Quanti in pratica

Attualità e prospettive delle tecnologie quantistiche

di Saverio Pascazio

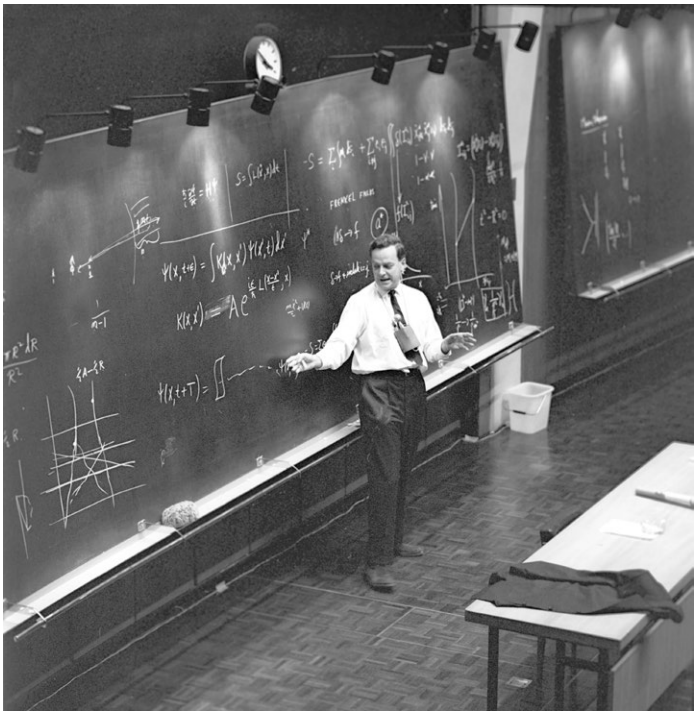
Quando Schrödinger coniò il termine entanglement, come traduzione della parola tedesca *Verschränkung*, non avrebbe mai immaginato che, dopo quasi un secolo, il principio di sovrapposizione e l'entanglement sarebbero diventati i cardini di buona parte di quelle che oggi vengono chiamate tecnologie quantistiche. Naturalmente, sovrapposizioni ed entanglement, per poter essere utilizzati a fini pratici (alle scale temporali che caratterizzano il nostro quotidiano), devono essere robusti, cioè devono durare sufficientemente a lungo. Questo richiede e rende necessaria una certa resilienza nei confronti delle perturbazioni esterne, che di solito sono incontrollabili e tendono a cancellare gli effetti quantistici (un fenomeno noto come "decoerenza").

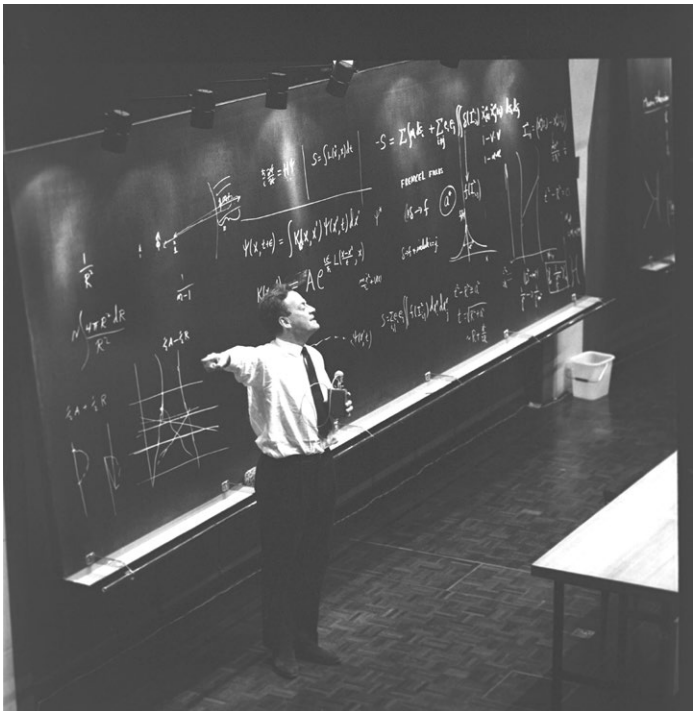
Le tecnologie quantistiche sono un campo emergente della fisica. Ma cosa consentono di fare? Come funzionano e perché? Cerchiamo di rispondere a queste domande. Il calcolo quantistico, le simulazioni quantistiche, i sensori, la crittografia e l'*imaging* quantistici sono tutti esempi di tecnologie quantistiche. Prima di descrivere brevemente queste applicazioni, è utile sottolineare alcune distinzioni. Molti dispositivi che utilizziamo nel quotidiano fanno pieno uso di effetti tipicamente quantistici. Fra questi i laser, i transistor e in generale i dispositivi basati sulle proprietà quantistiche dei semiconduttori, il cui utilizzo ha modificato profondamente la nostra vita (si pensi a telefonini e computer). Questi dispositivi vengono chiamati tecnologie "quantum 1.0" per differenziarli dalle tecnologie "quantum 2.0", che utilizzano sovrapposizioni ed entanglement, facendo uso di sistemi spesso ingegnerizzati, composti da un elevato numero di componenti quantistici elementari.

Il "calcolo quantistico" funziona utilizzando il cosiddetto "parallelismo quantistico", cioè eseguendo più calcoli allo stesso tempo.

Soltanto una misura quantistica opportunamente ingegnerizzata seleziona alla fine dell'intero processo il risultato del calcolo di nostro interesse. Questo consente di eseguire computazioni in modo esponenzialmente più rapido di un computer classico. Non esiste ancora un computer quantistico perfettamente funzionante, e il nemico da battere è la decoerenza: il parallelismo funziona, se i passaggi intermedi sono eseguiti in modo fra loro coerente, altrimenti il computer diventa classico. Uno degli algoritmi quantistici più famosi è quello di Shor, che consente di fattorizzare un numero in

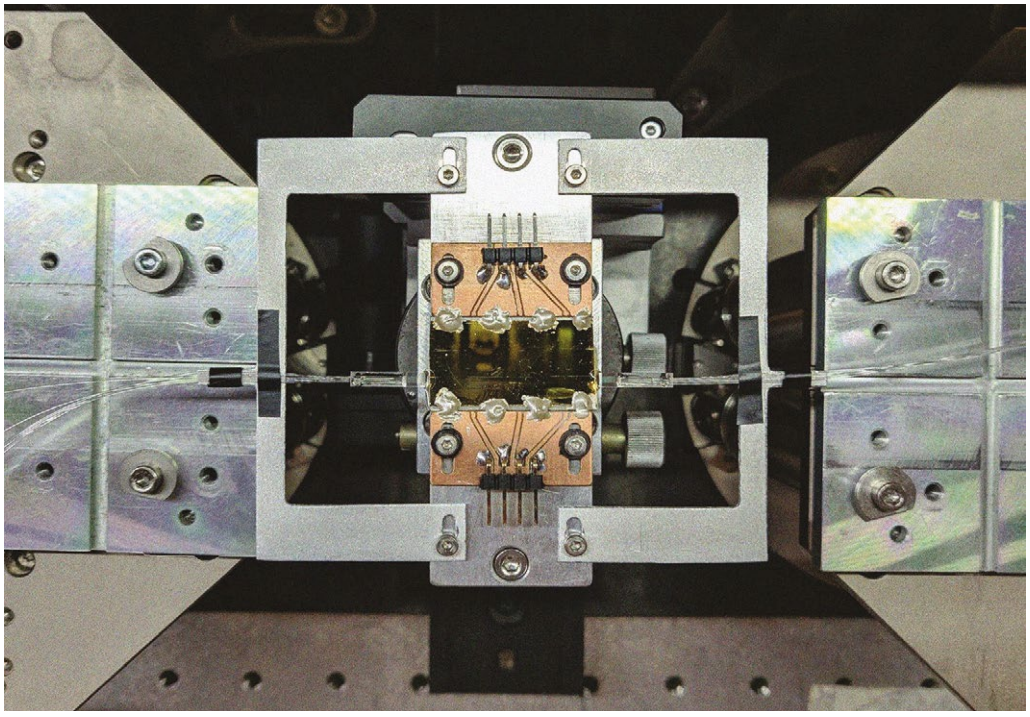
a.
Il nemico da battere nelle tecnologie quantistiche è la decoerenza. "HYBRID 2019 MAR 28", acrilico su tela e multistrato di betulla, opera di Eugenio Lopopolo (https://www.eugeniolopopolo.it).





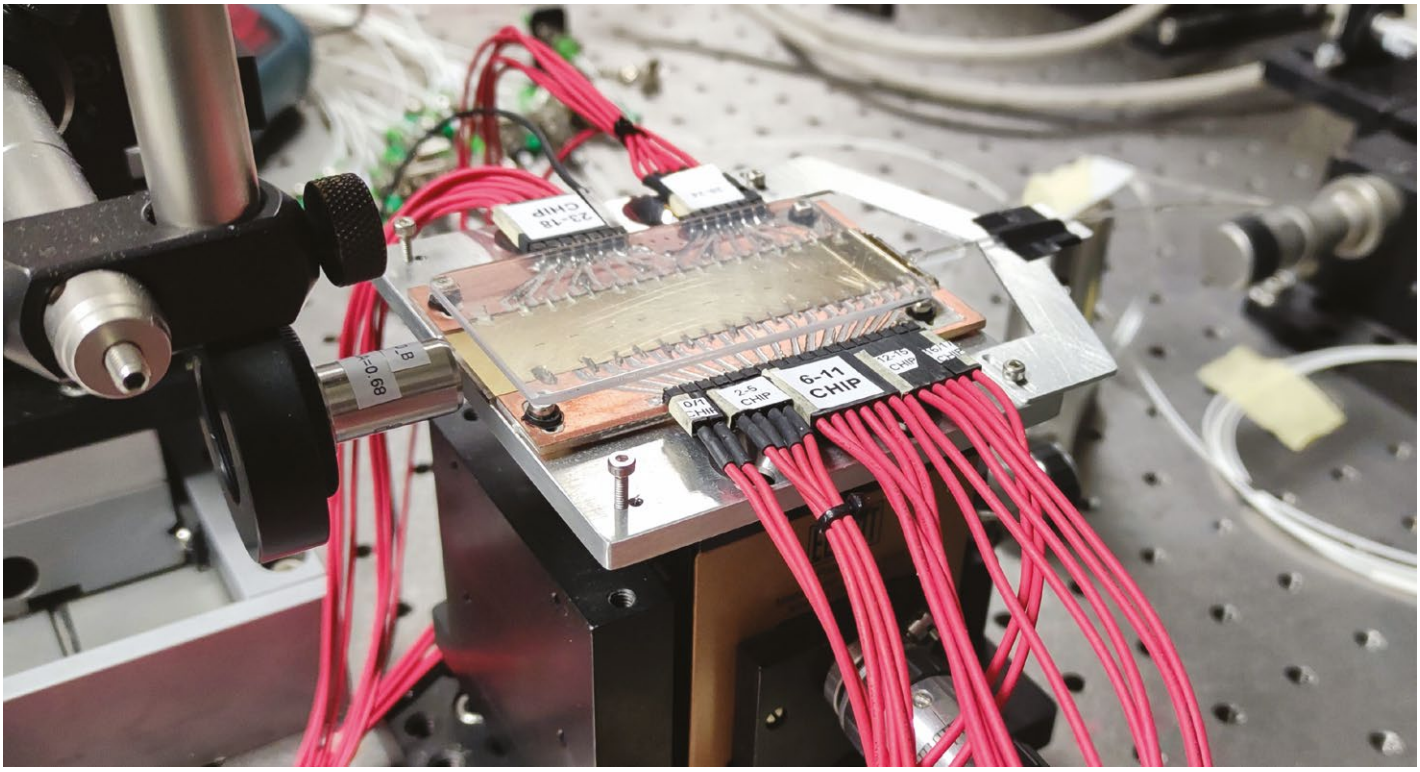
b./c.
Richard Feynman fu il primo a capire che un computer quantistico può simulare i fenomeni naturali meglio di un computer classico.

maniera esponenzialmente più rapida di qualsiasi algoritmo classico.
Le "simulazioni quantistiche" sono un buon compromesso. Fanno uso di computer quantistici dedicati, in grado di risolvere pochi problemi ben selezionati. Esistono già dei buoni simulatori quantistici, che fanno uso di sistemi atomici o ionici raffreddati: risolvono problemi che stanno molto a cuore ai fisici, quali alcune teorie quantistiche su reticolo, e problemi di sistemi a molti corpi, difficilissimi da trattare. L'idea di un simulatore quantistico risale a Feynman, che ne propose uno schema nel 1982.
I "sensori quantistici" sono in grado di fare misure estremamente precise utilizzando entanglement, interferenza e particolari stati quantistici. Le applicazioni sono svariate e molto diverse fra loro: si va dalla fotonica all'ottica quantistica, alle misure di campi elettrici e magnetici, alla gravimetria. L'esperimento LIGO, che ha rivelato le prime onde gravitazionali, utilizzava luce "*squeezed*" per misurare segnali di bassissima intensità, al di sotto del cosiddetto *standard quantum limit*.
La "crittografia quantistica" consente di comunicare in modo ultrasicuro (in gergo si dice "intrinsecamente sicuro") utilizzando l'entanglement. L'idea di base consiste nel distribuire una chiave crittografica quantistica che non può essere "copiata" grazie a una proprietà nota come "*no cloning theorem*". Si può fare un clone della pecora Dolly, ma non di uno stato atomico. Chi non è (fisicamente) in possesso della chiave non può decifrare i messaggi.
Le prime comunicazioni quantistiche ultrasicure sono già state effettuate, molte di esse in Europa e in Italia. Una bella applicazione è il "generatore quantistico di numeri casuali": i numeri generati superano tutti i test di aleatorietà che affliggono invece qualsiasi algoritmo non quantistico.
L'*imaging* quantistico sfrutta l'entanglement per ottenere superrisoluzione, cioè risolvendo sorgenti luminose al di sotto di tutti i limiti classici. Si riesce quindi a superare anche il famoso limite di Rayleigh, che è alla base dell'ottica tradizionale. Un esempio notevole è il cosiddetto "*ghost imaging*", con il quale si riesce a migliorare l'immagine di un oggetto incrociando l'informazione di due diversi rivelatori di luce.
La domanda spontanea a questo punto è: che cosa si può fare con le tecnologie quantistiche e in quali tempi? Rispondere a questa domanda, evitando facili ottimismi e slogan, non è semplice, soprattutto se si cerca di fare qualche previsione realistica.
Sensori, crittografia e *imaging* quantistici sono tutti esempi di tecnologie quantistiche il cui funzionamento è già stato provato, al di là di qualsiasi ragionevole dubbio. La domanda giusta qui è pertanto: quando potremo disporre di



d.
Interferometro in guida d'onda, realizzato tramite microfabbricazione laser a femtosecondi e utilizzabile per misure su stati di singoli fotoni. I fotoni sono iniettati all'ingresso del circuito e raccolti in uscita da collegamenti in fibra ottica.

queste tecnologie comprando i dispositivi che ci servono? L'indice che si utilizza è il TRL (Technology Readiness Level). Alcune tecnologie hanno già raggiunto TRL molto elevati, che vanno da 4 a 7. La commercializzazione è convenzionalmente fissata al valore 9.
Alcuni simulatori quantistici sono già funzionanti: qui il criterio giusto da considerare è il cosiddetto "vantaggio quantistico". Con questo termine si intende la dimostrazione sperimentale che un simulatore quantistico riesce a svolgere un compito che non è alla portata di nessun dispositivo classico esistente. La corsa verso il vantaggio quantistico è aperta, e sono in molti a competere, sia organi di ricerca che enti privati. Non esiste ancora un buon computer quantistico. Quelli disponibili sono in grado di fare calcoli che possono essere svolti anche su un computer classico oppure che realizzano il "vantaggio" con bassa probabilità. Tradotto in parole povere, questo vuol dire che i computer quantistici esistenti, se messi alla prova con problemi realmente difficili, fanno errori e danno il risultato giusto con probabilità molto piccola. Azzardare una previsione sui tempi è molto difficile. Possono volerci 10 anni.
Le tecnologie quantum 2.0 invece sono già disponibili o in certi casi dietro l'angolo. Fanno buon uso della sovrapposizione quantistica, dell'entanglement e di sistemi ingegnerizzati composti da molte particelle, creando, manipolando e misurando gli stati quantistici della materia e della radiazione. Attraggono enormi finanziamenti pubblici in Europa, negli Stati Uniti, in Canada, in Cina, in Giappone, in India e in Australia. Molte aziende private investono somme ingenti in questo settore, utilizzando ricercatori dedicati, spesso sottratti alle strutture pubbliche.
Le tecnologie quantistiche corrono verso TRL elevati e verso il vantaggio quantistico. Fanno uso di concetti che venivano rifiutati (o al meglio ritenuti "filosofia") fino agli anni '80. Come spesso accade in fisica, sono state le prime conferme sperimentali a spazzare via lo scetticismo e a farci capire che i paradossi erano ancorati al nostro modo di pensare, ai nostri pregiudizi di fisici classici. I paradossi di ieri sono la tecnologia di domani.
Anni fa, durante una conferenza a Napoli, un gruppo di fisici discuteva animatamente sull'interpretazione della meccanica quantistica. Il grande fisico George



Sudarshan, i cui contributi hanno spaziato dalla teoria delle particelle all'ottica quantistica, dai sistemi quantistici dissipativi all'effetto Zenone quantistico, ascoltava in silenzio. A un certo punto disse: "*It is a good thing that quantum mechanics does not depend on its foundations*" ("È una buona cosa che la meccanica quantistica non dipenda dai suoi fondamenti"). Vi è molta verità e anche una buona dose di saggezza in questa affermazione scherzosa. Le generazioni future utilizzeranno le tecnologie quantistiche senza chiedersi che fine abbia fatto il gatto di Schrödinger, un po' come noi usiamo il telefonino senza farci troppe domande sulle leggi quantistiche che governano il trasferimento di carica elettrica nei transistor.

e.
Processore fotonico riconfigurabile. Una complessa rete di microriscaldatori realizzata sulla superficie consente di modificare in modo dinamico la funzionalità del circuito ottico e realizzare così diverse operazioni quantistiche.

Biografia
Saverio Pascazio è un fisico teorico. È professore presso l'Università di Bari e si occupa di fisica quantistica, fenomeni complessi e complessità quantistica.

10.23801/asimmetrie.2022.33.5