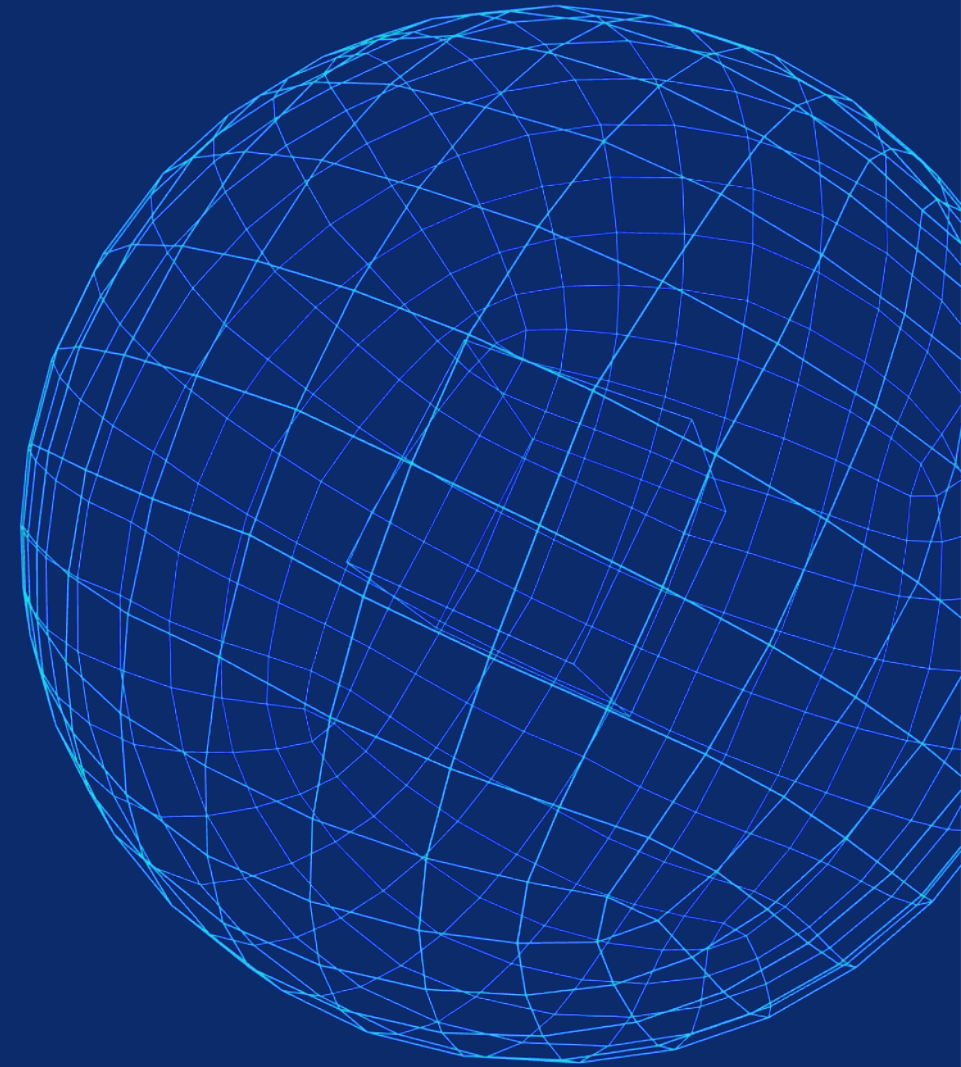


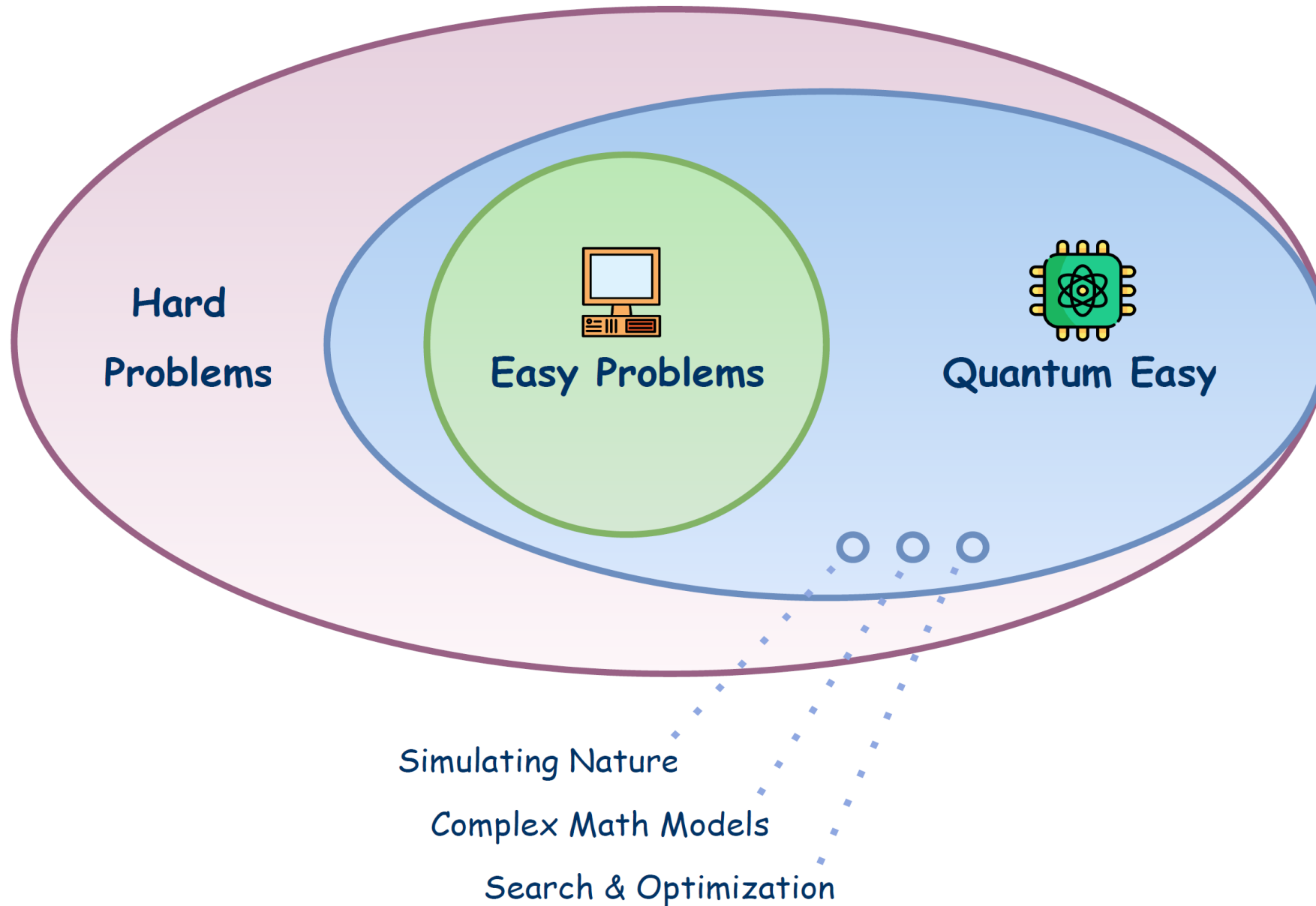
22 settembre
2026

Quantum is Coming!

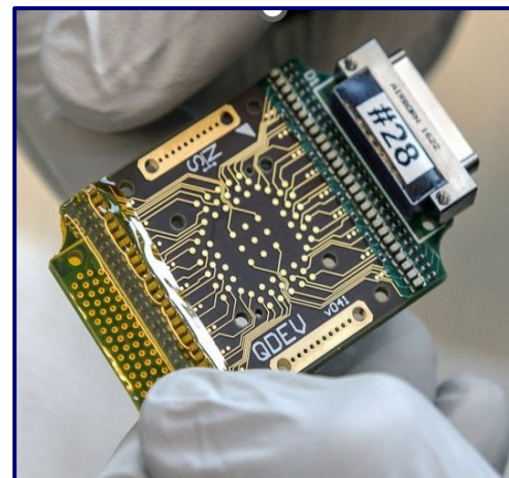
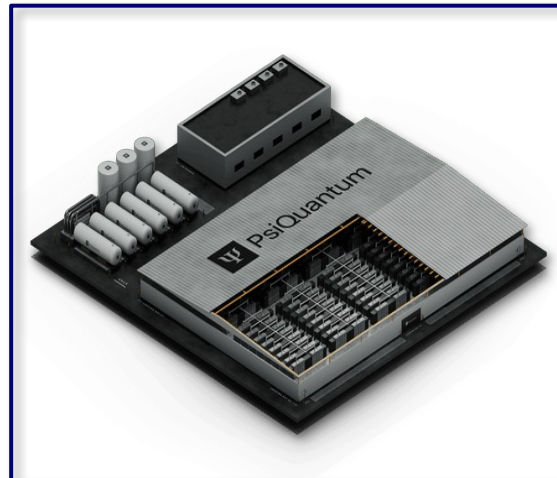
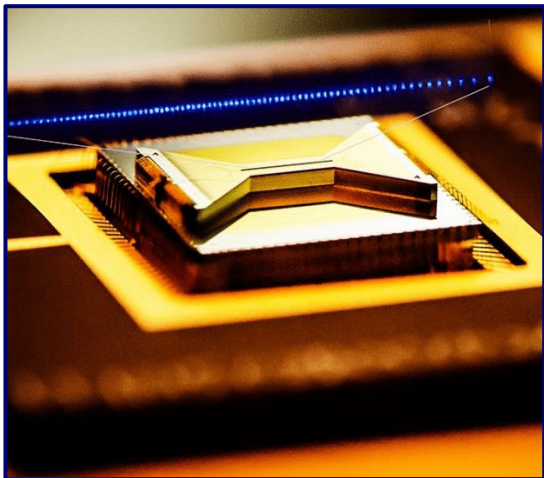
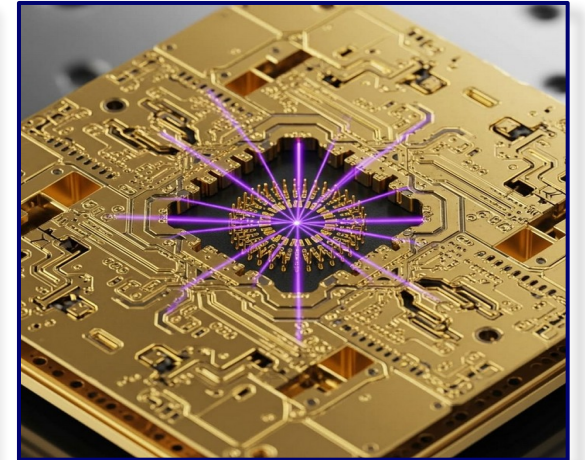
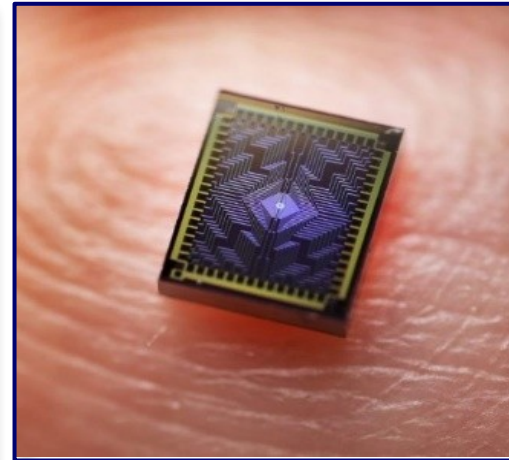
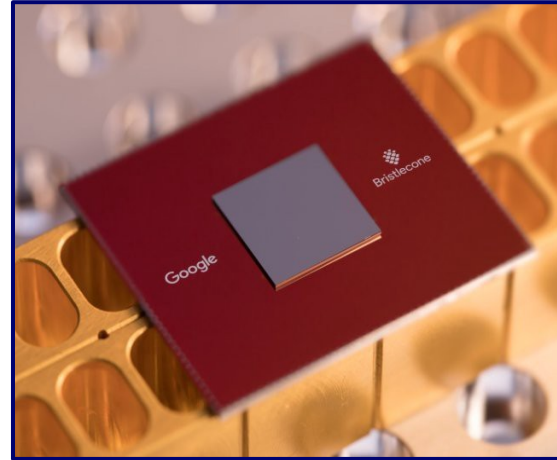
Mario Trinchera
Technical Coordinator



Quantum Computing



Diversità di approcci al Quantum Computing



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

La Standardizzazione del NIST

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

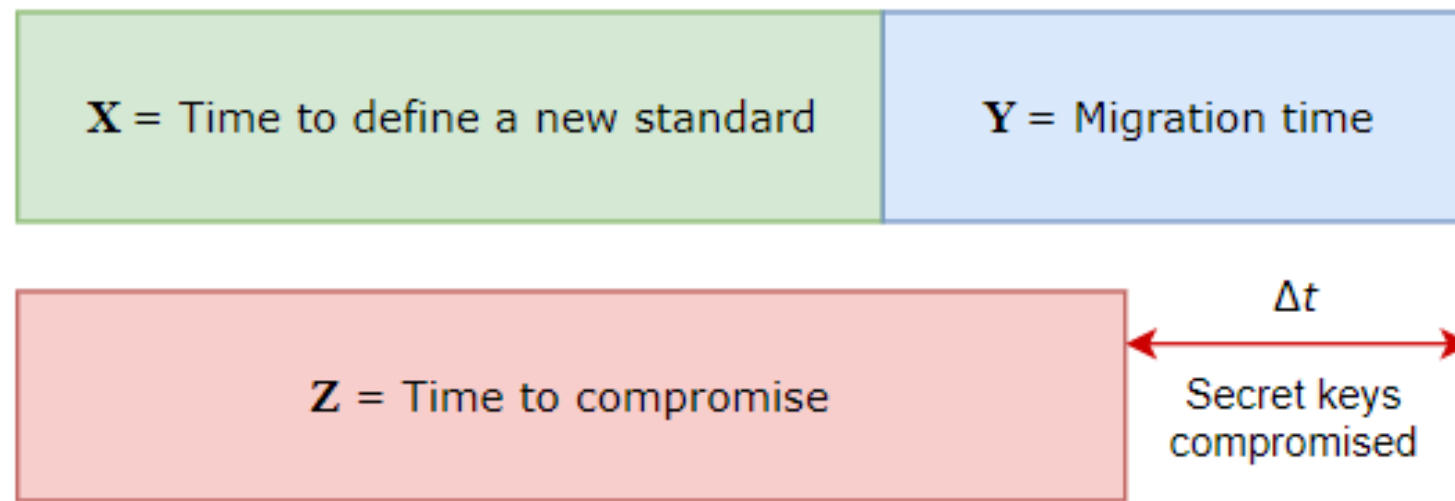
L'algoritmo per la crittografia a chiave pubblica scelto per il nuovo standard è **CRYSTALS-Kyber**.

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

Processo di Migrazione

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: Roadmap G7

In ambito G7, a fine 2025, il Cyber Expert Group ha definito una indicazione cronologica sugli step attuativi:





Defen
d.

Infor
m.

Evolve
.

GRAZIE!

Ricerca@certfin
.it