

WORKSHOP · CRITTOGRAFIA E CYBERSECURITY

DAL SUPERCALCOLO AL QUANTUM

CINECA, infrastruttura pubblica di ricerca, e la sfida quantistica alla crittografia

Fabio AFFINITO



Ancona

8 Ottobre 2026

CONSORZIO NON PROFIT

Dal 1969 al servizio del sistema accademico italiano



123 MEMBRI

2 ministeri, 71 università, 50 istituzioni accademiche e di ricerca



6 SEDI

Bologna, Milano, Roma, Napoli, Chieti, Palermo



≈ 1000

dipendenti nel 2025



≈ 160 MLN €

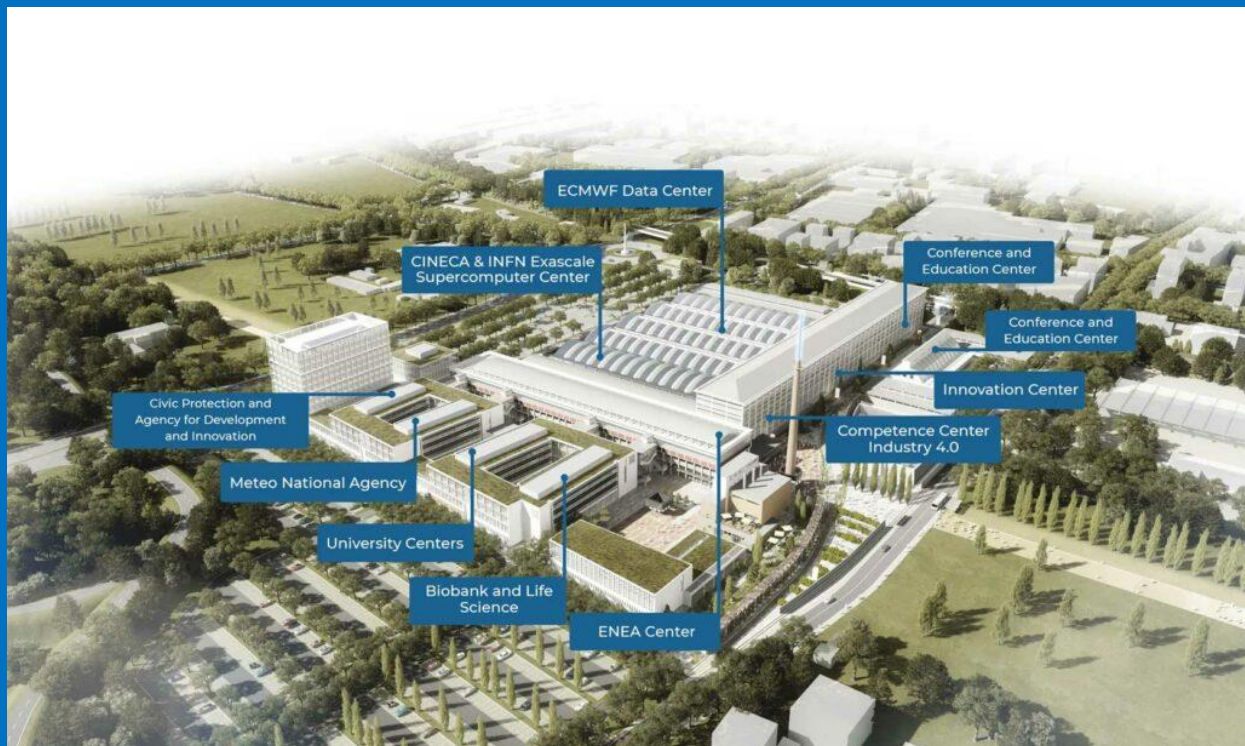
ricavi annui nel 2025



BOLOGNA • DATA VALLEY

TECNOPOLO DAMA

Supercalcolo, intelligenza artificiale e calcolo quantistico nella stessa sede, accanto al data center del centro meteo europeo



TECNOPOLO DATA MANIFATTURA EMILIA-ROMAGNA

EUROHPC · PRE-EXASCALE

LEONARDO

250 PF

PETAFL0P/S DI PICCO

#10

NELLA CLASSIFICA TOP500

13.824

GPU NVIDIA A100



SESSANT'ANNI DI CALCOLO PUBBLICO



Anni '60

Il primo
supercalcolatore
italiano



2022

Leonardo entra nella
rete EuroHPC



2024-25

AI Factory: il calcolo
per l'intelligenza
artificiale



2026

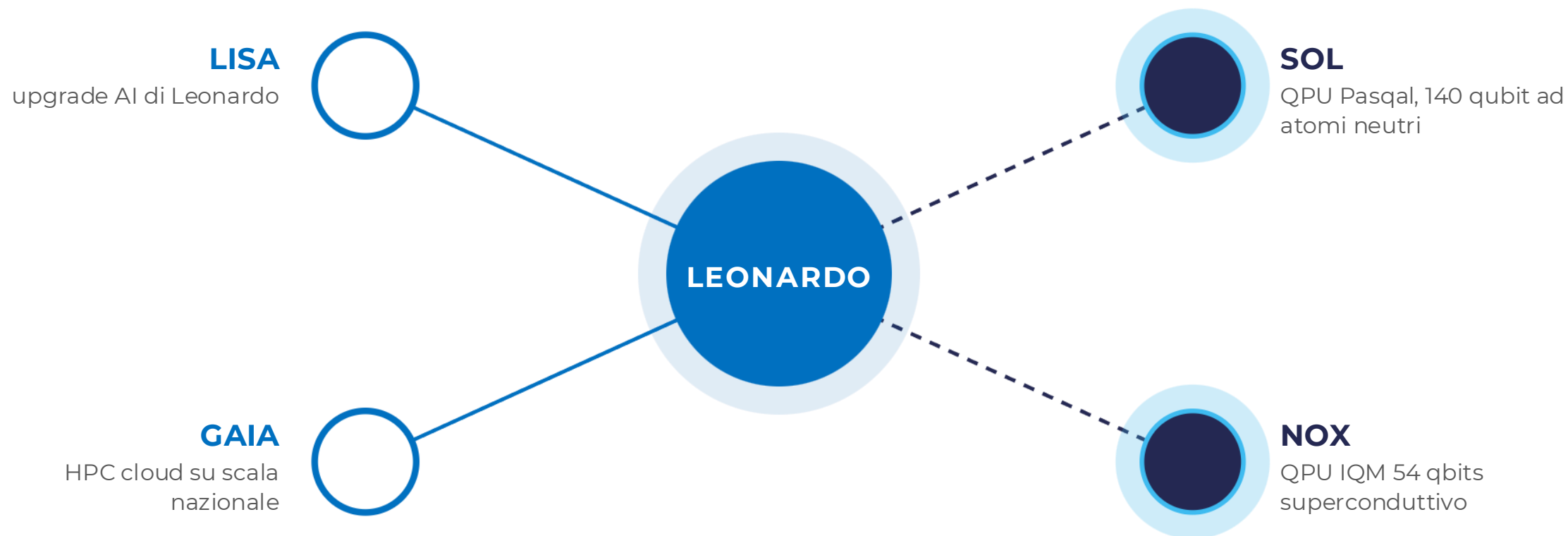
LISA, SOL e NOX: HPC,
AI e quantum



Domani

Calcolo ibrido e
infrastrutture
quantum-safe

UN ECOSISTEMA COSTRUITO ATTORNO A LEONARDO



Linea continua: risorse classiche · Linea tratteggiata: risorse quantistiche

DUE TECNOLOGIE QUANTISTICHE, UN'UNICA INFRASTRUTTURA



SOL • PASQAL ORION

140 qubit ad atomi neutri

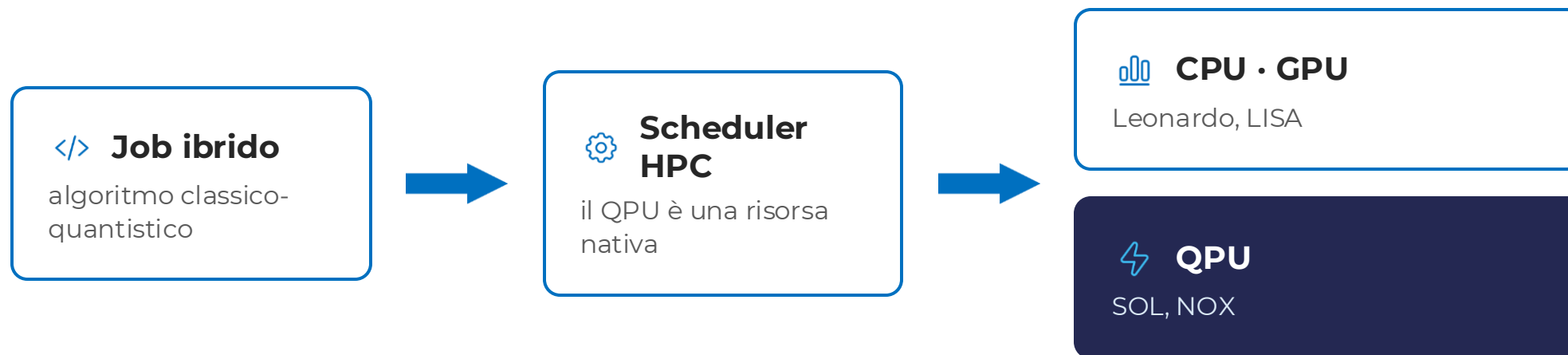


NOX IQM RADIANCE 54

Qubit superconduttivi, a temperature criogeniche

Inaugurati l'11 giugno 2026 al Tecnopolo DAMA · co-finanziati da EuroHPC JU e MUR tramite ICSC

IL QPU COME ACCELERATORE DEL SUPERCALCOLATORE



43 QUBIT

emulati su 2.048 GPU NVIDIA A100: una delle più grandi simulazioni statevector di un algoritmo di ottimizzazione



Q-DAY

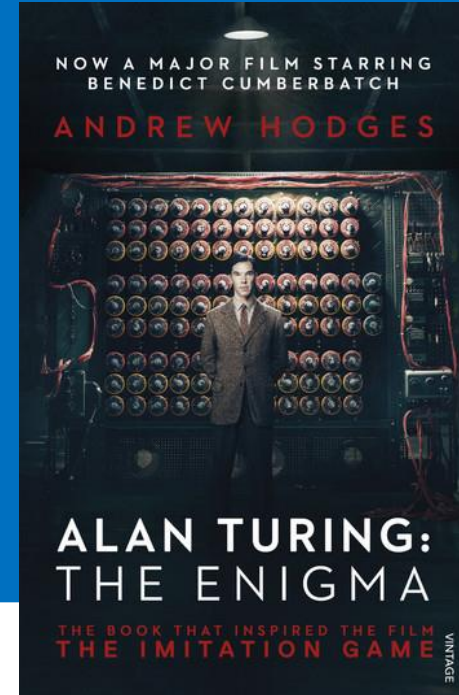
E LA CRITTOGRAFIA?

Un computer quantistico abbastanza grande romperebbe la crittografia a chiave pubblica che protegge Internet oggi.

DA ENIGMA AI QUBIT

158.962.555.217.826.360.000

impostazioni possibili di Enigma, ogni giorno



1940

La Bombe di Turing

Crib e logica

Non prova tutto: scarta le impostazioni impossibili partendo da parole note nei messaggi



OGGI

Leonardo

≈ 10 minuti

Stima giocosa: un'operazione per combinazione a 250 petaflop/s



DOMANI

Computer quantistico

≈ 13 miliardi

di passi con Grover ($\sqrt{N}$). Ma il vero bersaglio non è Enigma: è RSA, con Shor

Turing vinse con matematica e macchine. Oggi la sfida si ribalta: una crittografia che nessuna macchina sappia rompere.

COSA SI ROMPE, COSA REGGE



CHIAVE PUBBLICA

RSA · ECC · Diffie-Hellman

Algoritmo di Shor: fattorizzazione e logaritmo discreto diventano trattabili

Da sostituire



SIMMETRICA E HASH

AES · SHA-2 · SHA-3

Algoritmo di Grover: solo un vantaggio quadratico sulla ricerca esaustiva

Basta chiavi più lunghe: AES-256

HARVEST NOW, DECRYPT LATER

RACCOGLI OGGI, DECIFRA DOMANI

$$x + y > z$$

Se gli anni di riservatezza richiesti (x) più quelli per migrare (y) superano gli anni all'arrivo del computer quantistico (z), si è già in ritardo.

1

Oggi

traffico cifrato intercettato

2

Per anni

archiviato in attesa

3

Domani

decifrato con un computer quantistico

DUE RISPOSTE COMPLEMENTARI



MATEMATICA

CRITTOGRAFIA POST-QUANTISTICA

Nuovi problemi difficili, su hardware classico

NIST FIPS 203 · 204 · 205 (2024): ML-KEM, ML-DSA, SLH-DSA



FISICA

DISTRIBUZIONE QUANTISTICA DI CHIAVI

Chiavi trasmesse con fotoni: chi intercetta si rivela

Richiede fibra dedicata, distanze limitate, nodi fidati

ACN • CINECA

SUPERCALCOLO PER LA CYBERSICUREZZA NAZIONALE

L'Agenzia per la cybersicurezza nazionale porta a Napoli
il proprio sistema HPC, gestito da CINECA

1

2023 • Protocollo d'intesa

ACN mette oltre 20 mln €; CINECA è stazione appaltante e gestore del sistema

2

Ricerca e sviluppo

Attività congiunte su HPC; accesso per l'ecosistema cyber coordinato da ACN

3

27 giugno 2025 • Megaride

Inaugurato nel data center CINECA di Napoli, a San Giovanni a Teduccio

Fonti: protocollo d'intesa (settembre 2023);
comunicato ACN-MUR-ICSC-CNR-CINECA-UNINA
(giugno 2025)

NAPOLI • SAN GIOVANNI A TEDUCCIO

MEGARIDE

28.000

CPU

340

GPU

≈ 50 mln €

INVESTIMENTO COMPLESSIVO



Interconnesso con Leonardo: Bologna e Napoli lavorano come un'unica infrastruttura



Nucleo di HyperSOC, la piattaforma ACN a supporto dei Security Operations Center

QUID · EUROQCI ITALIA

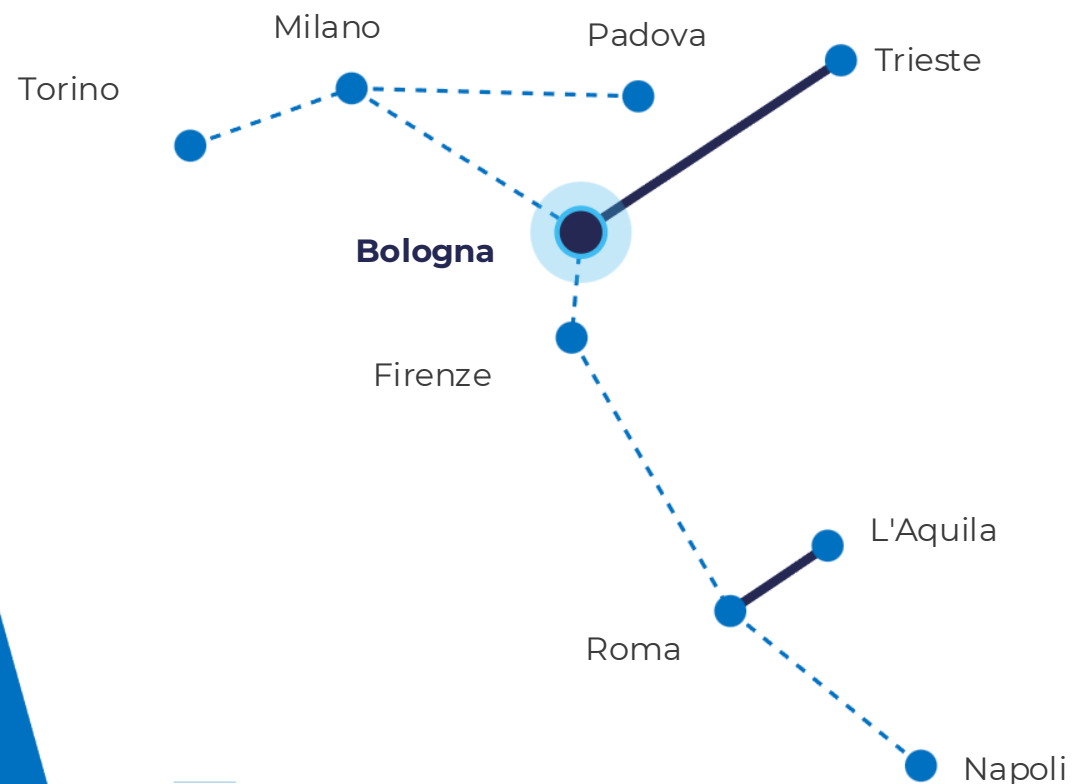
LA RETE QUANTISTICA ITALIANA

14+

nodi QKD in reti metropolitane di 9 città

2

collegamenti a lunga distanza: Bologna–Trieste
e Fucino–L'Aquila–Roma



Fonte: progetto QUID, coordinato da INRiM · schema indicativo

IL RUOLO DI UN CENTRO DI CALCOLO PUBBLICO



SIMULARE

Emulare algoritmi quantistici per capire quanto è vicina la minaccia



MISURARE

Provare e confrontare la PQC su sistemi reali e su larga scala



PROTEGGERE

Rendere quantum-safe servizi, reti e dati della ricerca



FORMARE

Scuole e corsi sul calcolo quantistico per la comunità



CINECA

[email relatore]
hpc.cineca.it

GRAZIE

Domande?

