPS 205, Stateless Hash- Based Digital Signature Standard. These standards specify key establishment and digital signature schemes that are designed to resist future attacks by quantum computers, which threaten the security of current standards. The three algorithms specified in these standards are each derived from different submissions in the NIST post-quantum cryptography standardization project

Check for updates

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

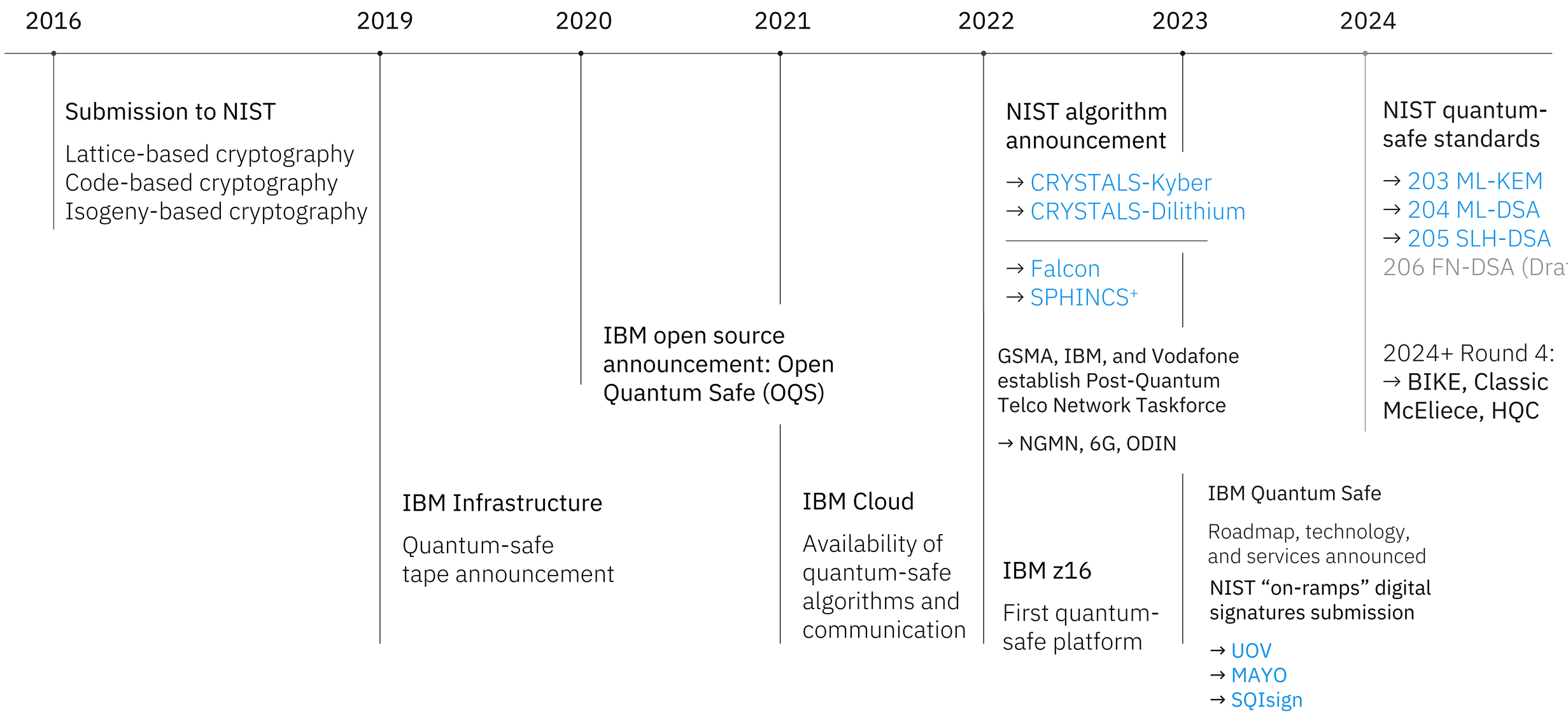
This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

or Standards and Technology

IBM **Quantum**

Launching the era of quantum safe



The time to start is now

Understand quantum risks and quantum-safe priorities

Identify cryptography footprint and prioritize actions

Initiate and implement a quantum-safe program

Beware of imitations

AI imitations

AI hardware companies are keen to expand into every market they can, prompting the joke:

“The answer is more GPUs—now what’s the question?”

Simulating quantum on AI or classical is inefficient, costly, and very constrained (to <46 qubits).

These are nowhere near utility-scale systems

Classical imitations

Companies that sell classical cloud computing are keen to jump on the quantum bandwagon…

despite no viable quantum hardware.

“Quantum-inspired” is repackaging classical cloud compute.

Thank you

IBM **Quantum**