



## Quantum Risk

**Gianbiagio Curato**

Cybersecurity Architecture and Innovation  
Chief Security Office

# Agenda

01

**Quantum Risk**

02

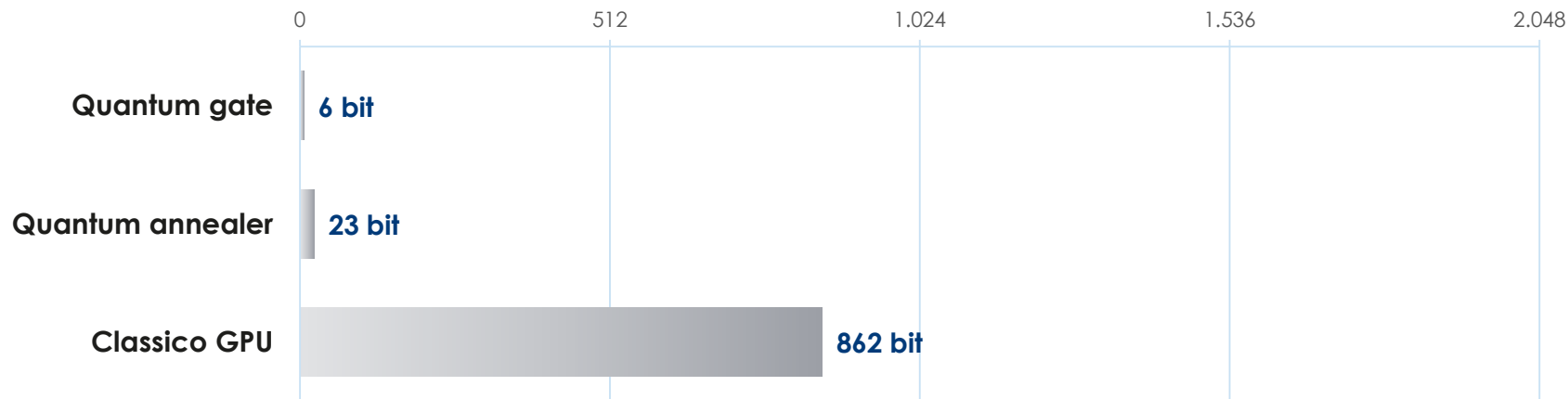
Il Cyberlab e l'esperienza in Quantum Risk

03

Fattorizzazione Benchmark CPU

- **RSA-2048** è lo standard più diffuso di crittografia pubblica asimmetrica
- La chiave pubblica **RSA (N,e)** contiene un semiprimo  **$N = p \times q$**  come modulo pubblico, insieme all'esponente pubblico **e**. I fattori p e q sono segreti
- La chiave privata rimane segreta se **fattorizzare N risulta impraticabile**

**TARGET RSA-2048 · 2.048 bit**

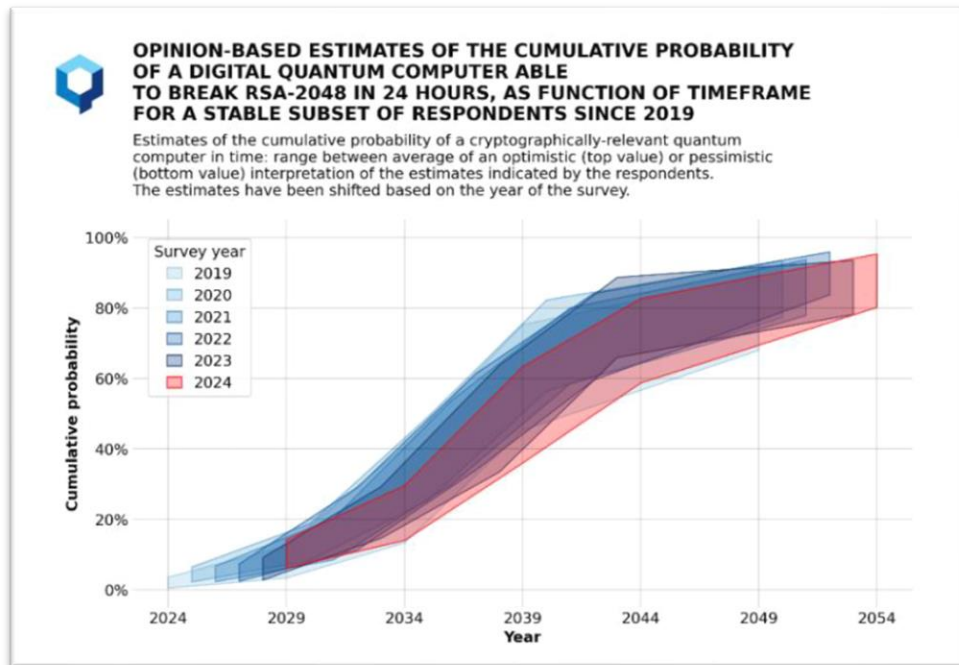


Scala lineare: 6 e 23 bit appaiono come segmenti minimi rispetto al target.

**Nessun record oggi raggiunge RSA-2048; il rischio va gestito come scenario prospettico, con monitoraggio e crypto-agility.**

# Timeline attesa del rischio quantum

- **Rischio Quantistico** è la probabilità di realizzazione di un CRQC entro un certo orizzonte temporale
- **CRQC** è un Computer Quantistico Crittograficamente Rilevante
- Le stime degli esperti indicano una probabilità inferiore al 20% al 2030
- Verrebbero abilitati attacchi del tipo **HNDL** (Harvest Now Decrypt Later)



## Computer Quantistico Crittograficamente Rilevante(CRQC)

- CRQC permette di implementare efficientemente l'algoritmo di Shor.
- I computer quantistici attuali non hanno ancora la potenza di calcolo necessaria a compromettere l'attuale protocollo RSA-2048.
- Le stime non sono stabili nel tempo, a causa dell'immaturità tecnologica.

Source: Mosca, Michele, & Piani, Marco. (2025). Quantum Threat Timeline Report 2025. Global Risk Institute and evolutionQ, Inc.  
<https://globalriskinstitute.org/publication/quantum-threat-timeline-report-2025b/>

# Agenda

01

Quantum Risk

02

**Il Cyberlab e l'esperienza in Quantum Risk**

03

Fattorizzazione Benchmark CPU

# Il Cyberlab contribuisce all'innovazione della Cybersecurity per il Gruppo

Chief Security Officer

Cybersecurity, Antifraud and Business  
Continuity Management

Cybersecurity Architecture and Solutions

Cybersecurity Architecture and Innovation



- Definire framework, standard tecnici e architetturali ai fini cybersecurity, garantire l'adeguatezza in termini di sicurezza dell'architettura complessiva
- Cyberlab**: promuovere l'evoluzione e l'innovazione di misure e soluzioni di cybersecurity, anche attraverso attività di sperimentazione, in coerenza con le strategie del Gruppo ed in considerazione di trend evolutivi e leading practice di riferimento

Le attività del Cyberlab

Quantum Risk



Presidio del rischio quantistico, attraverso attività di analisi, sperimentazione e collaborazioni con **partner accademici** e **leader di mercato**

Digital Asset



Sicurezza di **modelli di tokenizzazione e custodia** degli asset digitali, a supporto dell'evoluzione dei servizi e delle infrastrutture del Gruppo

Tecnologie emergenti



Proof of Concept di tecnologie crittografiche innovative e identificazione di nuovi use case applicativi in ambito bancario

# Agenda

01

Quantum Risk

02

Il Cyberlab e l'esperienza in Quantum Risk

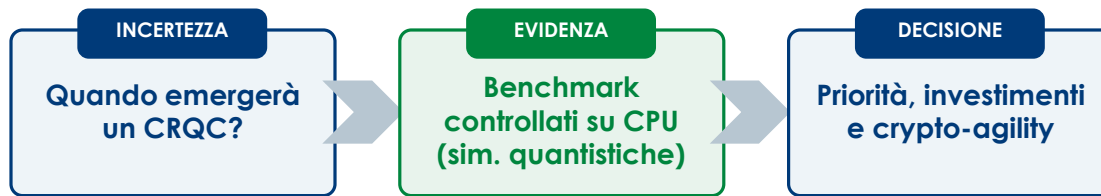
03

**Fattorizzazione Benchmark CPU**

# Dalla previsione alla quantificazione del rischio

7

La data del CRQC resta incerta. Il presidio può evolvere da una timeline basata su stime esterne a un processo empirico, ripetibile e aggiornabile internamente.



## MESSAGGIO STRATEGICO

**Non attendere una data certa. Costruire oggi metriche riproducibili per realizzare progressivamente gli scenari di rischio quantistico.**

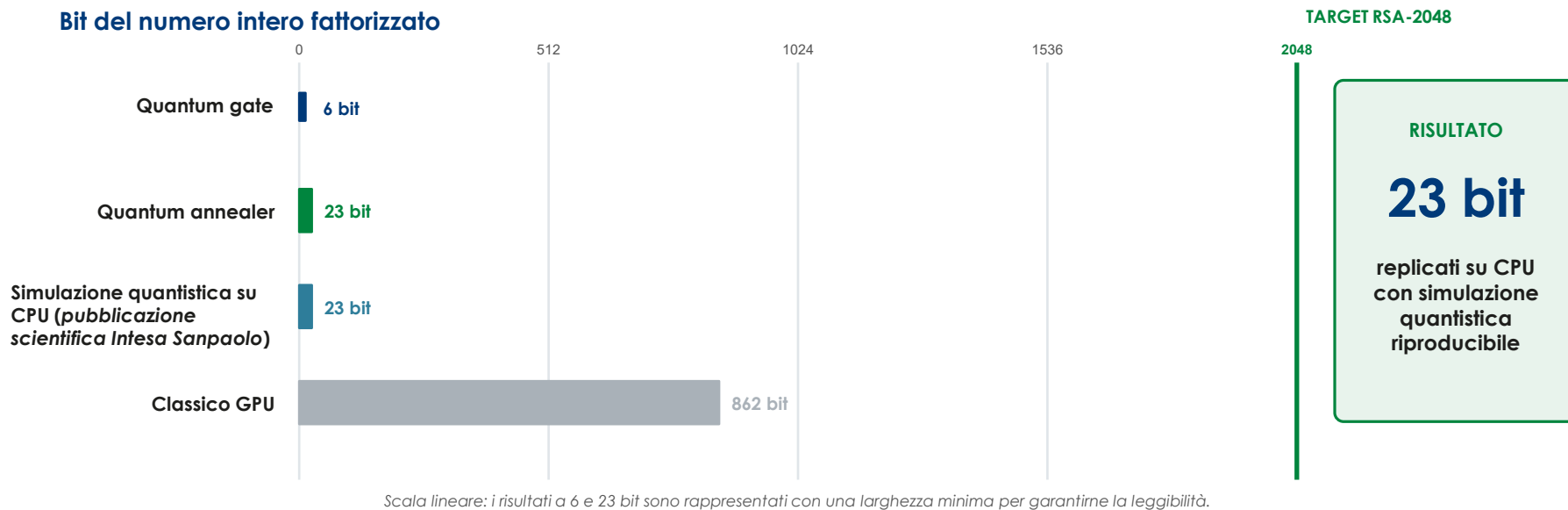
Capacità interna proposta



# Fattorizzazione: scenario attuale

8

## Bit del numero intero fattorizzato



### IMPLICAZIONI

#### CONFRONTO

Stesso numero N del record di fattorizzazione eseguito su un quantum annealer D-Wave.

#### RIPRODUCIBILITÀ

Benchmark eseguibile su infrastruttura CPU controllata.

#### RISCHIO

Base empirica per metriche TTS e studi di scalabilità.

Il benchmark non misura oggi il rischio quantistico su RSA-2048, ma abilita scenari aggiornabili con l'evoluzione di hardware e algoritmi.

Grazie per l'attenzione