CERTFin

BANCHE E SICUREZZA

27 Maggio 2025

Quantum is coming!

Mario Trinchera

Technical Coordinator

TLP:GREEN

La Meccanica Quantistica

CERTFin

La meccanica quantistica è una teoria fisica che descrive il comportamento della materia e dell'energia a livello atomico e subatomico.

È una **teoria controintuitiva** e si basa su principi radicalmente diversi dalla meccanica classica, che ben descrive invece il mondo macroscopico che ci circonda.

Application Development Areas

CERTFin

Lo sviluppo delle tecnologie quantistiche ha dato luogo a diversi filoni applicativi ben distinti:

Quantum Cryptography

*I principi della meccanica quantistica vengono utilizzati per garantire la sicurezza delle comunicazioni, sfruttando fenomeni come l'entanglement e la sovrapposizione degli stati per creare sistemi crittografici inviolabili. Nello specifico, è la **Quantum Key Distribution** (QKD) che permette di rilevare eventuali tentativi di intercettazione grazie alle proprietà quantistiche delle particelle.*

Quantum Communications

Gli stessi principi, applicati alle telecomunicazioni, permetteranno di trasmettere informazioni in modo estremamente sicuro e a lungo raggio. Queste includono tecniche come la Quantum Key Distribution, ma non solo, con l'obiettivo di creare reti di comunicazione resistenti a qualsiasi tipo di intercettazione o attacco.

Quantum Sensing

Il quantum sensing è una tecnologia che utilizza le proprietà della meccanica quantistica per misurare grandezze fisiche con estrema precisione. Questo consente di rilevare cambiamenti minimi in campi magnetici, forze, temperature, e altre grandezze, superando i limiti dei sensori tradizionali. Troverà applicazione in molti ambiti come la medicina, la fisica e la geofisica.

Quantum Computing

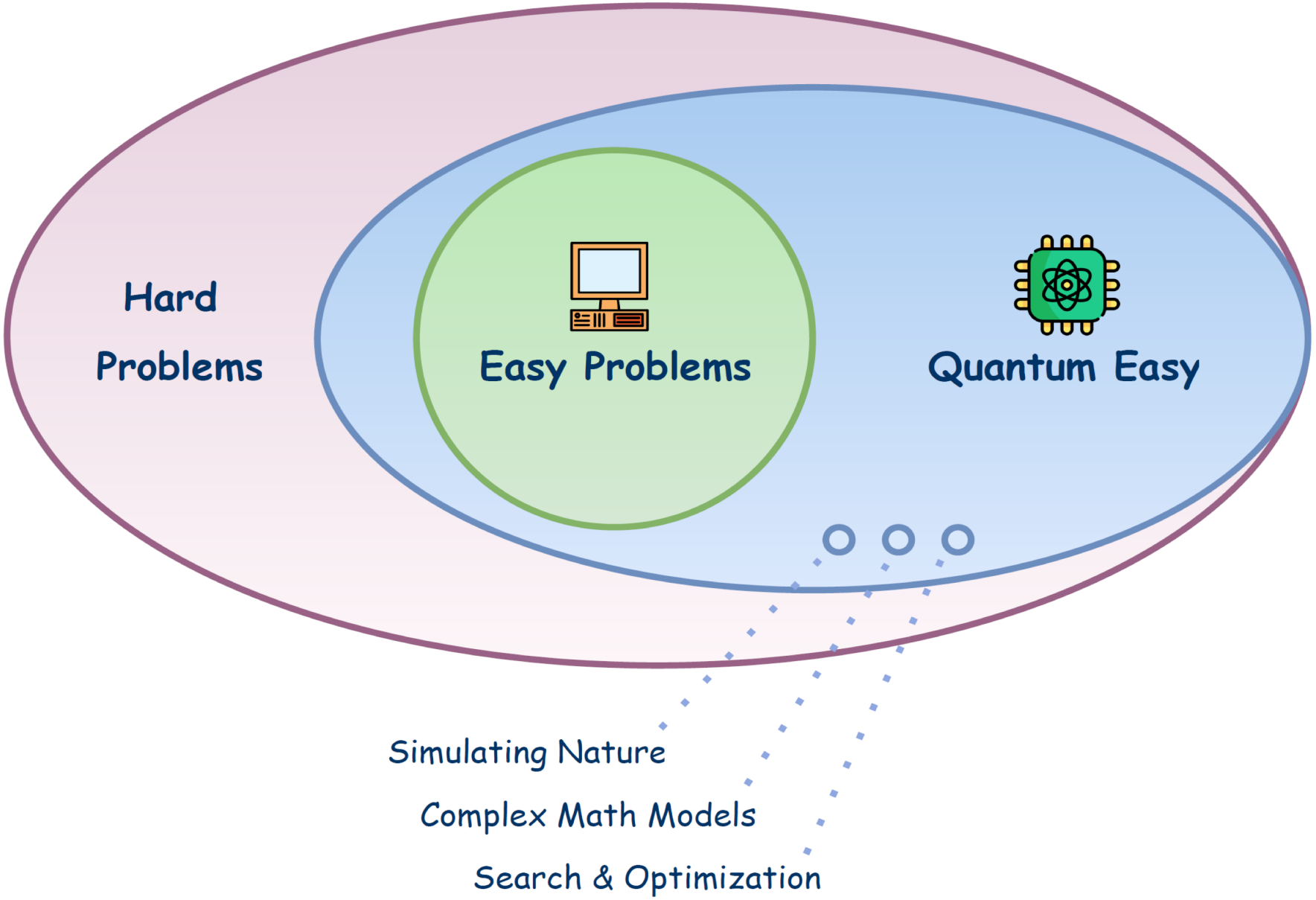
*Il quantum computing è un paradigma di calcolo in cui i principi della meccanica quantistica, come la sovrapposizione e l'entanglement, sono sfruttati a fondo al fine di eseguire operazioni su dati in modo esponenzialmente più veloce rispetto ai computer classici. I quantum computer utilizzano **qubit** al posto dei bit tradizionali, permettendo di risolvere problemi complessi impraticabili per i calcolatori convenzionali.*

Post-Quantum Cryptography

La crittografia post-quantistica è un insieme di suite e algoritmi crittografici progettati per essere resistenti agli attacchi effettuati con computer quantistici. Questi algoritmi mirano a sostituire le attuali tecniche crittografiche, come RSA ed ECC, che diventerebbero vulnerabili con l'avvento della computazione quantistica. L'obiettivo è garantire la sicurezza delle informazioni anche nell'era dei computer quantistici avanzati.

Quantum Computing

CERTFin



Computer Quantistico vs Computer Classico

CERTFin

Come capire se, per un certo calcolo, è conveniente utilizzare un computer quantistico?

Quantum Speedup

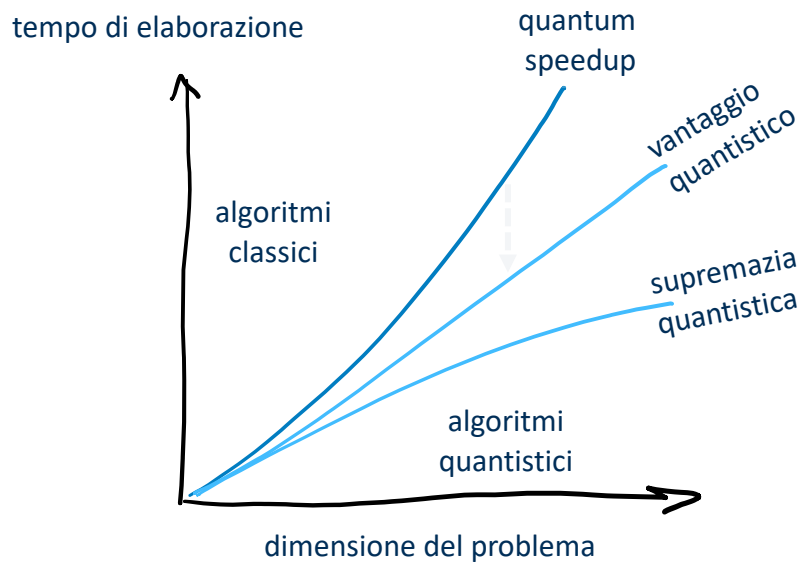
Per uno specifico problema, un algoritmo quantistico supera un algoritmo classico in termini di scalabilità rispetto alla crescita del problema.

Quantum Advantage

Un computer quantistico può eseguire un particolare calcolo in modo significativamente più veloce del miglior computer classico (es. Fattorizzazione)

Quantum Supremacy

Il quantum computer riesce a risolvere un problema che non sarebbe risolvibile da un computer classico

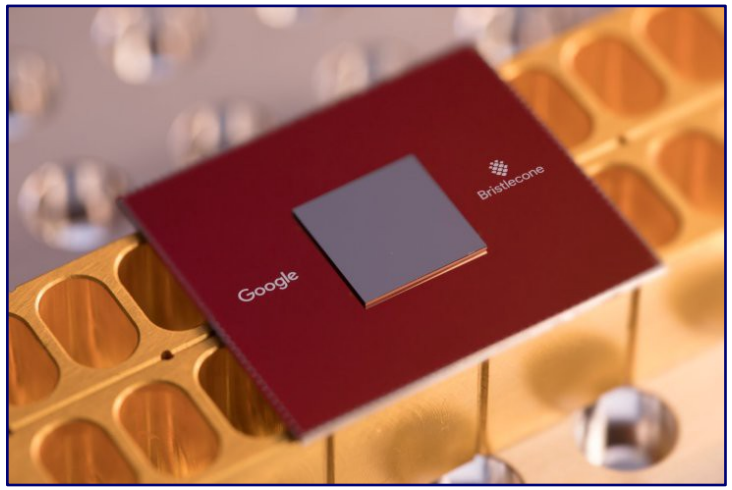


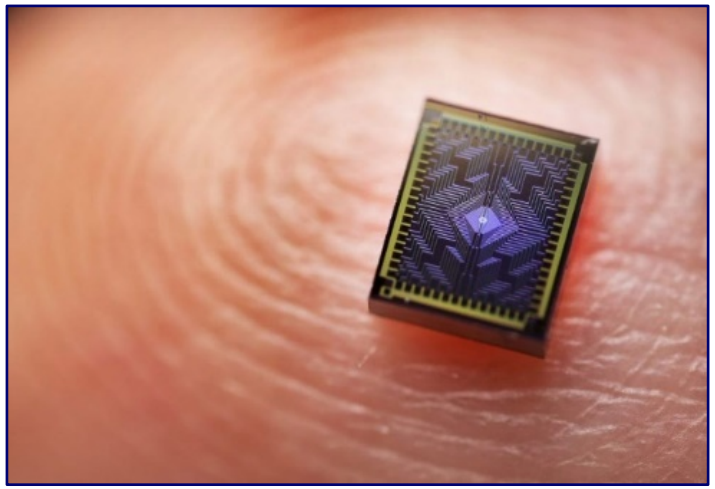
All'abbassarsi della curva, lo speedup diventa **esponenziale** e il quantum computing risulta vantaggioso anche per problemi relativamente «piccoli»

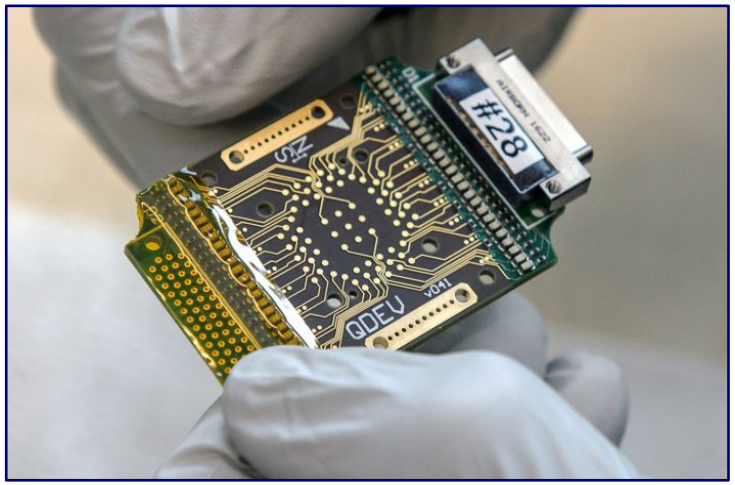
Fonte: MIT, Q2B Conference 2019

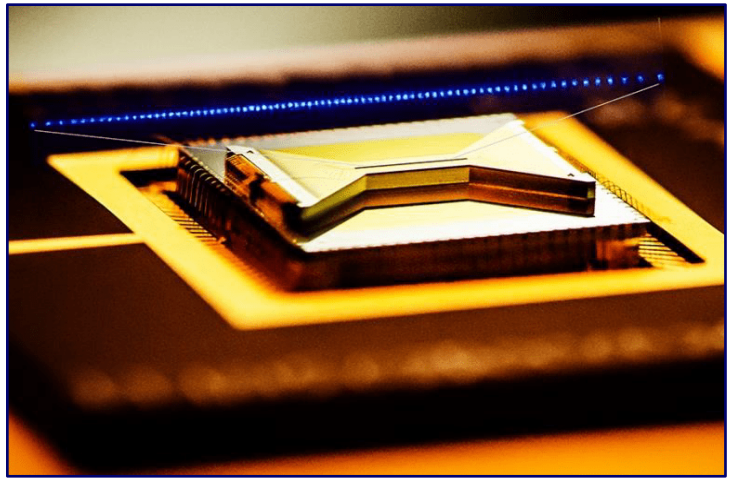
Diversità di approcci al Quantum Computing

CERTFin









Credit: IBM, Google, Intel, Microsoft, IonQ, D-Wave

CERTFin

BANCHE E SICUREZZA

27 Maggio 2025

Quantum is coming!

Mario Trinchera

Technical Coordinator

TLP:GREEN

Post-Quantum Cryptography

CERTFin

La *crittografia post-quantistica* è lo studio di sistemi crittografici che possono essere eseguiti su computer classici ma continuano a garantire la confidenzialità **anche se un attaccante può avvalersi di un computer quantistico**.

La sicurezza degli attuali sistemi crittografici **a chiave pubblica** è basata su problemi che consideriamo molto difficili, ovvero problemi per i quali non si conosce un algoritmo polinomiale che conduca alla soluzione. Tali problemi, matematicamente chiamati **NP-hard** (*Non-deterministic polynomial-time hard problems*), sono fondamentalmente di tre tipologie:

- il calcolo della fattorizzazione in numeri primi (**RSA**)
- il calcolo del logaritmo discreto in campo finito (**El Gamal**)
- il calcolo del logaritmo discreto dei punti di una curva ellittica (**ECC**)

Tali tipologie di problemi ricadono tutte in quella classe di problemi che può essere risolta in modo efficiente e senza difficoltà, ad esempio usando l'**algoritmo di Shor**, da un computer quantistico sufficientemente potente.

Dunque, lo sviluppo dei computer quantistici mette in serio pericolo tutte le applicazioni basate sulle confidenzialità (il traffico TLS, la conservazione di dati sensibili, le sicurezza delle transazioni, etc.).

La Standardizzazione del NIST

CERTFin

Nel dicembre del 2016, il NIST ha avviato un processo di standardizzazione di algoritmi crittografici **capaci di resistere ad attacchi basati su computer quantistici**, lanciando una competizione internazionale aperta a candidati provenienti da aziende ed enti di ricerca di tutto il mondo, durata 3 round e terminata a fine 2022.

NIST Post-Quantum Cryptography Standardization

Call for Proposal - First Round

- 82 total submissions received
  - 23 signature schemes
  - 59 Encryption/KEM schemes

	Signatures	KEM/Encryption	Overall
Lattice-based	4	24	28
Code-based	5	19	24
Multi-variate	7	6	13
Hash-based	4		4
Other	3	10	13
Total	23	59	82

L'algoritmo per la crittografia a chiave pubblica scelto per il nuovo standard è **CRYSTALS-Kyber**.

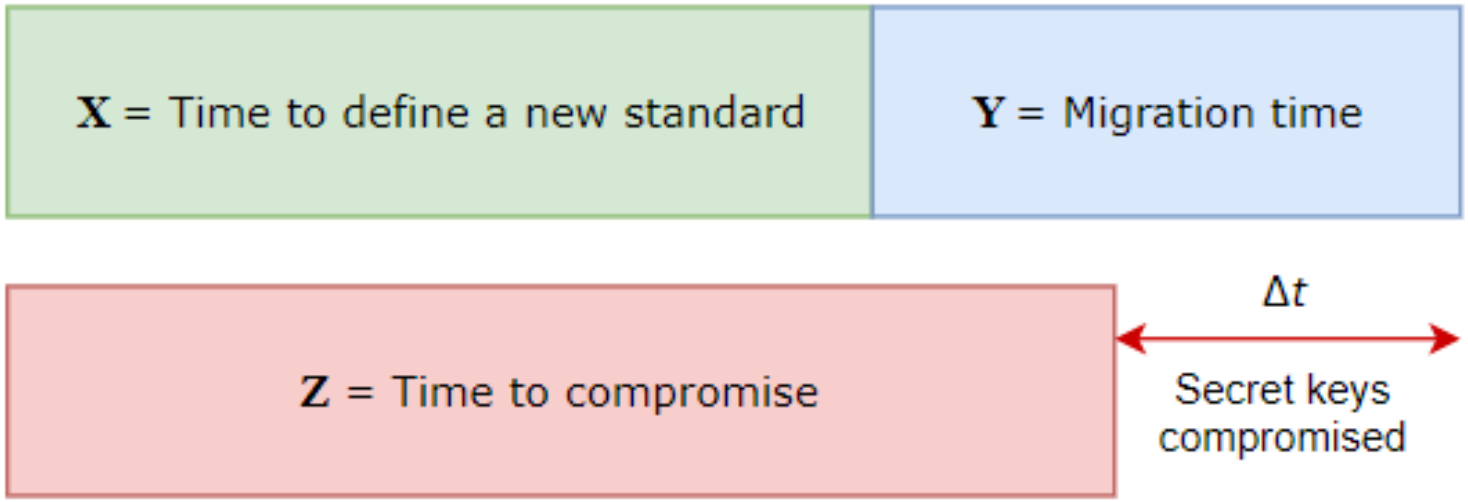
Gli algoritmi per le firme digitali che saranno standardizzati sono **CRYSTALS-Dilithium, FALCON** e **SPHINCS+**.

Processo di Migrazione

CERTFin

La migrazione verso algoritmi *quantum-resistant* è un passo preventivo per garantire che i sistemi di sicurezza delle informazioni rimangano **robusti e affidabili** anche quando la computazione quantistica diventerà una realtà pratica e scalabile.

La migrazione verso tecnologie quantum-safe richiede risorse significative in termini di tempo, denaro e competenze e poiché un processo di migrazione strutturato passa attraverso delle fasi fondamentali dalle quali non si può prescindere, **è prudente iniziare il processo con opportuno anticipo** per evitare future esposizioni a rischi.



Processo di Migrazione

CERTFin

Negli Stati Uniti si è già aperta la strada alla transizione verso un'informatica quantum safe: nel dicembre 2022, il presidente degli Stati Uniti, Joe Biden, ha firmato il **Quantum Computing Cybersecurity Preparedness Act**, che stabilisce una serie di obblighi per le agenzie federali per preparare la loro transizione alla crittografia post-quantistica con una roadmap tanto precisa quanto stringente.

La National Security Agency (NSA) ha infatti pubblicato un aggiornamento della *Commercial National Security Algorithm Suite* (CNSA 2.0) in cui si prescrive che questa transizione dovrà essere completata entro il 2033, secondo il programma descritto nella seguente tabella:

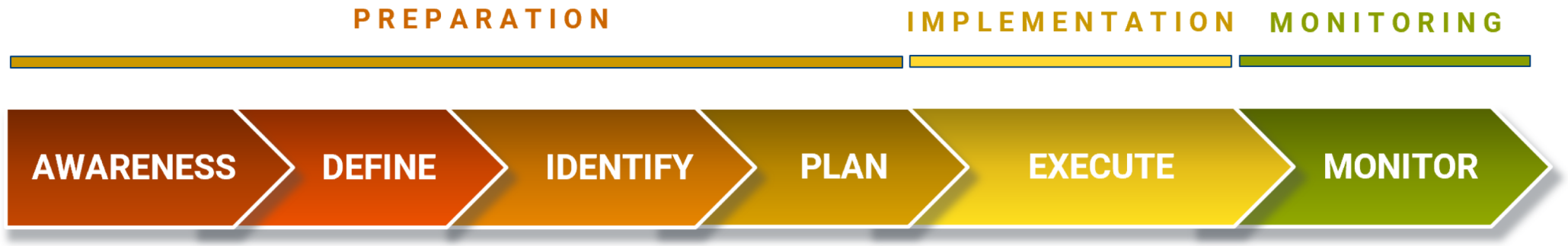
Timing for:	**Support/Prefer CNSA 2.0**	**Exclusively Use CSNA 2.0**
Software and firmware signing	2025	2030
Web browsers/servers and cloud services	2025	2033
Traditional networking equipment (VPNs, routers, switches	2026	2030
Operating systems	2027	2033
Niche equipment - constrained devices, large public key infrastructure systems	2030	2033

Processo di Migrazione: Metodologie

CERTFin

CSA	Education & Awareness	Create a Post-Quantum Project		Take Data Protection Inventory	Analysis & Planning	Implement PQ Migration
ETSI	Create a Crypto-Inventory		Preparation on a Mitigation Plan		Implement the Mitigation Plan	
DHF	Awareness	Data Inventory	System Inventory	Updating Regulations	Plan the Transition	Execute the Transition
WEF	Define	Identify		Plan		Execute
CFDIR	Preparation	Discovery	Risk Assessment	Risk Mitigation	Migration	Validation
FS-ISAC	Discovery	Risk Assessment	Vendor Assessment	Create a Migration Framework	Apply a Risk Model	Remediation

Processo di Migrazione: approccio CERTFin



Awareness: *finalizzata ad allineare il management, informando e fornendo tutti gli elementi utili a rendere comprensibili i rischi associati ad a facilitare una scelta decisionale che eviti la gestione tardiva della problematica.*

Define: *Definizione degli obiettivi, della strategia, della costruzione di una roadmap, stima del budget necessario, creazione del gruppo di lavoro, etc. È fondamentale focalizzare le aspettative sul breve, medio e lungo termine*

Identify (o Discovery): *Identificare tutti gli ambiti in cui vengono utilizzati algoritmi di cifratura (applicazioni, hw e servizi) sia dall'azienda sia dalle terze parti. Lo scopo primario è quello di costruire un* ***crypto-inventory*** *interrogabile*

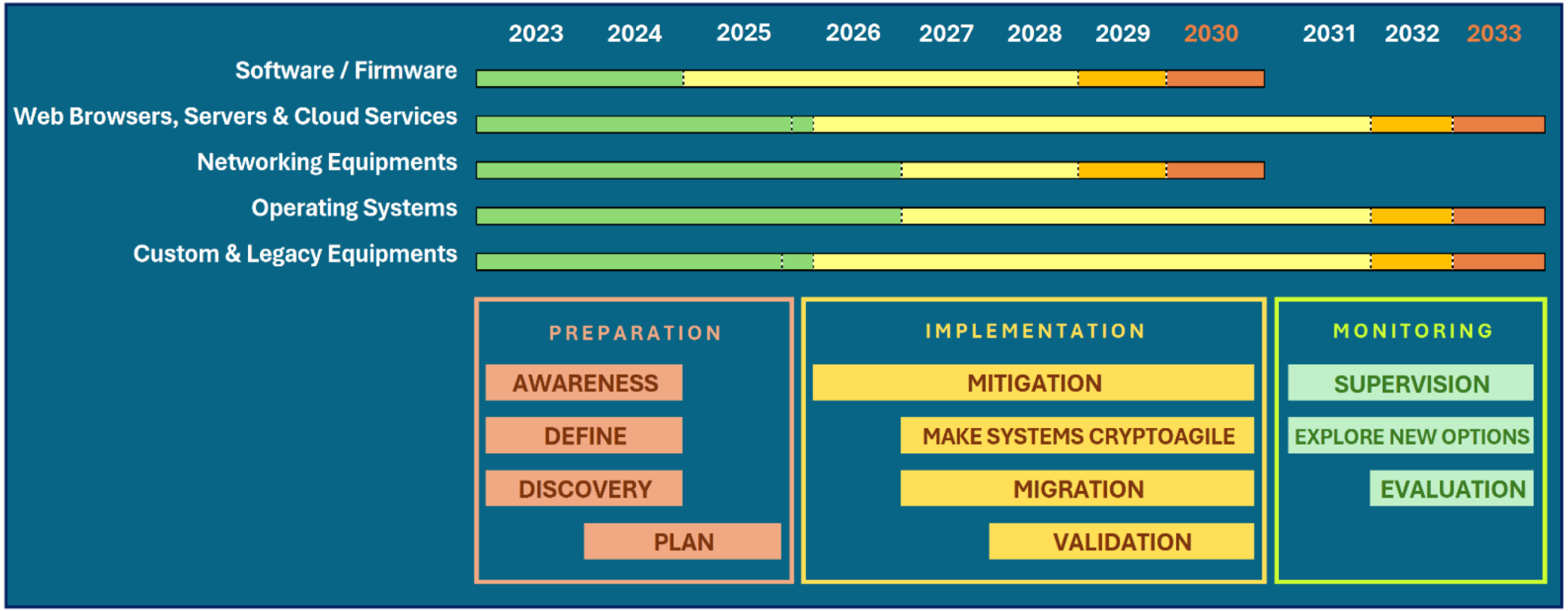
Plan (o Analysis/Risk Assessment): *in questa fase si pianificano gli interventi in linea con un "Quantum Threat Model" finalizzato ad assegnare delle priorità di intervento.*

Execute: Implementare l'utilizzo di logiche ibride e/o logiche interamente post-quantum. In questa fase, ha senso concentrarsi sul rendere i sistemi e le infrastrutture ***crypto agili***.

Monitor: *Fase di supervisione in cui si osservano e analizzano potenziali minacce emergenti ma si valutano anche nuove alternative in grado di offrire un grado di sicurezza maggiore.*

Processo di Migrazione: approccio CERTFin

Mettendo insieme la roadmap statunitense e le varie fasi del processo, si ottiene anche una indicazione cronologica sugli step attuativi:



CERTFin

Grazie!

ricerca@certfin.it

TLP:GREEN