Il computer che batte il computer

La fisica quantistica riuscirà a cambiare tutto Velocità di calcolo enorme, sicurezza a rischio

di STEFANO GATTEI

Il Novecento si apre con una profonda crisi della fisica, segnata dalla nascita di due grandi teorie: la relatività generale, che sostituisce la teoria della gravitazione universale di Newton; e la meccanica quantistica, basata sull'idea che l'energia sia trasmessa in modo non continuo, ma per pacchetti discreti (i quanti).

Entrambe le teorie hanno conseguenze spesso inaspettate e controintuitive: in base alla meccanica quantistica, per esempio, sia la radiazione sia la materia hanno caratteristiche tanto ondulatorie quanto particellari, al contrario della meccanica classica, in base alla quale la luce è trattata come un'onda e l'elettrone come una particella. Entrambe, tuttavia, hanno avuto importanti riscontri sperimentali, rivoluzionando l'impianto teorico della fisica e la nostra vita di tutti i giorni (basti pensare alla risonanza magnetica o ai telefoni cellulari).

Nei primi anni Ottanta Richard Feynman osservò che non sarebbe stato possibile simulare alcuni fenomeni governati dalla meccanica quantistica per mezzo di un computer classico. D'altra parte, i continui progressi della tecnologia portavano a una crescente miniaturizzazione dei circuiti, e in un tempo relativamente breve ogni componente si sarebbe ridotto alle dimensioni di pochi atomi. Su scala atomica, i fenomeni sono governati da leggi che non seguono la fisica classica, ma quella quantistica; Feynman suggerì allora di sostituire la «macchina di Turing», proposta nel 1936, con la sua versione quantistica che, a differenza della precedente, era in grado di simulare i fenomeni previsti dalla fisica dei quanti senza subire un calo esponenziale di velocità.

Ne discutiamo con Yuri Manin, che propose per primo l'idea, nel 1980, anche se il suo lavoro divenne noto solo successivamente a quello di Feynman, in quanto apparso originariamente in russo. Tra i maggiori matematici viventi, Manin divide oggi la propria attività tra la Germania, dove è professore al Max Planck Institut für Mathematik di Bonn, e la Russia, dove insegna al celebre Istituto Steklov di Mosca. Lo contattiamo in una pausa di lavoro e gli chiediamo come sia giunto all'idea di un computer quantistico.

«Negli anni Settanta tenevo un corso di logica matematica a Mosca, e al medesimo tempo avevo intrapreso alcune ricerche di fisica matematica: volevo trovare un ponte fra le due discipline, solitamente considerate disgiunte. Nel 1977 le mie lezioni confluirono in un libro, edito da Springer, in cui un intero capitolo era dedicato alla logica quantistica. L'edizione russa del testo apparve in due volumi, nel 1979 e nel 1980. Nell'introduzione che scrissi per il secondo proposi l'idea di un computer quantistico. Fui stimolato da due ordini di problemi: comprendere la fisica alla base della replicazione del Dna e calcolare in modo efficiente le caratteristiche fisiche di un sistema quantistico».

Quali sono le differenze tra la sua proposta e quella avanzata da Feynman nel celebre articolo «Simulating Physics with Computers» del 1982?

«Credo che la motivazione principale di Feynman fosse identica alla mia. Entrambi avevamo compreso che le potenzialità dei computer classici non potevano essere sufficienti, realisticamente, per dare conto anche dei calcoli più semplici di meccanica quantistica. Potremmo dire che, ogniqualvolta osserviamo un sistema quantistico, come per esempio nel caso della misura dello spettro di emissione dell'atomo di idrogeno, utilizziamo tale atomo come un computer quantistico per risolvere un problema matematico concreto. Certo, dal punto di vista storico, il cammino è stato inverso: è stata l'osservazione dei sistemi fisici a contribuire alla realizzazione dell'apparato matematico della meccanica quantistica».

Sfruttando alcune peculiarità della nuova fisica, non disponibili in un quadro classico, si arriverebbe a una crescita esponenziale della velocità di computazione, con ovvi vantaggi per la trattazione di problemi complessi. La realizzazione di un computer quantistico universale, sul modello della macchina di Turing, è però molto lontana.

«Non disponiamo ancora di una corretta comprensione teorica di quella che potrebbe essere la versione quantistica della macchina di Turing. Il punto è che negli anni Trenta e Quaranta, quando fu creata la moderna teoria della computabilità, vennero proposte varie definizioni degli algoritmi di computazione, alquanto diverse fra loro. Molto presto ne venne dimostrata l'equivalenza, e si arrivò alla cosiddetta "tesi di Church": qualunque schema di computazione immaginabile in futuro sarà equivalente a quelli che già esistono. È un esempio di quella che mi piace chiamare "una scoperta sperimentale nel mondo delle idee". Niente di tutto questo si è ancora verificato per i computer quantistici, ed è improbabile che si verifichi in tempi brevi».

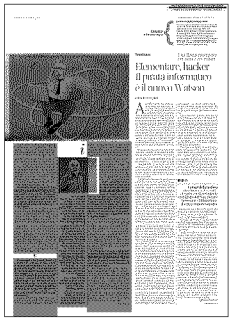
Per i computer tradizionali, basati sui transistor, il costituente di base dell'informazione è il bit, mentre per i computer quantistici è il qubit (o quantum bit). Se un bit può assumere uno solo di due stati differenti (sì o no, vero o falso, zero o uno), un bit quantistico può essere codificato come combinazione di due stati, tipo gli stati di spin 1/2 o i differenti stati elettronici di un atomo. In questo modo i computer quantistici hanno la possibilità di essere in più di uno stato simultaneamente, con vantaggi enormi dal punto di vista della velocità di elaborazione delle informazioni.

«In senso proprio, le computazioni quantistiche sono processi fisici che si sviluppano su uno o più dispositivi. Teoricamente, si trattano anche processori con dimensioni "consistenti", ma i successi ottenuti, in pratica, sono molto pochi. Già alcune dozzine di qubit sono considerate un successo (la D-Wave, nel 2012, aveva per esempio sostenuto di utilizzare 84 qubit). I processori quantistici lavorano sotto l'attenta supervisione di computer classici che svolgono alcuni compiti di base: fornire gli input, misurare gli output, ripetere più volte la medesima operazione. Anche per la memorizzazione dei dati si ricorre alle memorie di computer classici».

Molti codici cifrati attualmente in uso funzionano non perché teoricamente impenetrabili, ma perché violarli comporterebbe tempi estremamente lunghi anche per i computer più potenti. Nel 1994 Peter Shor dimostrò che il problema della fattorizzazione dei numeri primi (classicamente considerato intrattabile, e per questo


Orizzonti

Il computer che batte il computer



Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.

strettamente legato ai sistemi cifrati di sicurezza) si può risolvere in un tempo ragionevole attraverso un algoritmo quantistico. Perché questo non è possibile su un computer classico?

«Uno dei modi per aumentare la velocità con cui si eseguono gli algoritmi classici è quello di ricorrere a calcoli in parallelo. Gli algoritmi quantistici, come quello di fattorizzazione di Shor, sostituiscono ai classici calcoli in parallelo dei calcoli in parallelo quantistici. La cosa è resa possibile dal fenomeno noto come *entanglement* (o "correlazione quantistica"): dal punto di vista matematico, significa che lo stato quantistico di un sistema è, in generale, la combinazione di molti (o addirittura di un numero infinito di) stati classici».

In altre parole: se anche i più potenti computer classici potrebbero impiegare decenni per violare un codice cifrato, i computer quantistici potrebbero farlo nel giro di pochi minuti. La loro introduzione costituirebbe allora una minaccia per la sicurezza elettronica?

«Le minacce sono determinate dagli uomini, non dai prodotti della loro scienza e della loro tecnologia. E dato che gli esseri umani utilizzano invariabilmente le migliori creazioni della loro mente collettiva per l'autodistruzione, non posso essere molto ottimista nemmeno per quanto riguarda i computer quantistici. Isaiah Berlin intitolò una raccolta dei propri scritti *Il legno storto dell'umanità*, con riferimento a Kant. Berlin voleva dire che tutti i progetti sociali di ampio respiro sono destinati a fallire: non è possibile costruire un edificio su un legno storto. Ma continuiamo a sperare».

© RIPRODUZIONE RISERVATA

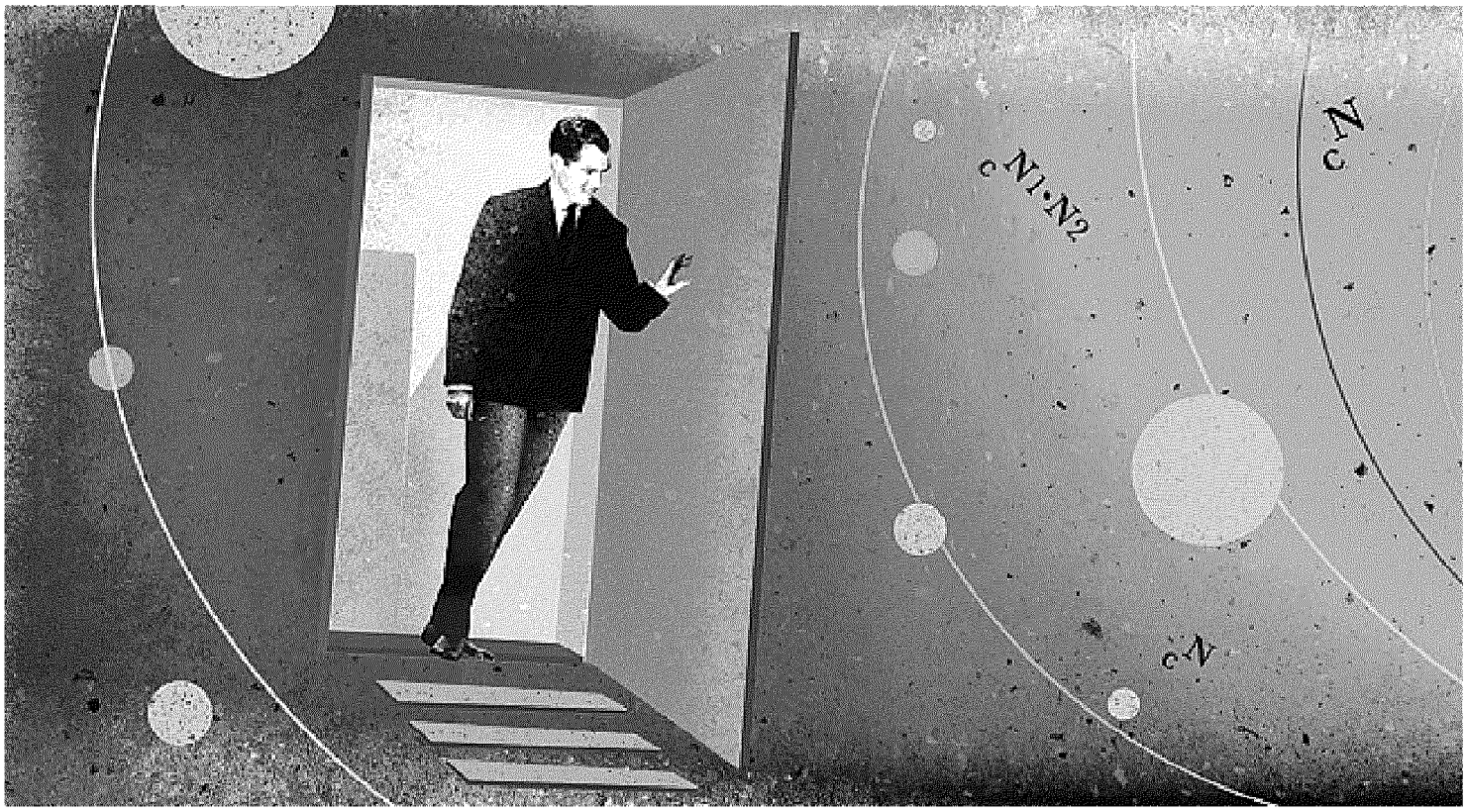
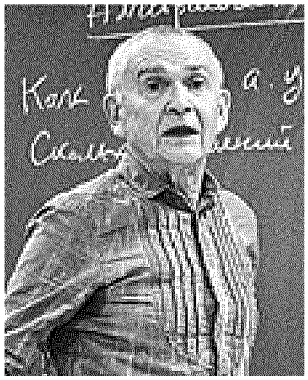
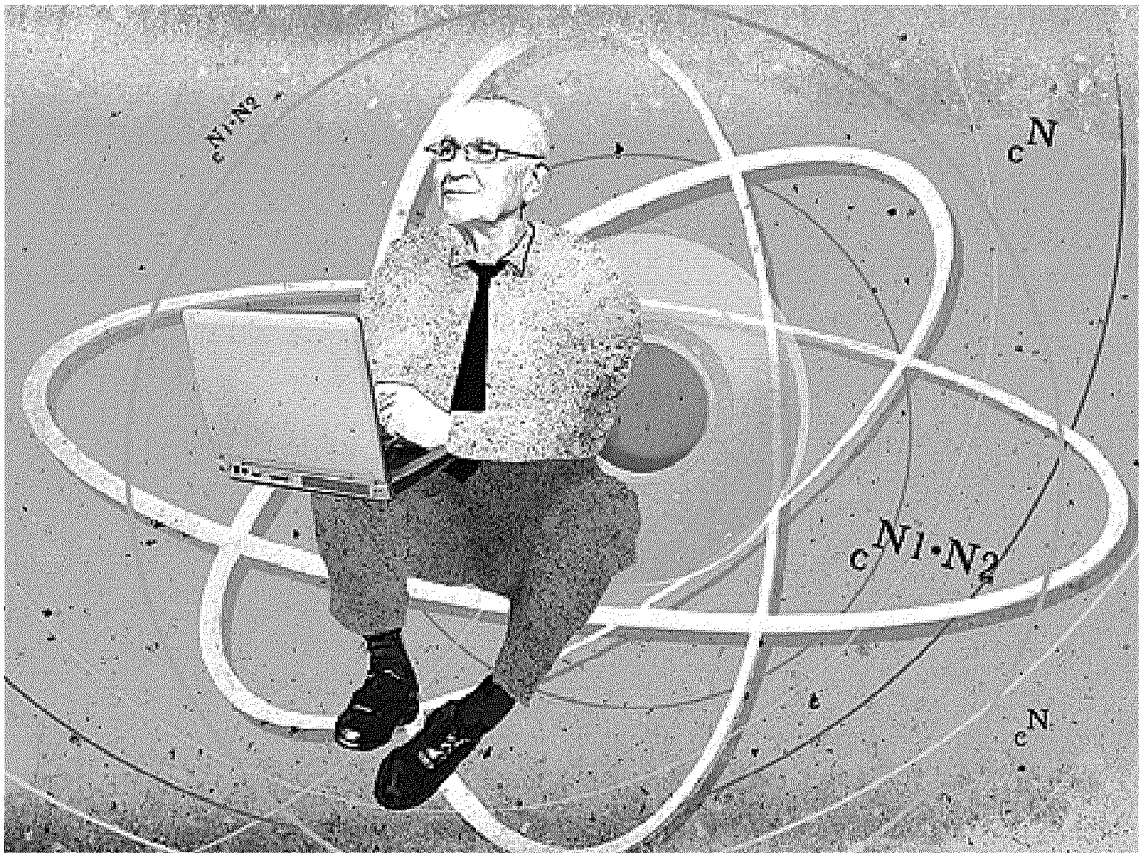


ILLUSTRAZIONE
DI FRANCESCA CAPELLINI

L'intervista Colloquio con Yuri Manin, uno dei maggiori matematici viventi, docente a Bonn e a Mosca, che per primo propose di sostituire la «macchina di Turing». Ma violare i codici cifrati (operazione che oggi richiede anni) diventerebbe un gioco da ragazzi

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.





Il personaggio
Nato nel 1937 a Sinferopoli, in Crimea, lo scienziato russo Yuri Manin (nella foto qui sopra, courtesy Denis Mironov/Simons Foudation) è uno dei matematici più noti a livello internazionale. Docente al Max Planck Institut für Mathematik di Bonn e all'Istituto Steklov di Mosca (dove ha ottenuto il suo dottorato nel 1960), ha insegnato anche in Usa, alla Northwestern University

Un'ipotesi rivoluzionaria
Nella introduzione a un suo libro uscito nel 1980, Manin avanzò per primo l'ipotesi di utilizzare i fenomeni tipici della meccanica quantistica per l'elaborazione delle informazioni. Due anni dopo, del tutto autonomamente, una proposta analoga venne avanzata dallo scienziato americano Richard Feynman (1918-1988), premio Nobel per la fisica nel 1965, in un articolo apparso nel 1982 sulla rivista «International Journal of Theoretical Physics»

La macchina di Turing
Introdotta negli anni Trenta dal matematico inglese Alan Turing (1912-1954), l'omonima macchina manipola i dati contenuti su un nastro di lunghezza infinita. Ha fornito un modello astratto di calcolo automatico, essenziale per lo sviluppo dell'informatica

Ritaglio stampa ad uso esclusivo del destinatario, non riproducibile.