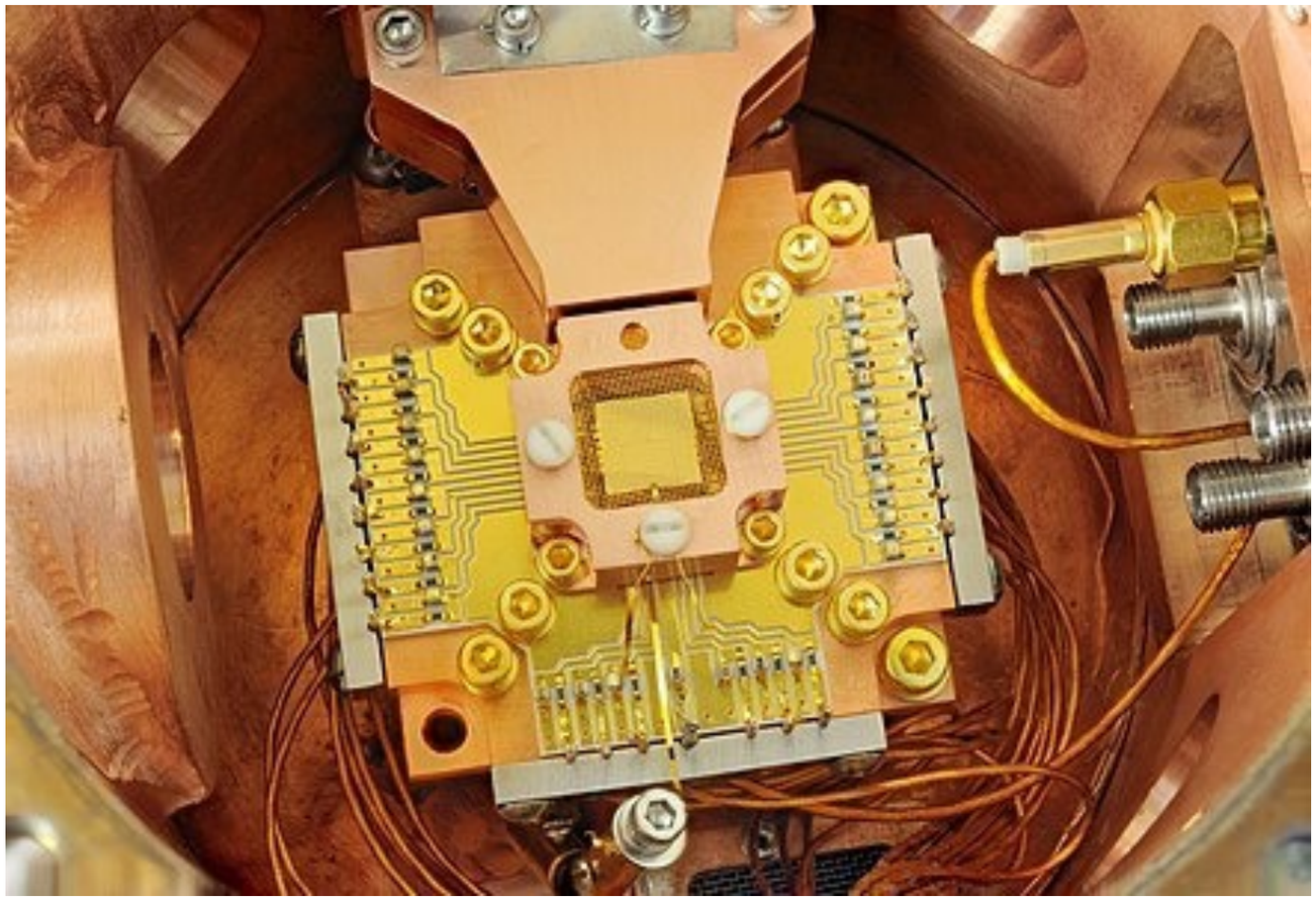
Dal bit al quantum bit



Indirizzo di computazione e informazione quantistica

Laurea interateneo in Fisica dei sistemi complessi

Dagli anni 1950 in poi, la velocità dei calcolatori raddoppia e le dimensioni dei loro componenti si dimezzano circa ogni due anni.

Le dimensioni medie del sistema fisico impiegato per immagazzinare un' unità di informazione sono passate:

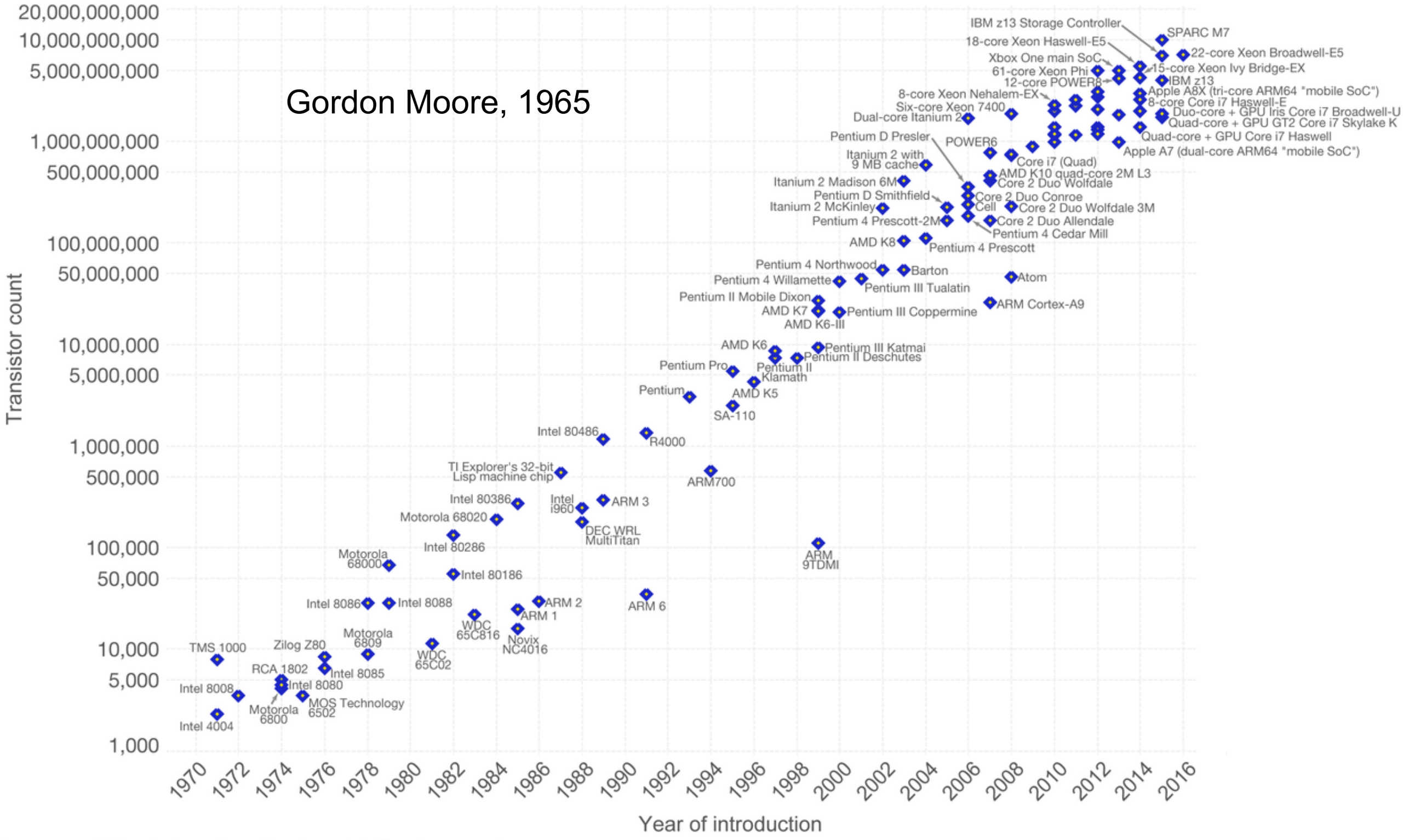
dai centimetri delle valvole usate nei primi calcolatori
ai micrometri (10^{-6} metri) dei moderni componenti circuitali.

Moore's Law – The number of transistors on integrated circuit chips (1971-2016)

Our World in Data

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important as other aspects of technological progress – such as processing speed or the price of electronic products – are strongly linked to Moore's law.

Gordon Moore, 1965



Data source: Wikipedia (https://en.wikipedia.org/wiki/Transistor_count)

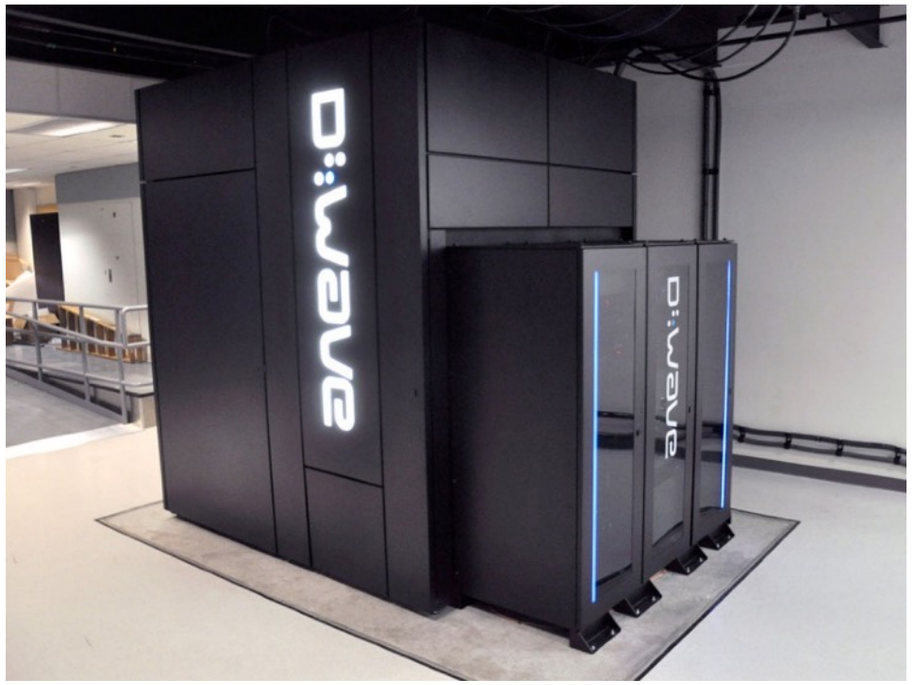
The data visualization is available at OurWorldinData.org. There you find more visualizations and research on this topic.

Ci si aspetta che questa progressione termini intorno al 2020, a causa degli *effetti quantistici* che cominciano a farsi sentire su microcomponenti di dimensioni appena superiori a quelle atomiche, cioè dell' ordine del nanometro (10^{-9} metri).

D' altra parte proprio gli *effetti quantistici* possono essere sfruttati per lo sviluppo di algoritmi esponenzialmente più efficienti di quelli realizzabili su calcolatori ordinari.

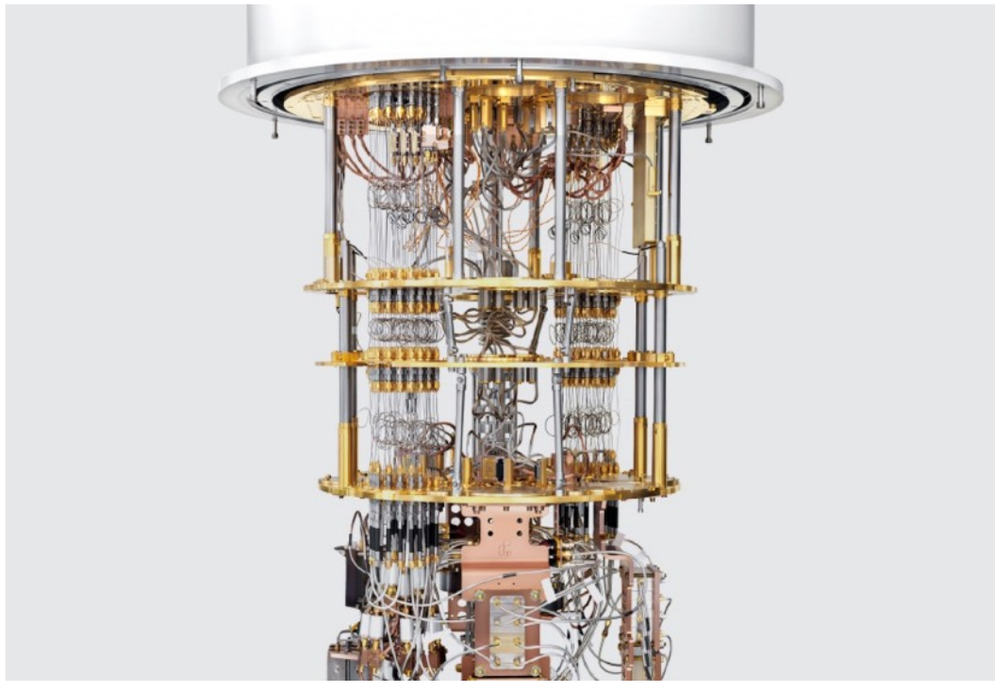
I *calcolatori quantistici* implementano questi algoritmi, controllando e manipolando gli stati quantistici delle microcomponenti.

Attualmente ne esistono solo alcuni prototipi, con un piccolo numero di componenti (**quantum bits**)

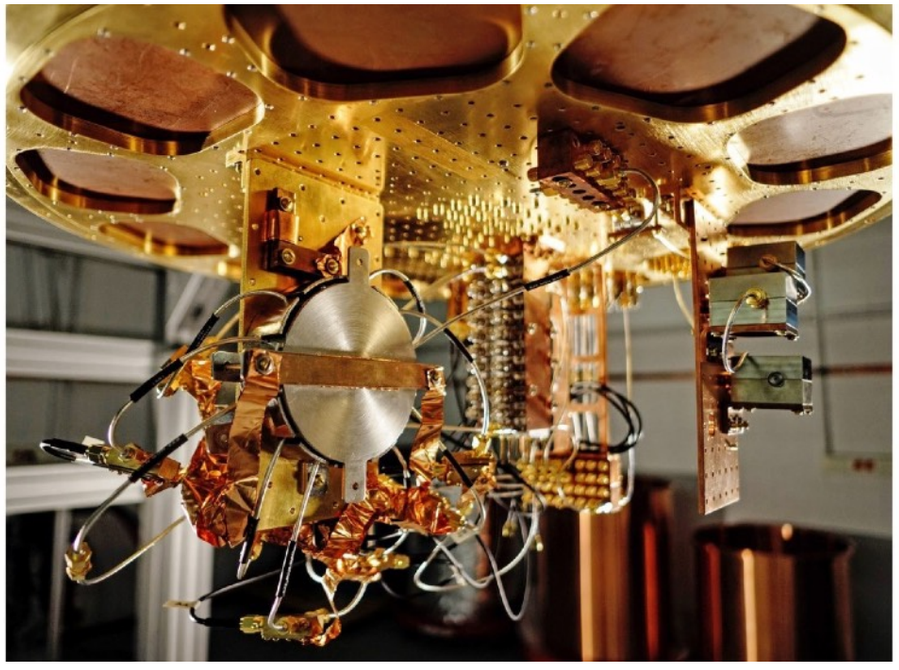


D-WAVE*

microcorrenti in
anelli superconduttori



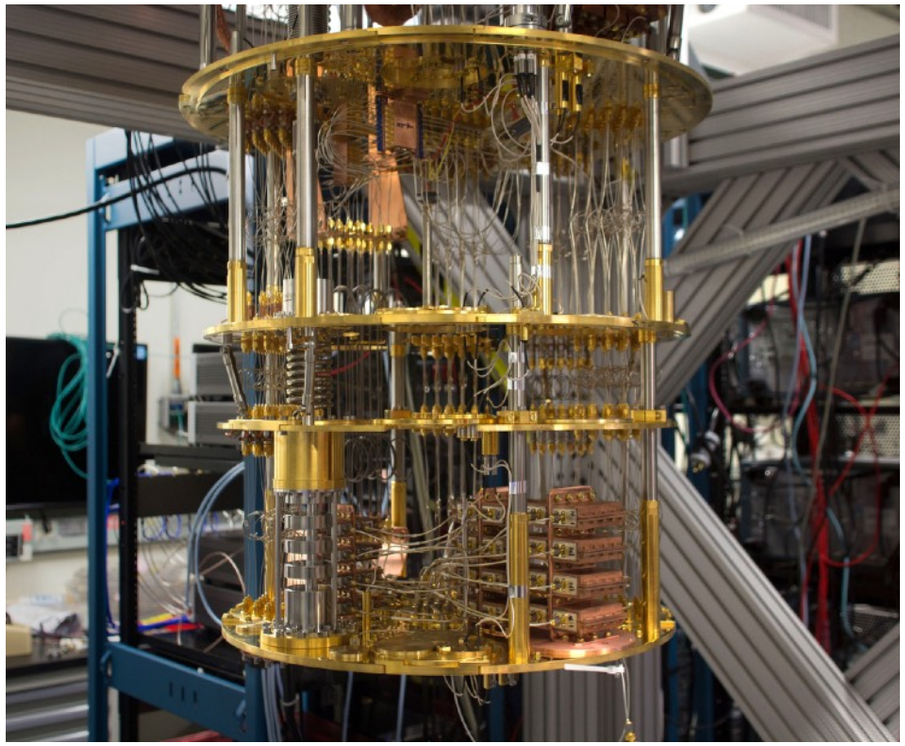
Rigetti



Google

Applicazioni: medicina (diagnostica)
chimica
energia
logistica

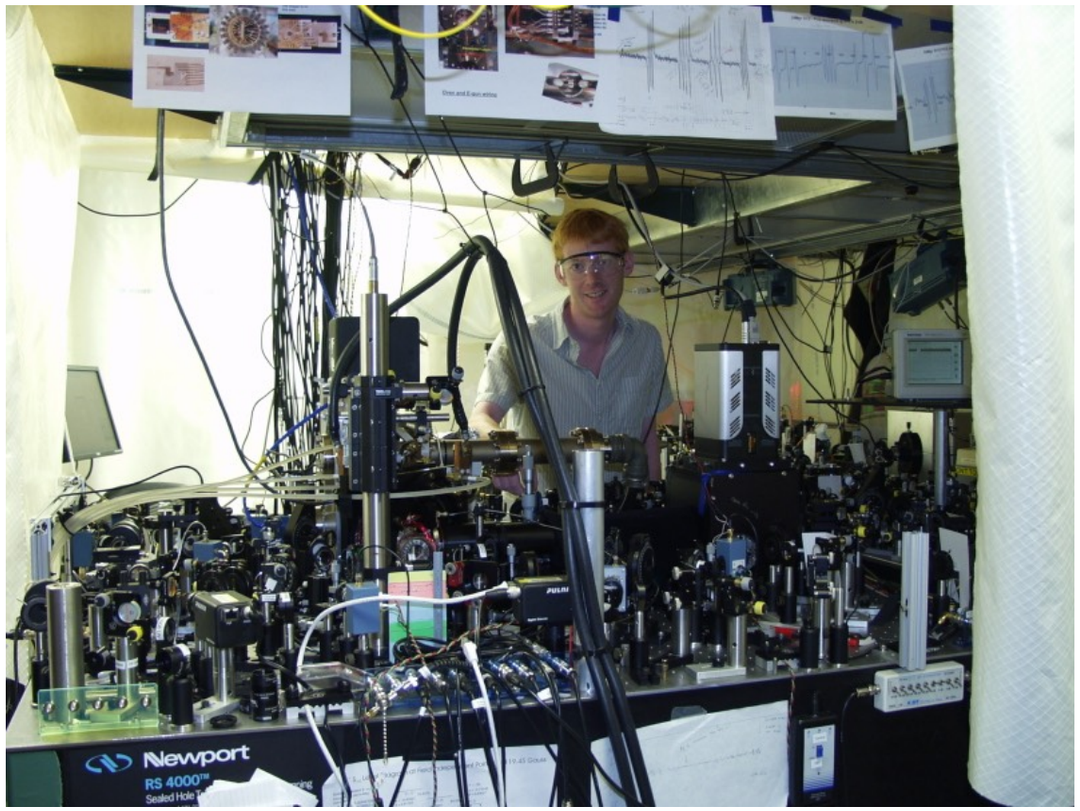
simulazione sistemi complessi



IBM quantum experience*

* Accessibili in rete

ioni intrappolati



atomi di Itterbio
160 qubit fisici
79 qubit logici
gate fidelity 98%

ION-Q

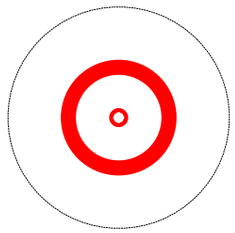
SISTEMA *CLASSICO* A DUE STATI
= BIT

Esempio: un interruttore
può trovarsi in uno di *2 possibili stati*

SISTEMA *MICROSCOPICO* A DUE STATI DI BASE:
QUANTUM BIT (QUBIT)

Esempio: un atomo. Può trovarsi negli stati

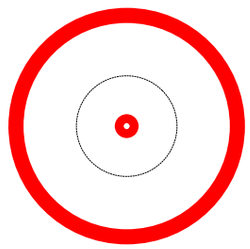
$|0\rangle$ =



elettrone nell' orbita bassa:
STATO FONDAMENTALE

oppure

$|1\rangle$ =



elettrone nell' orbita alta:
STATO ECCITATO

STATI SOVRAPPOSTI

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Potendo assumere tutti gli stati $|\psi\rangle$, intermedi tra $|0\rangle$ e $|1\rangle$, il *qubit* è molto più ricco di informazione di un registro binario classico (che può solo assumere gli stati 0 e 1).

STATI INTRECCIATI (ENTANGLED)

· NON possono scriversi come PRODOTTO:

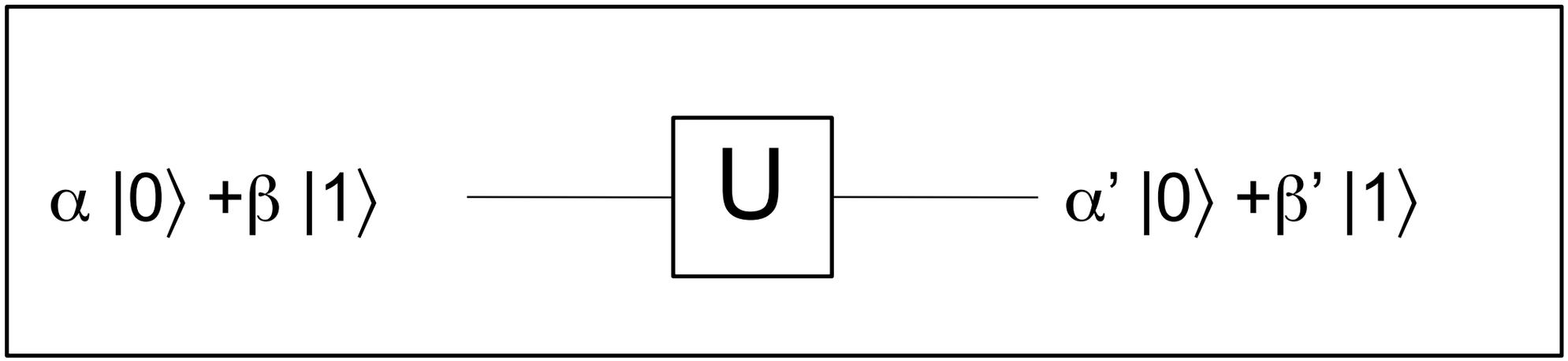
$$|0,0\rangle = |0\rangle\,|0\rangle$$ STATO SEPARABILE

· Esempio:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{\sqrt{2}}|1,1\rangle$$ STATO INTRECCIATO

→ Correlazioni tra le misure di Alice e Bob !

PORTE QUANTISTICHE a 1 QUBIT

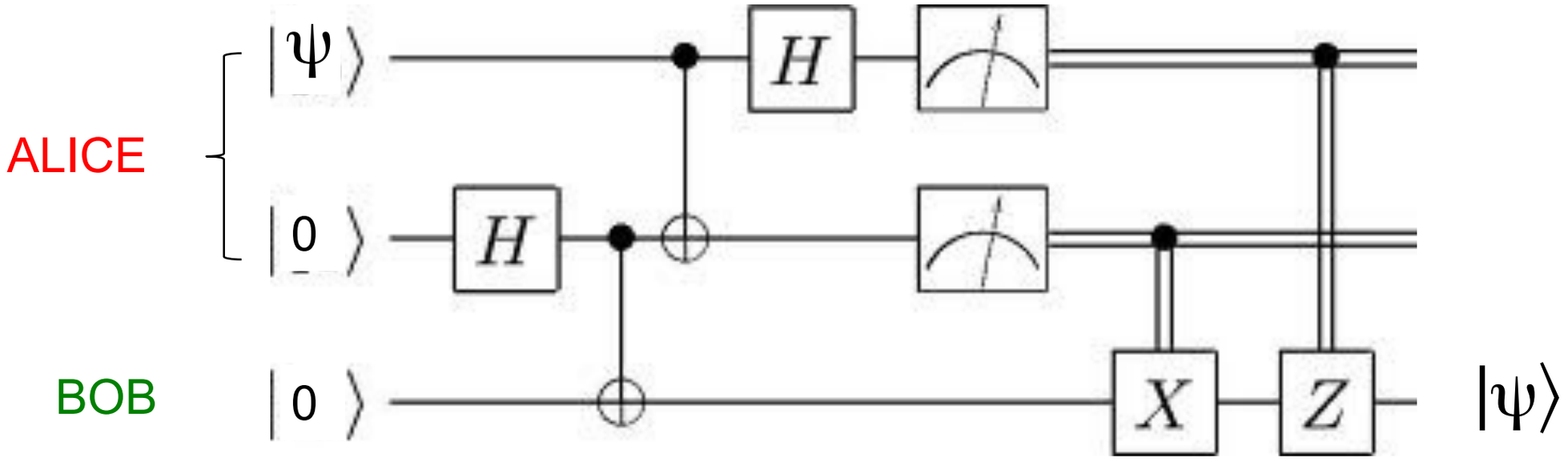


con $|\alpha|^2 + |\beta|^2 = |\alpha'|^2 + |\beta'|^2 = 1$

U è un elemento di U(2)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

TELETRASPORTO (DI STATO QUANTISTICO)



· La misura di Alice DISTRUGGE lo stato $|\psi\rangle$, riducendolo allo stato $|0\rangle$ oppure allo stato $|1\rangle$

· $|\psi\rangle$ può essere anche SCONOSCIUTO ad Alice

· Il teletrasporto non può essere ISTANTANEO : la telefonata di Alice a Bob trasferisce informazione a velocità uguale od inferiore a quella della luce.

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

Abstract

A digital computer is generally believed to be an efficient universal computing device; that is, it is believed able to simulate any physical computing device with an increase in computation time by at most a polynomial factor. This may not be true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

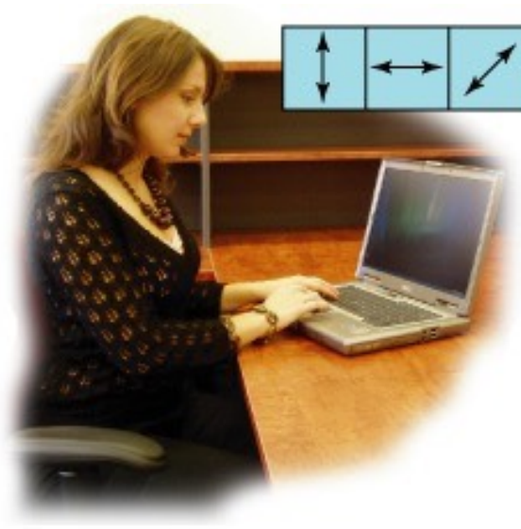
Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

*A preliminary version of this paper appeared in the Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, Nov. 20–22, 1994, IEEE Computer Society Press, pp. 124–134.

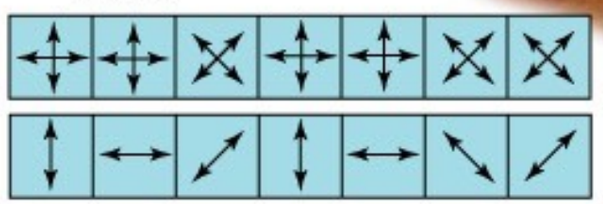
†AT&T Research, Room 2D-149, 600 Mountain Ave., Murray Hill, NJ 07974.

CRITTOGRAFIA QUANTISTICA: PROTOCOLLO BB84



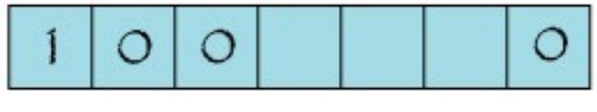
Alice sends photons using
A secret basis

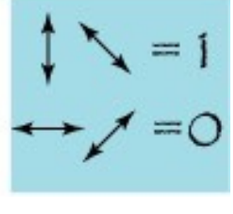
Bob uses a random detector orientation to measure the photons. He only gets some correct.



Alice indicates to Bob what measurements will be correct. These become the new key.

Bob phones Alice and tells her over a public channel what basis he used.





EN

INRiM
ISTITUTO NAZIONALE
DI RICERCA METROLOGICA

TECNOLOGIE QUANTISTICHE

I laboratori di Tecnologie quantistiche, nell'ambito dell'attività sull'Ottica Quantistica dell'INRIM, hanno come obiettivo lo studio degli stati di luce quantistici sia dal punto di vista dell'indagine sui fondamenti della meccanica quantistica, sia relativamente allo sviluppo di tecniche innovative, volte al superamento dei limiti classici di misura, e lo sviluppo di metodi accurati di caratterizzazione metrologica di sorgenti e detector utilizzati nelle emergenti tecnologie quantistiche.

Essi sono dotati di strumentazione allo stato dell'arte per quanto riguarda le tecnologie ottiche, optoelettroniche e quantistiche (Laser, rivelatori di singolo fotone, etc.). Tale linea di ricerca nata a partire

NTT DATA

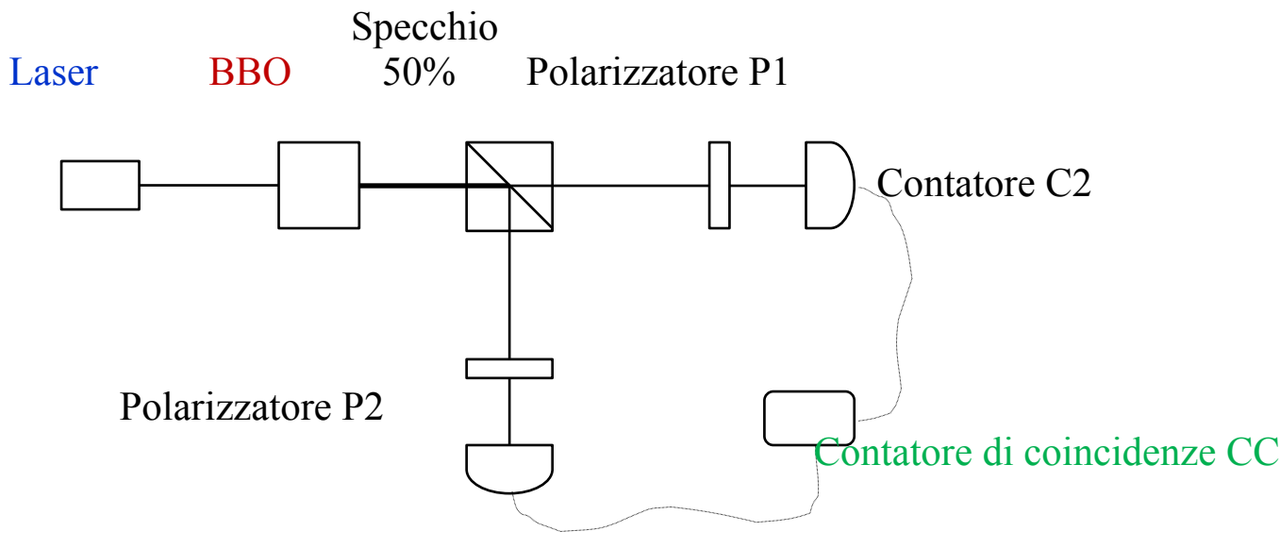
(/global/en)

ABOUT US

Company Profile

NTT DATA is your Innovation Partner anywhere around the world.
Headquartered in Tokyo, with business operations in more than 50 countries and regions, we emphasize long-term commitment and combine global reach and local intimacy to provide premier professional services from consulting, system development to business IT outsourcing.
Since 1967, NTT DATA has played an instrumental role in establishing and advancing IT infrastructure. Originally part of Nippon Telegraph and Telephone Public Corporation, its heritage contributed to social benefits with a quality-first mindset. A public company since 1995, the company builds on this proven track record of innovation by providing novel IT solutions to bring results in a greater quality of life for people, communities, and societies around the world.

PRODUZIONE DI STATI INTRECCIATI A DUE FOTONI IN UN LAB DIDATTICO



Laser a 406 nanometri

BBO: cristallo di beta-borato di Bario. Con prob $\sim 10^{-9}$ il fotone incidente si converte in due fotoni a 812 nanometri (parametric down conversion, PDC) con polarizzazioni perpendicolari tra loro

Il contatore di coincidenze seleziona i fotoni intrecciati (prodotti nello stesso istante nel cristallo)

Lo stato dei fotoni che attivano il contatore di coincidenze è intrecciato

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0,1\rangle + |1,0\rangle\right)$$