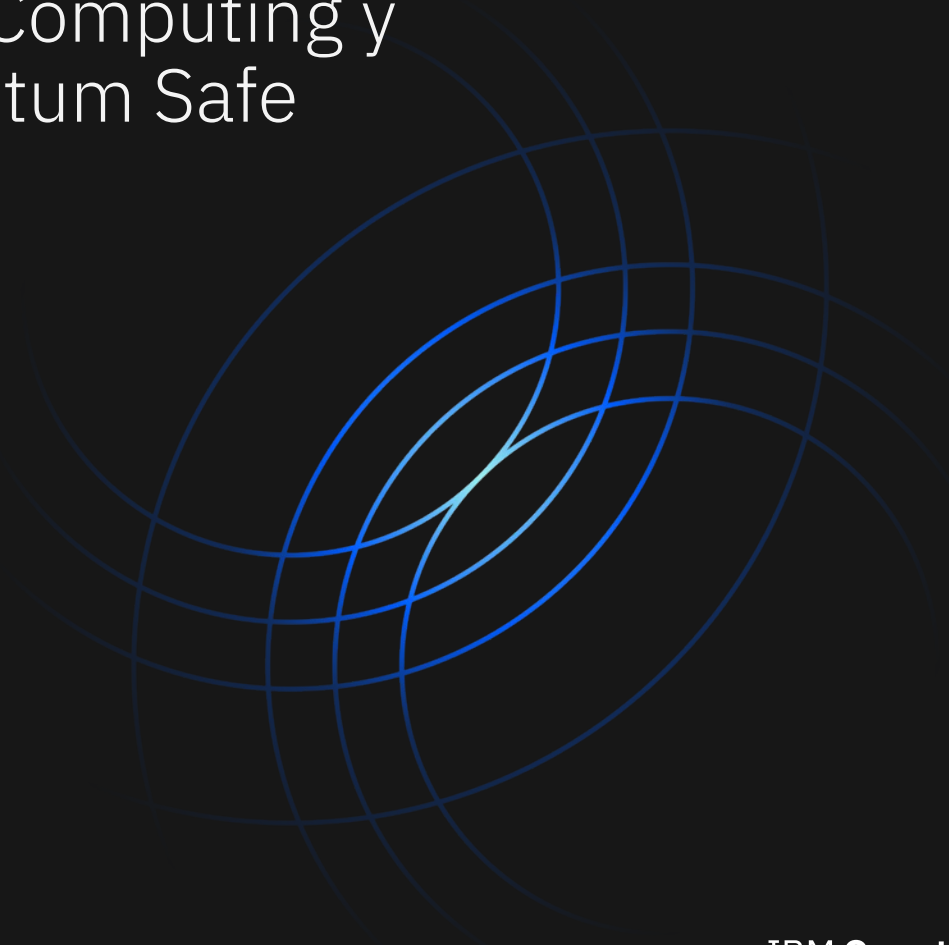
Amenazas del Quantum Computing y mitigación con IBM Quantum Safe

28.10.2023

Iván Cantero
IBM Quantum Safe Project Executive



IBM **Quantum**

Our mission

Bring useful quantum computing to the world

Make the world quantum safe

Our mission

Bring useful quantum computing to the world

Make the world quantum safe

Understanding the Quantum Threat

Exponential speedup for some algorithms

IBM **Quantum**

A quantum computer can solve certain problems much faster

2048-bit composite integer

25195908475657893494027183240
04839857142928212620403202777
71378360436620207075955562640
18525880784406918290641249515
08218929855914917618450280848
91200728449926873928072877767
35971418347270261896375014971
82469116507761337985909570009
73304597488084284017974291006
42458691817195118746121515172
65463228221686998754918242243
36372590851418654620435767984
23387184774479207399342365 84
82382428119816381501067481045
16603773060562016196762561338
44143603833904414952634432190
11465754445417842402092461651
57233507787077498171257724679
62926386356373289912154831438
16789988504044536402352738195
13786365643921201039712282212
0720357

Problem: find prime factors

= p x q

Expected computation time

Most powerful computer today

millions of years

Shor's Quantum Algorithm

some hours

Shor's algorithm will crack our asymmetric form of cryptography

- Public Key Encryption
- Digital Signatures
- Key Exchange Algorithms

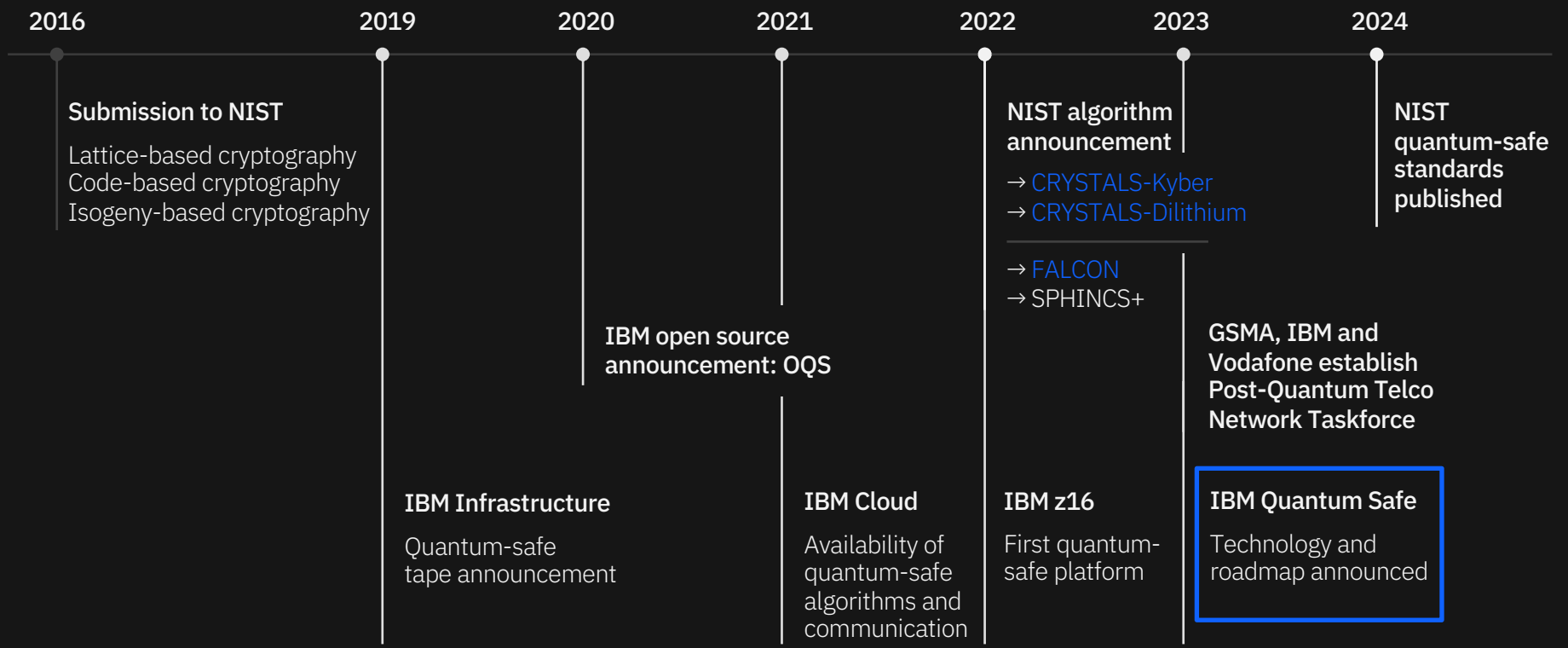
- RSA
- DSA
- ECC

- ECDSA
- DH

Quantum Threats
Summary

- The impact is in the future, but the problem is NOW
- We need new cryptography
- We need to transition to new cryptography

Launching the era of quantum safe



IBM technology helping clients throughout their journey to quantum safe

Technology with expertise powering client engagements

IBM Quantum Safe Explorer –
↳ discover your cryptography
Scan source code and object code for cryptography usage and generate cryptography bill of materials (CBOM

IBM Quantum Safe Advisor –
↳ observe your cryptography
Analyze cryptography posture of compliance and vulnerabilities, prioritize remediation actions

IBM Quantum Safe Remediator –
↳ transform your cryptography
Apply remediation patterns for implementation of crypto-agility

The time to start is now

IBM **Quantum**

Understand the quantum risks	Identify cryptography and prioritize actions	Begin transformation following a quantum safe roadmap

Let’s get you quantum safe