*Adopt Quantum Safely*

QuRISK ADVISORY

# Quantum Technologies Cyber Threat over Encryption Protocols & Mitigation Options

FRnOG 38 – 06/10/2023

# AGENDA

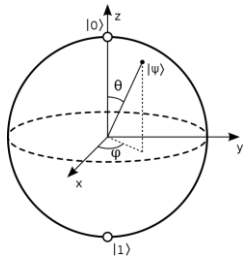
- Introduction to Quantum Technologies
- Understand the Quantum Cyber Threat
- Quantum-based Mitigation Options
- Quantum-proof Mitigation Options
- Timeline(s) & Regulations
- PQC Migration Roadmap

# Introduction to Quantum Technologies

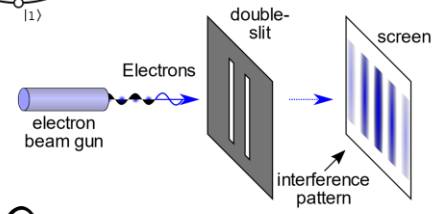
# What are Quantum Technologies?

When we harness Quantum Mechanics properties…

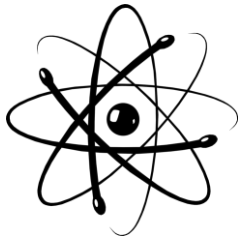
Quantum Superposition



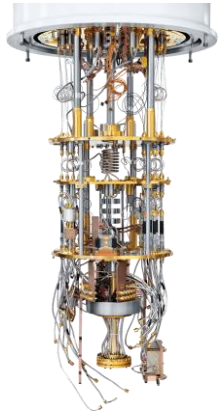

Quantum Interference




Quantum Entanglement



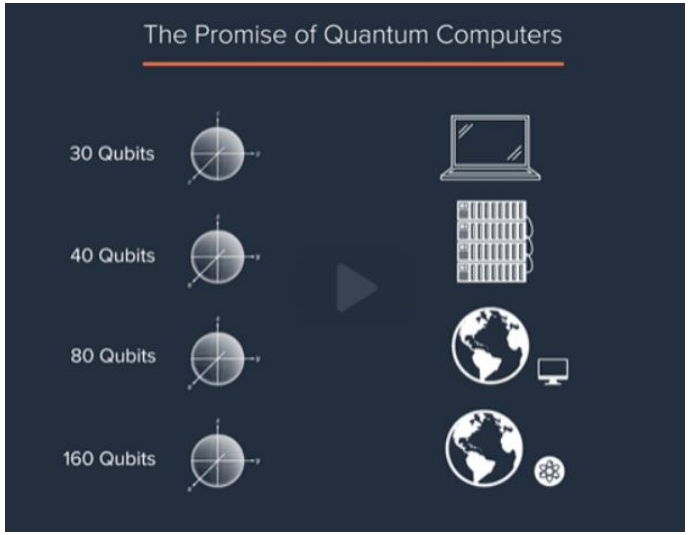
…to enhance today's Technologies…

| Computational Calculation | Secured Communications | Sensors and detectors |
|---|---|---|
|  |  |  |

…we get Quantum Technologies:

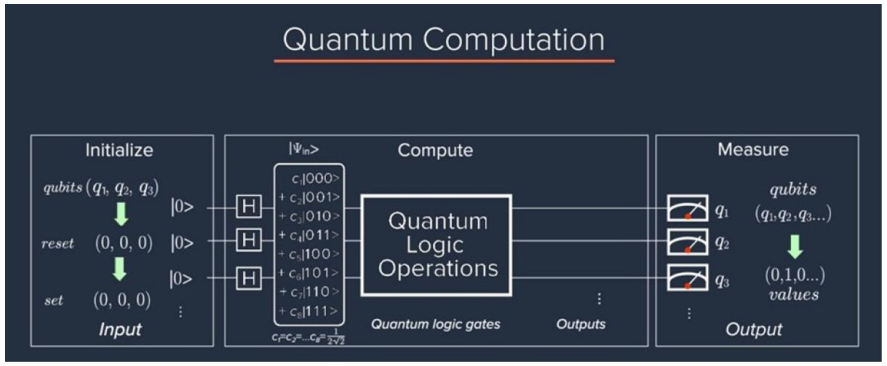
| **Quantum Computing** | **Quantum Communication** | **Quantum Sensing** |
|---|---|---|

# Insight on Quantum Computing

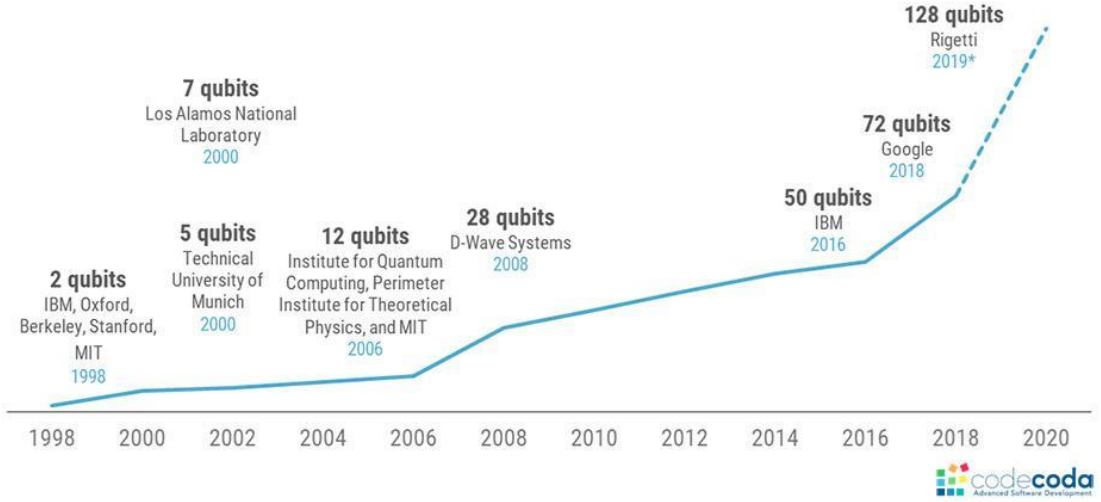



Sufficient demonstrations exist to proceed to the 100 qubit level
Concepts and/or first demonstrations exist
No realistic concepts yet developed

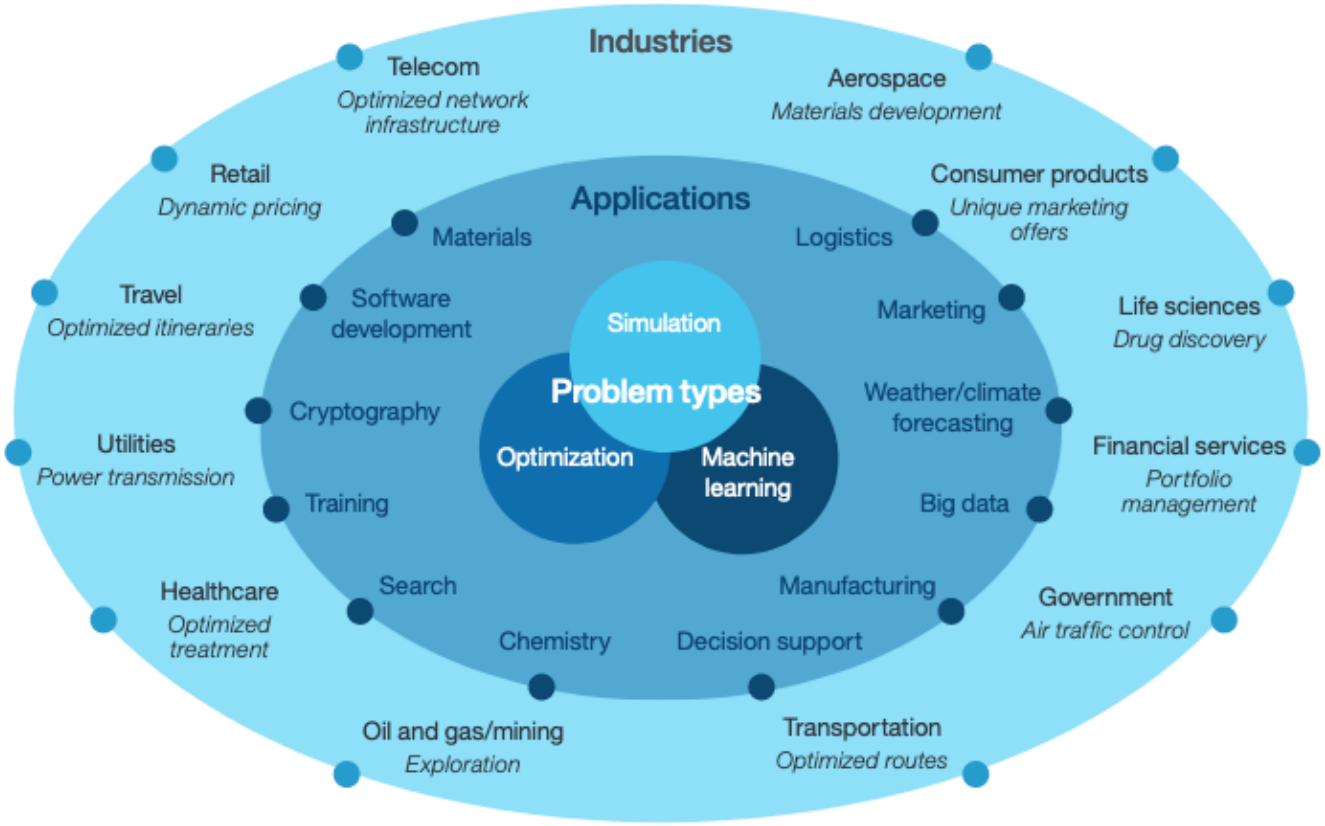
| | D1 SCALABLE SYSTEM | D2 INITIALIZATION | D3 MEASUREMENT | D4 UNIVERSAL GATES | D5 COHERENCE | D6 INTERCONVERSION | D7 COMMUNICATION |
|---|---|---|---|---|---|---|---|
| SiGe Quantum Dots | | | | | | | |
| Doped Silicon | | | | | | | |
| NV Centers | | | | | | | |
| Neutral Atoms | | | | | | | |
| Trapped Ions | | | | | | | |
| Superconductors | | | | | | | |




*Source: MITxPRO*



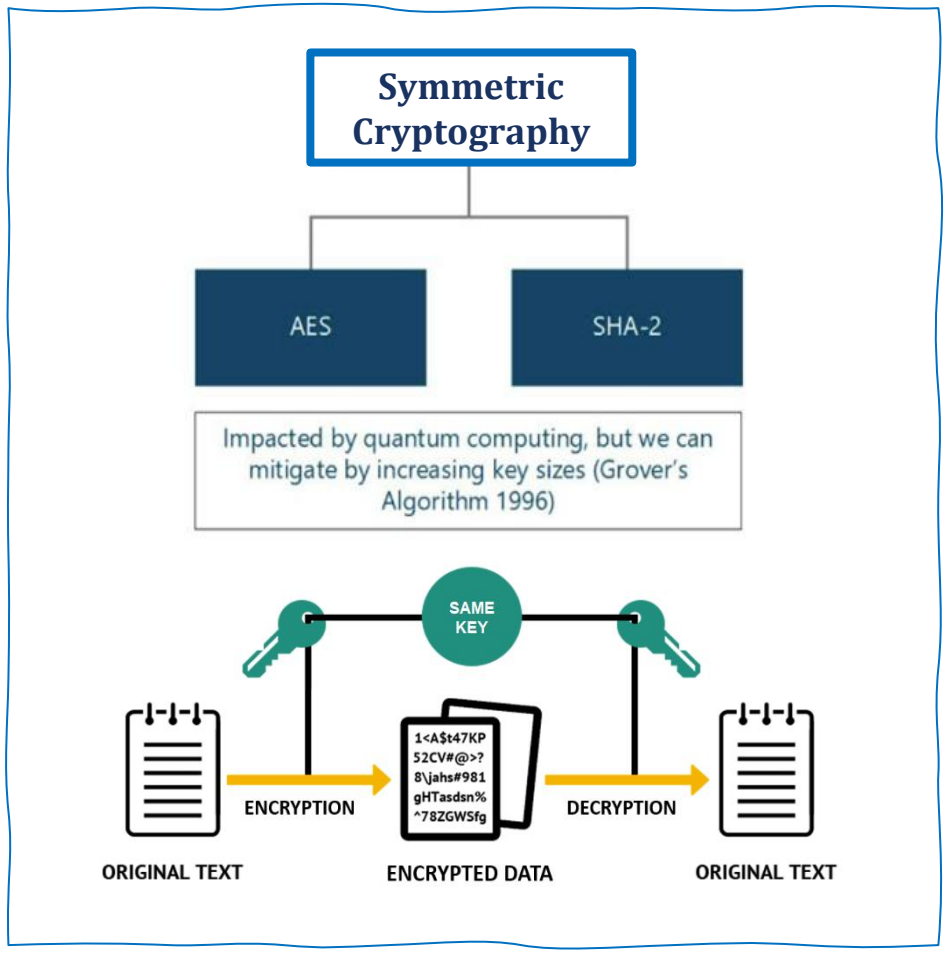
# Quantum Computing Applications

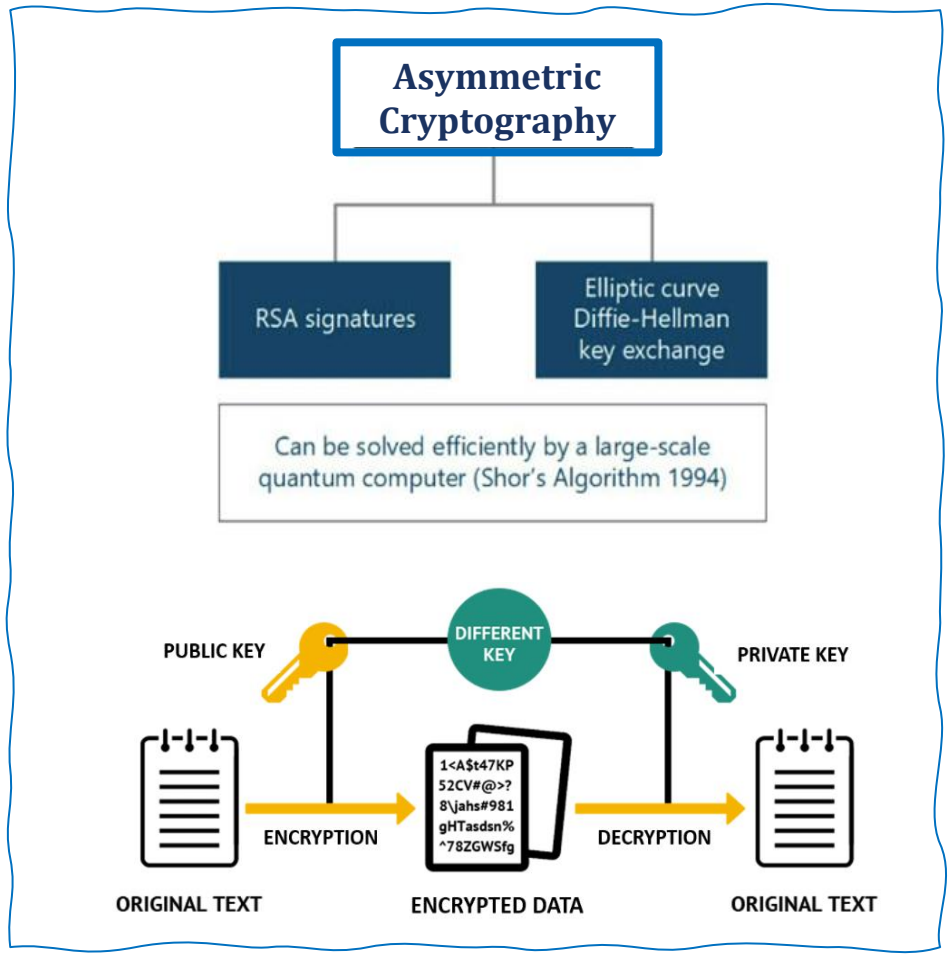



*Source: IBM*

# Understand the Quantum Cyber Threat

# Quantum Computing Threat on Cyber-Cryptography



# How to break RSA encryption?

## How does RSA encryption work?

**Key Generation**

- 2 large prime numbers p and q
- $n = p * q$
- $z = (p - 1)(q - 1)$
- Choose e where $1 < e < z$
- $d = e\text{-}1 \bmod (p - 1)(q - 1)$
- Bundle Private key pair (n, d)
- Bundle Public key pair (n, e)

**Encr.**

- $cipher = m * e \bmod n$

**Decr.**

- $plaintext = cipher * d \bmod n$

Classical computers have been able to break RSA protocols up to RSA-250 (829 bits keys equaling 250 decimal digitals)

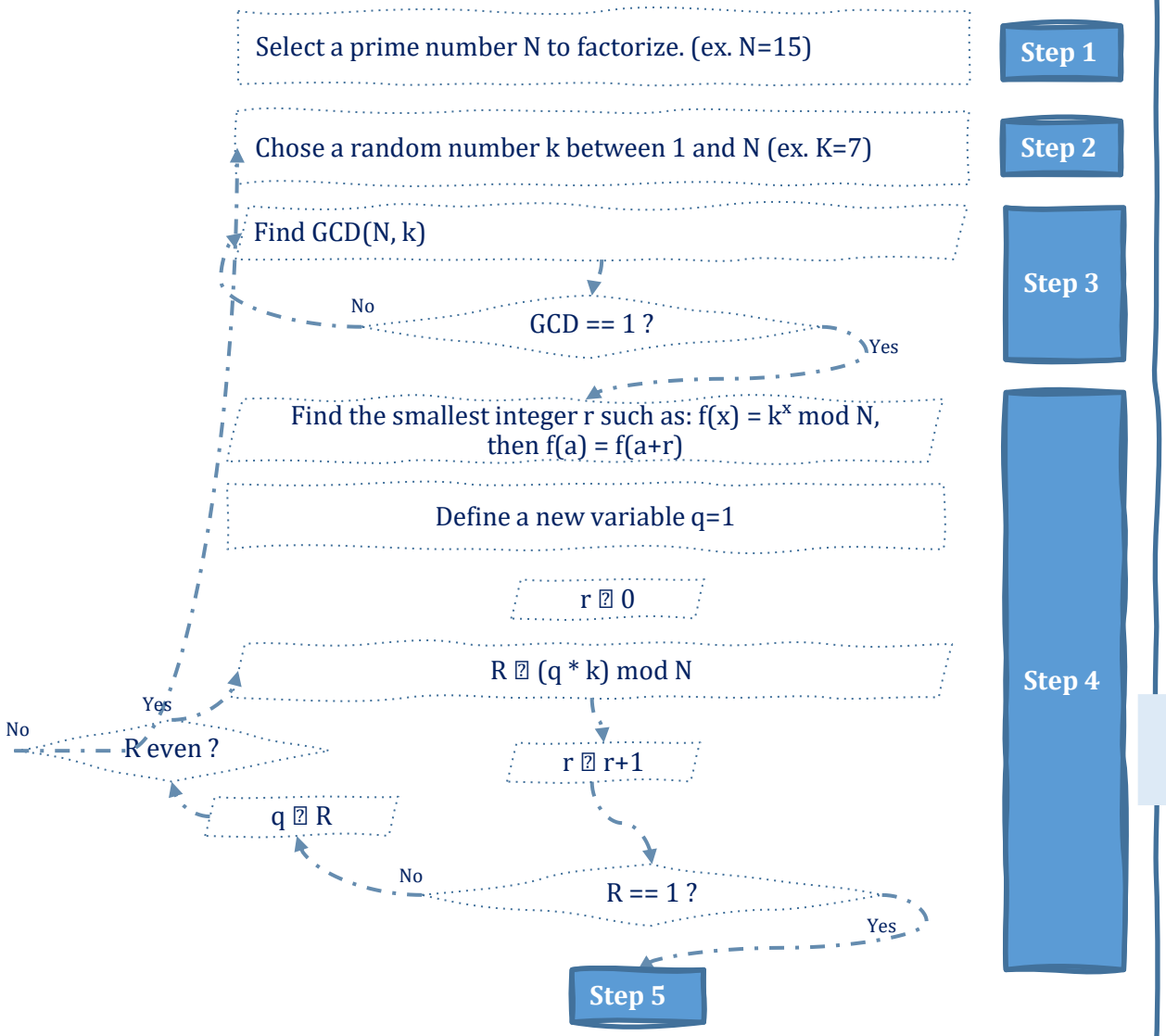
| | | | | | |
|---|---|---|---|---|---|
| RSA-100 | RSA-170 | RSA-230 | RSA-290 | RSA-360 | RSA-450 |
| RSA-110 | RSA-576 | RSA-232 | RSA-300 | RSA-370 | RSA-460 |
| RSA-120 | RSA-180 | RSA-768 | RSA-309 | RSA-380 | RSA-1536 |
| RSA-129 | RSA-190 | RSA-240 | RSA-1024 | RSA-390 | RSA-470 |
| RSA-130 | RSA-640 | RSA-250 | RSA-310 | RSA-400 | RSA-480 |
| RSA-140 | RSA-200 | RSA-260 | RSA-320 | RSA-410 | RSA-490 |
| RSA-150 | RSA-210 | RSA-270 | RSA-330 | RSA-420 | RSA-500 |
| RSA-155 | RSA-704 | RSA-896 | RSA-340 | RSA-430 | RSA-617 |
| RSA-160 | RSA-220 | RSA-280 | RSA-350 | RSA-440 | RSA-2048 |

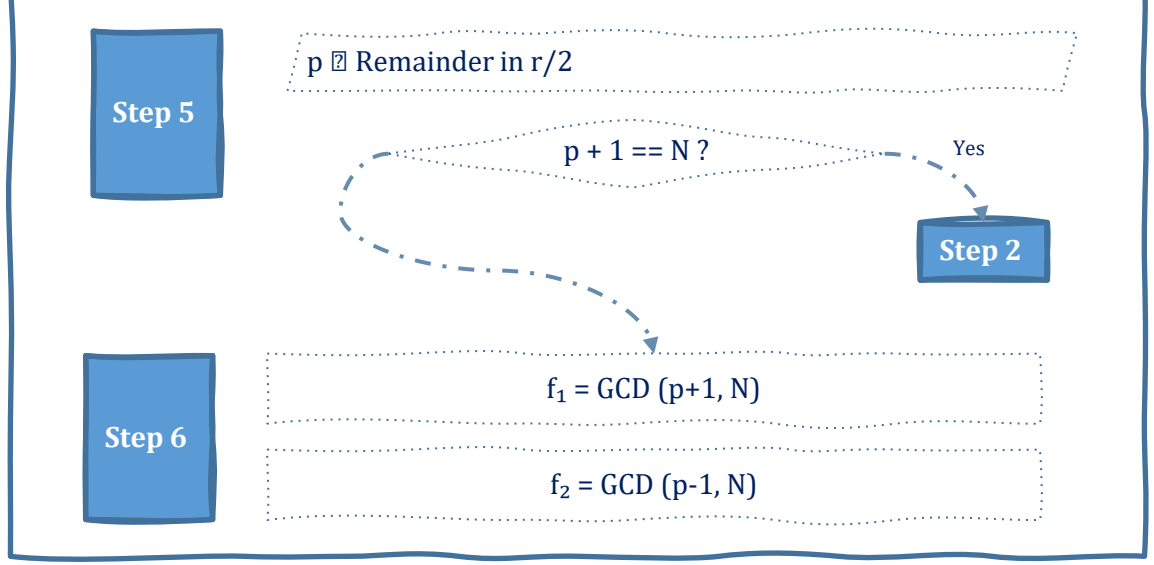
- ✓ General Number Field Sieve
- ✓ Quadratic Sieve
- ✓ Lenstra Elliptic Curve factorization

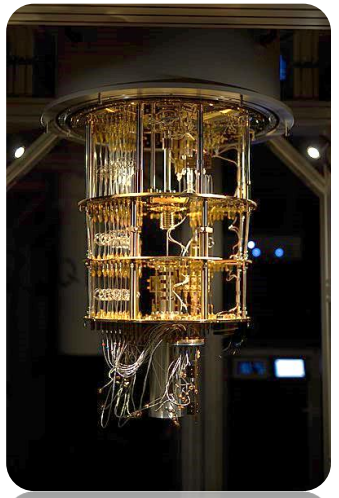
*Factorization is key to breaking RSA encryption*

**Each logical Qubit (stable Qubit) equals 100 to 1000 physical Qubits (unstable Qubits)*

# Shor's Algorithm at work



*Step 4 is performed by a Quantum Computer*

# Quantum-based Mitigation Options

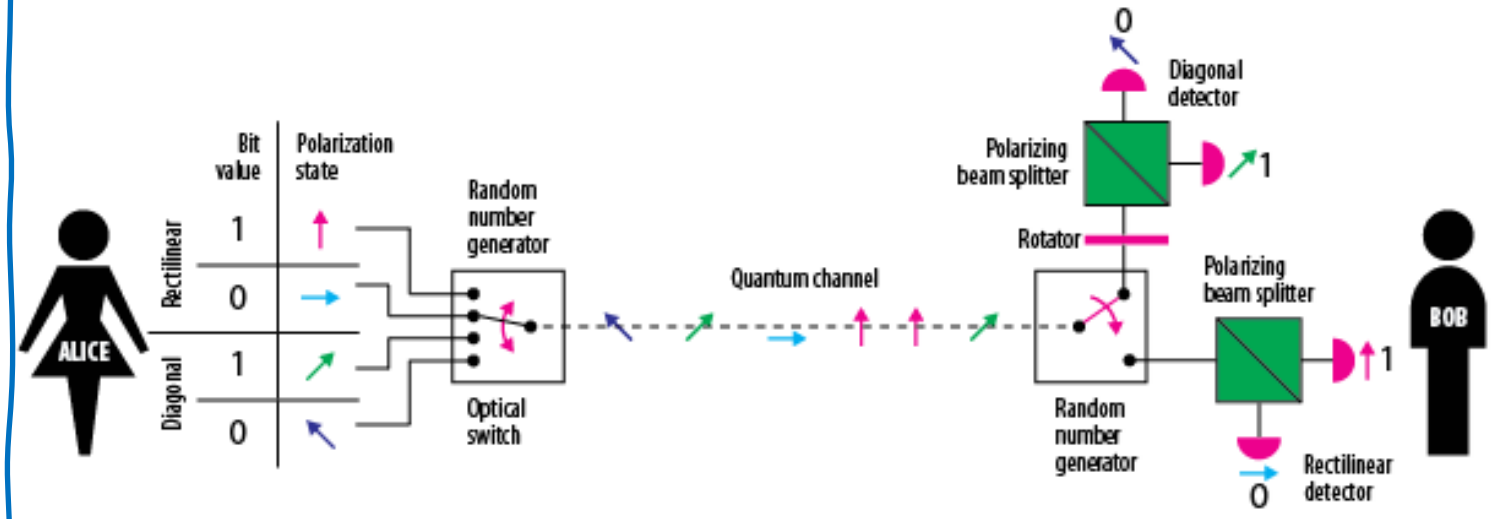
*(Quantum Communication)*

# Quantum Key Distribution (QkD)

**Quantum key distribution** (QKD):

- secure communication method for exchanging encryption keys only known between shared parties;
- based on properties found in quantum physics;
- uses a quantum system to protect the data, rather than relying on mathematics.

**Advantage**: The no-cloning theorem states that it is impossible to create identical copies of an unknown quantum state, which prevents attackers from simply copying the data in the same manner that they can copy network traffic today. Additionally, if an attacker disturbs or looks at the system, the system will change in such a way that the intended parties involved will know.




| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Quantum transmission & detection | ALICE sends photons | ↖ | ↗ | → | ↑ | ↑ | ↗ | ↖ | ↑ |
| | ALICE's random bits | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| | BOB's detection events | ↑ | ↗ | ↖ | ↑ | ↗ | ↗ | ↖ | ↖ |
| | BOB's detected bit values | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Public discussion (i.e., sifting) | BOB tells ALICE the basis choices he made | Rect | Diag | Diag | Rect | Diag | Diag | Diag | Diag |
| | ALICE tells BOB which bits to keep | | ✓ | | ✓ | | ✓ | ✓ | |
| | ALICE and BOB's shared sifted key | – | 1 | – | 1 | – | 1 | 0 | – |

# Challenges & Promises of Quantum Communication

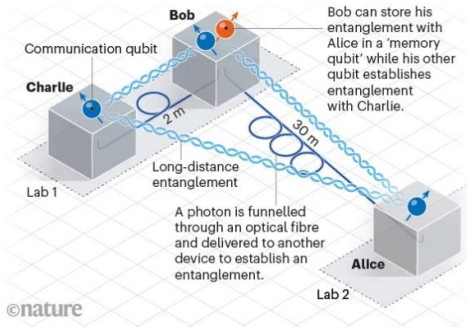
## CHALLENGES

Integration of QKD systems into current infrastructure

Distance in which photons can travel

Difficulties in implementing infrastructure for QKD

## PROMISES




**Quantum Internet**

# Quantum-proof Mitigation Options

*(Post-Quantum Cryptography)*

# NIST Post-Quantum Cryptography Initiative

National Institute of Standards and Technology

Evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms

- 5 years ago NIST initiated a project seeking "to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms."
- Currently in fourth round
- Even if one of NIST 'finalist' solutions is fully developed, tested and proven effective, it can never be fool-proof.

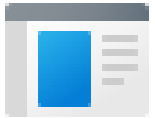
» "We have no absolute guarantee of security for any cryptosystem. The best we can say is that after a lot of study by a lot of smart people, nobody has found any cracks." —Dustin Moody, NIST

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| CRYSTALS-KYBER | CRYSTALS-Dilithium |
| | FALCON |
| | SPHINCS+ |

# Challenges of PQC Migration

PQC protocols efficiency toward Quantum Computers

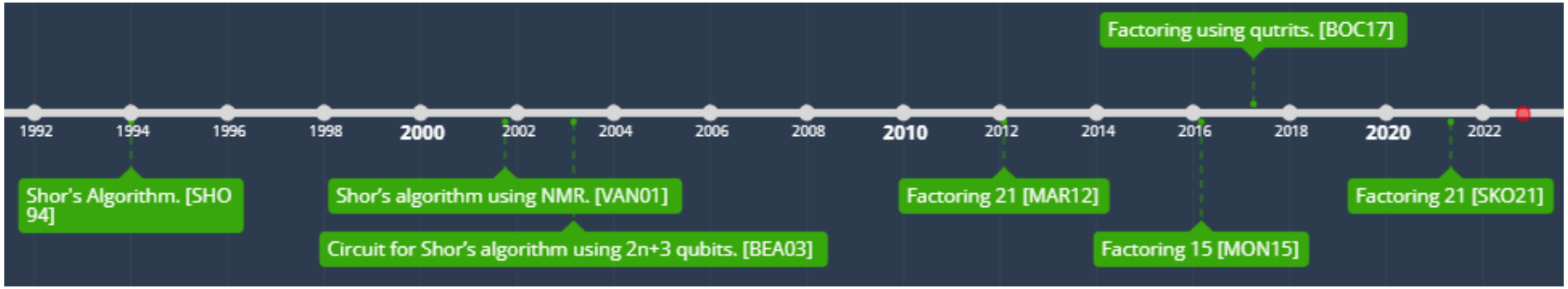
Hardware implementation security issues



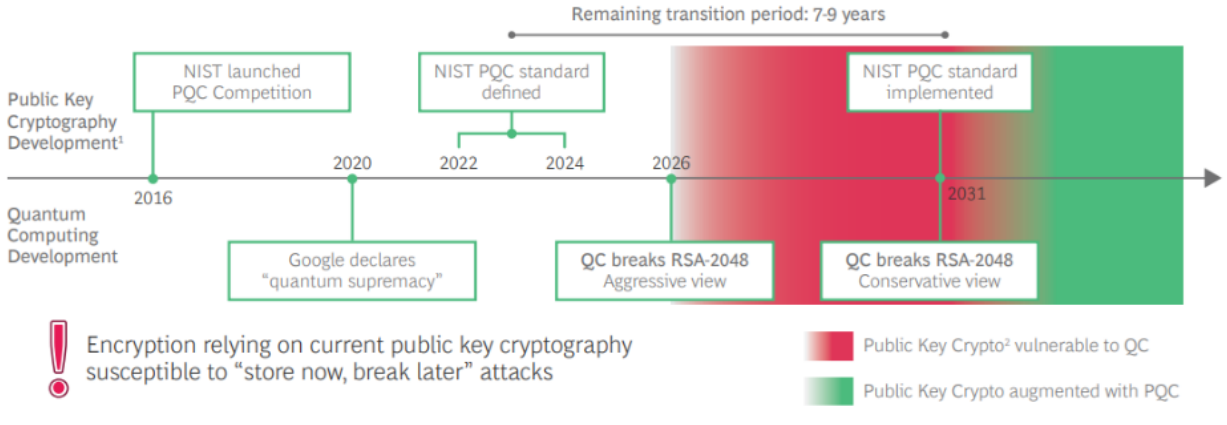
PQC protocols adequacy to applications

# Timeline(s)
# & Regulations

# Forecast & Migration Timelines




## Exhibit 1 - The Time Window for Upgrading Cryptographic Infrastructure Is Closing Rapidly



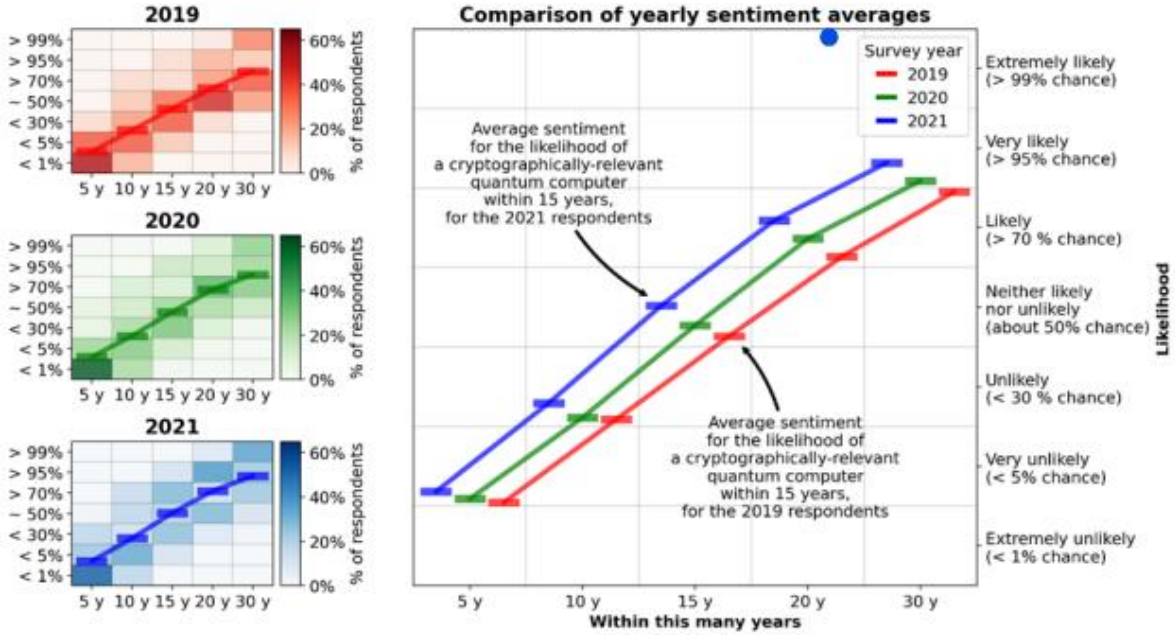

**Sources:** NIST Post-Quantum Cryptography timeline, BCG analysis.

**Note:** PQC: Post-Quantum Cryptography. NIST: National Institute of Standards and Technology USA.

[1]Based on NIST PQC timeline.

[2]Public Key Cryptography (up to RSA-2048).

## Experts' estimates for the likelihood of a quantum computer able to break RSA-2048 in 24 hours - Comparison of yearly surveys



# ANSSI views about PQC Transition - 2022

Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term. However, this immaturity should not serve as an argument for postponing the deployments. ANSSI encourages all industries to initiate in the next months a gradual overlap transition in order to progressively increase trust on the post-quantum algorithms and their implementations while ensuring no security regression as far as classical (pre-quantum) security is concerned.

**What is the recommended post-quantum transition roadmap?**

To support a gradual transition, ANSSI encourages the following 3-phase roadmap (see below for a detailed description):

- Phase 1 (today): hybridation to provide some additional post-quantum *defense-in-depth* to the pre-quantum security assurance.
- Phase 2 (not earlier than 2025): hybridation to provide *post-quantum security assurance* while avoiding any pre-quantum security regression.
- Phase 3 (probably not earlier than 2030): optional standalone post-quantum cryptography.

ANSSI, January 4, 2022
*https://www.ssi.gouv.fr/en/publication/anssi-views-on-the-post-quantum-cryptography-transition/*

# Update on ANSSI views about PQC Transition - 2023

This document is an update of ANSSI's position on the post-quantum cryptography transition in view of the recent advances in the topic. It should be read as an addendum to 2022's publication [1]. We will detail our recommendations in terms of post-quantum algorithms and hybridation techniques.

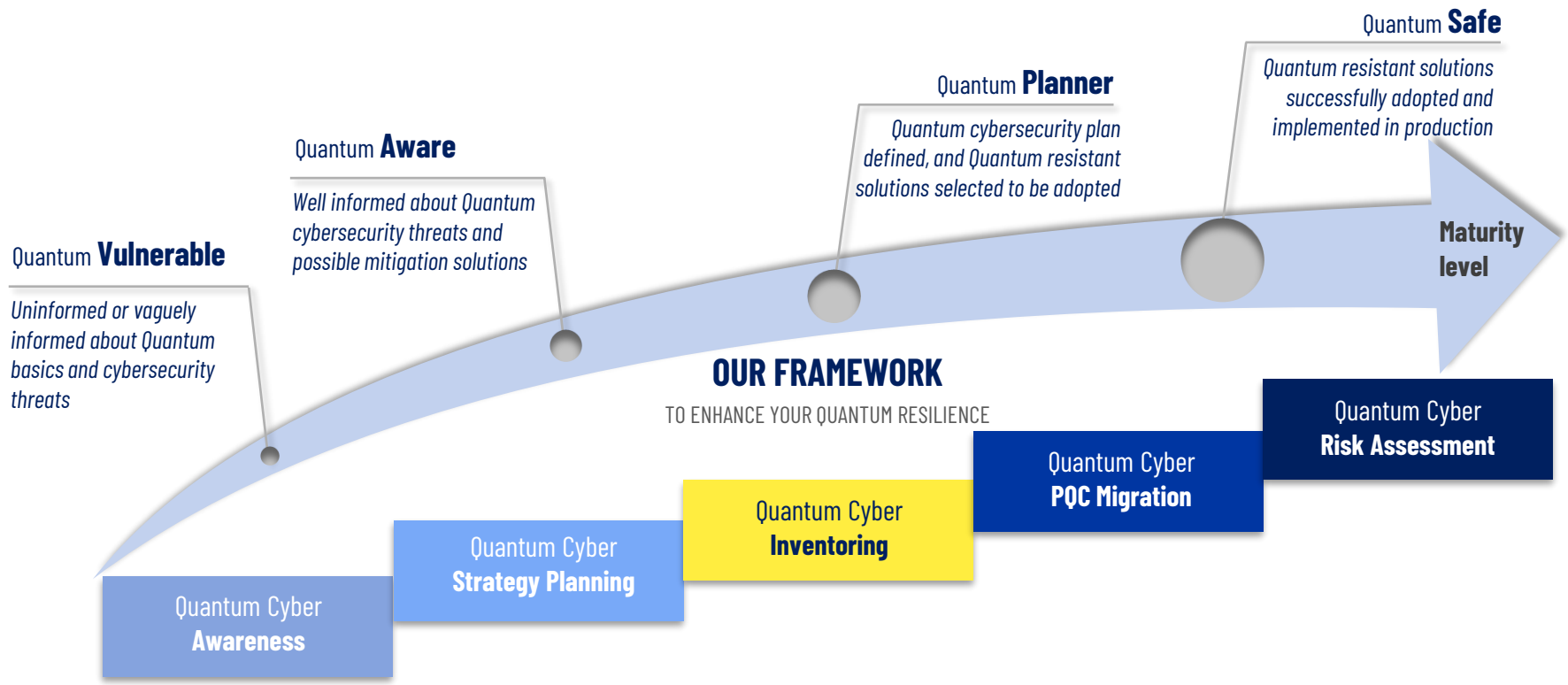
ANSSI also decided to speed-up the original agenda. First French security visas for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024-2025.

1. It is important to avoid modifying the parameters of the standardized instance.
2. The parameters are defined for several minimum security levels. We recommend to use the highest NIST security level as possible, preferably level-5 (i.e. equivalent to AES-256) or level-3 (i.e. equivalent to AES-192).
3. We recommend to use ephemeral keys as much as possible. The systematic use of ephemeral private keys allows to prevent many attacks like decryption failures ones.
4. We also recommend to use the actively secure version (IND-CCA) that will be standardized by NIST. There are some cases, like in provable authenticated protocols, where the passively secure (IND-CPA) version in static or ephemeral mode may still be secure. But an extra care must then be paid to make sure that no decryption oracle is available under any circumstance even in the case of side-channel attacks.

ANSSI, August 29, 2023
*https://www.ssi.gouv.fr/uploads/2023/09/follow_up_position_paper_on_post_quantum_cryptography.pdf*

# PQC Migration Roadmap

# Roadmap to Quantum-Resistant Cryptography



QuRISK ADVISORY

Quantum Risk Advisory
25, quai du Président Paul Doumer
92400 Courbevoie
FRANCE

contact@qurisk.fr