

Claudio Bonechi (clavicordo)

QUANTUM

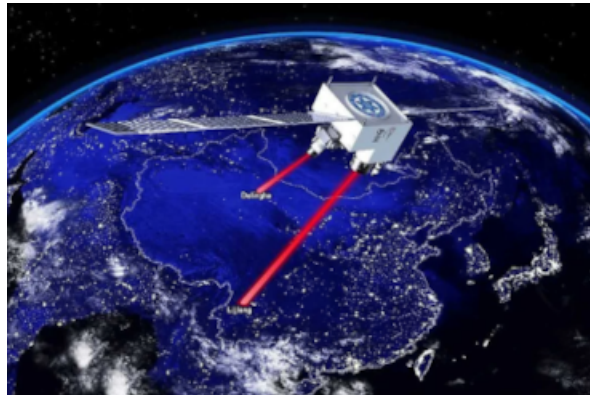
12 June 2021

Premessa

Ho scritto quanto segue utilizzando articoli scritti da *Michael Irving* e pubblicati online, come al solito da me liberamente rielaborati, tratti da pubblicazioni su *Nature Photonics*.

Già da tempo si sente parlare di computer quantistici, mentre le telecomunicazioni basate sui *quantum bit* (termine coniato da Benjamin Schumacher per indicare il bit quantistico ovvero l'unità di informazione quantistica) o *qbit* costituiscono un argomento più recente e di cui non si parla spesso ma che sta acquistando sempre maggiore importanza.

All'alba dell'Internet quantistica globale



Satellite cinese "Micius"

Grazie a Internet, abbiamo una grande quantità di informazioni, ma il rovescio della medaglia è che i dati sensibili sono spesso vulnerabili a intercettazioni e furti. Anche la protezione della crittografia tenderà a essere vanificata dalla crescente potenza di calcolo dei computer.

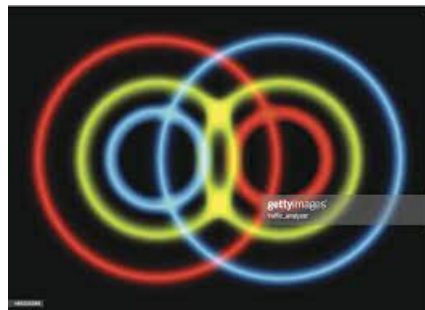
La buona notizia è che la crittografia quantistica può rendere la decodifica non autorizzata letteralmente impossibile e, per una nuova dimostrazione di questo tipo di sicurezza, gli scienziati hanno utilizzato **il satellite cinese Micius** per inviare dati crittografati in modo quantistico tra Cina e Austria.

L'esperimento avvicina ulteriormente il mondo a un'internet quantistica globale.

Micius è stato lanciato nell'agosto 2016, per sperimentare le comunicazioni quantistiche e la relativa crittografia. I satelliti per comunicazioni convenzionali trasmettono informazioni tramite segnali radio a microonde, ma Micius utilizza fotoni con *entanglement* quantistico per "teletrasportare" efficacemente le informazioni.

I due fotoni *entangled* sono indissolubilmente legati, il che significa che se un utente conosce lo stato di una particella può dedurre lo stato dell'altra, non importa quanto siano distanti. L'anno scorso, Micius ha battuto il record di distanza di entanglement quantistico, inviando un messaggio su una distanza di 1.200 km (746 mi).

Entanglement



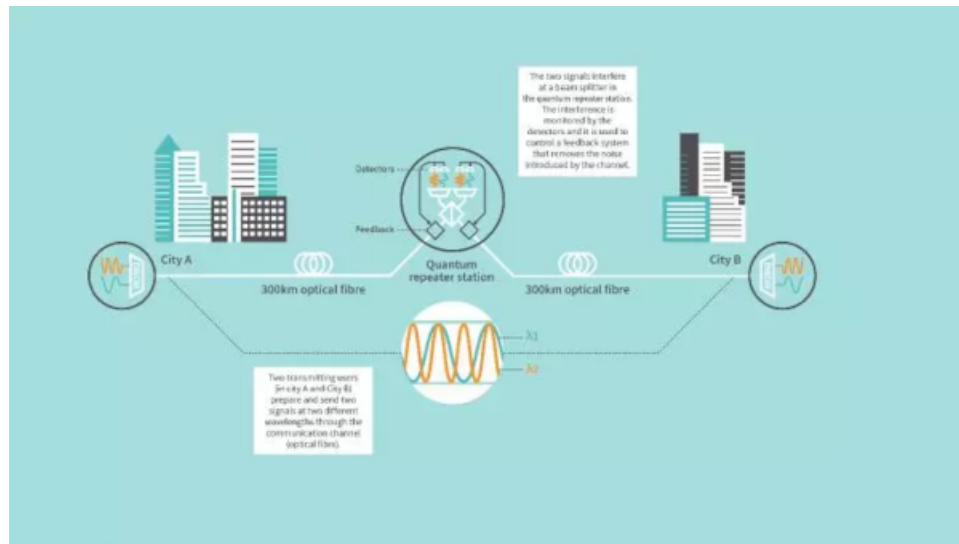
L'*entanglement* quantistico è un fenomeno così bizzarro che persino *Einstein* ha discusso contro la sua esistenza, riferendosi notoriamente ad esso come "azione spettrale a distanza".

Le coppie di particelle *entangled* sono così indissolubilmente legate che lo stato dell'una può essere dedotto dallo stato dell'altra, non importa quanto distanti siano.

In sostanza, questo processo può essere utilizzato per "teletrasportare" istantaneamente informazioni su distanze teoricamente infinite, ciò avrebbe violato la legge della relatività generale per la quale nulla può viaggiare più velocemente della luce. Pare che invece questo non sia più un problema, ma personalmente non so darne una spiegazione.

Per quanto utile possano essere un giorno, gli effetti quantistici sono molto sensibili alle interferenze dall'ambiente.

Esperimenti precedenti hanno racchiuso i fotoni in una fibra ottica per proteggerli, trasmettendo il messaggio lungo la linea da particella a particella.



Questo metodo è stato utilizzato per stabilire il record precedente di 100 km, ma maggiore è la distanza, maggiore è la possibilità che il messaggio venga perso o distorto.

Scienziati cinesi hanno infranto il record della distanza di *entanglement* quantistico. La trasmissione di informazioni attraverso fotoni *entangled* era stata precedentemente possibile solo fino a circa 100 km (62 mi), ma utilizzando il satellite *Micius* lanciato ad agosto 2016, le informazioni sono state effettivamente teletrasportate fino a 1.200 km (746 mi).

Lanciato dal programma *Quantum Experiments at Space Scale (QUESS)*, il satellite *Micius* è stato il primo passo verso la costruzione di una **rete di comunicazione quantistica globale**.

Invece di usare fibre fisiche, il sistema invia fotoni *entangled* tramite raggi laser e, sebbene ciò possa aiutare a ridurre al minimo le interferenze, allineare la sorgente e il ricevitore è una bella sfida, specialmente quando il satellite si muove velocemente.

"Sarà come lanciare una moneta da un aereo a 100.000 metri sopra il livello del mare esattamente nella fessura di un salvadanaio rotante", ha detto *Wang Jianyu*, comandante in capo del progetto *QUESS*, in una dichiarazione lo scorso agosto, quando il satellite è stato lanciato per la prima volta.

Ma il team è riuscito a portare a termine quell'impresa apparentemente impossibile, utilizzando il sistema per trasmettere fotoni in *entanglement* quantistico su una distanza di 1.200 km.

Per fare ciò, il raggio laser sul satellite passa attraverso un "divisore di raggio", che crea due diversi stati polarizzati: uno per ricevere i fotoni *entangled* e uno per inviarli.

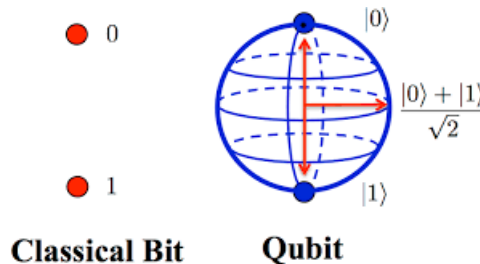
Usando questo metodo, *Micius* comunica con tre diversi satelliti riceventi, su una distanza 12 volte più grande del record precedente e in modo molto più efficiente di quanto siano in grado di fare le fibre ottiche.

"Per il networking quantistico, in questo lavoro, abbiamo già raggiunto un'efficienza di distribuzione dell'*entanglement* a due fotoni un trilione di volte più efficiente rispetto all'utilizzo delle migliori fibre di telecomunicazione", afferma *Jian-Wei Pan*, ricercatore capo del progetto.

Computer quantistici

Nei computer tradizionali, le informazioni sono codificate in bit rappresentati come "zero" e "uno". Ma nei computer quantistici, le informazioni sono codificate in bit quantistici (o *qubit*) che possono essere "zero" o "uno" o entrambi allo stesso tempo.

Da ciò discende che, se come è noto con 3 bit si rappresentano $2^3 = 8$ stati, con 3 *qubit* si rappresentano $2^3 \times 2^3 = 64$ stati.



L'impiego dei *qubit* espande drasticamente la potenza di calcolo e di conseguenza la possibilità di affrontare problemi oltre l'ambito dei normali computer o dei supercomputer.

L'anno scorso, ad esempio, un computer quantistico cinese chiamato *Jiuzhang* ha eseguito in 200 secondi un calcolo che richiederebbe 2,5 miliardi di anni per essere completato da un normale supercomputer.

Ma la sfida che pone il calcolo quantistico è che questi *qubit* sono sensibili alle interferenze dall'ambiente, quali piccole fluttuazioni di temperatura o vibrazioni che minacciano di confondere i dati. Ciò rende difficile la trasmissione di informazioni quantistiche su lunghe distanze.

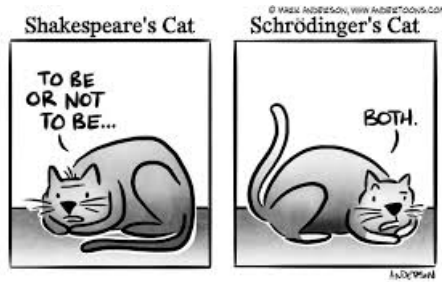
Comunicazione quantistica e sicurezza

Una rete di comunicazione quantistica potrebbe non solo rendere le telecomunicazioni molto più veloci, ma anche più sicure: la sensibilità dei fotoni *entangled* alle interferenze funziona effettivamente a loro vantaggio.

Se una terza parte non autorizzata cerca di attingere a un segnale, lo interrompe, rendendolo illeggibile e avvisando gli utenti ufficiali della presenza dell'hacker.

Oltre ad essere quasi istantanee, le comunicazioni quantistiche sono estremamente sicure.

Funzionano allo stesso modo del famoso esperimento mentale di Schrödinger, che coinvolge un gatto in una sovrapposizione quantistica di essere simultaneamente sia vivo che morto.



È solo quando un osservatore sbircia nella scatola e controlla il gatto che la sovrapposizione crolla in uno stato o nell'altro.

Nella distribuzione delle chiavi quantistiche (QKD), un messaggio viene inviato come singoli fotoni che si trovano in stati di sovrapposizione quantistica: in termini di dati, quei fotoni rappresentano contemporaneamente uno e zero. Il messaggio viene codificato e decodificato tramite dispositivi a ciascuna estremità, che di fatto riducono ogni fotone in arrivo nello stato richiesto, uno o zero.

Se una persona non autorizzata tenta di intercettare il messaggio lungo il percorso, l'atto stesso di osservarlo causerà il collasso della sovrapposizione di ciascun fotone in uno stato casuale, confondendo il messaggio per l'hacker e avvisando della violazione il destinatario ufficiale.

Gli scienziati nel 2018 hanno utilizzato *Micius* per trasmettere dati crittografati con QKD tra Austria e Cina, su una distanza record di 7.600 km (4.722 mi).

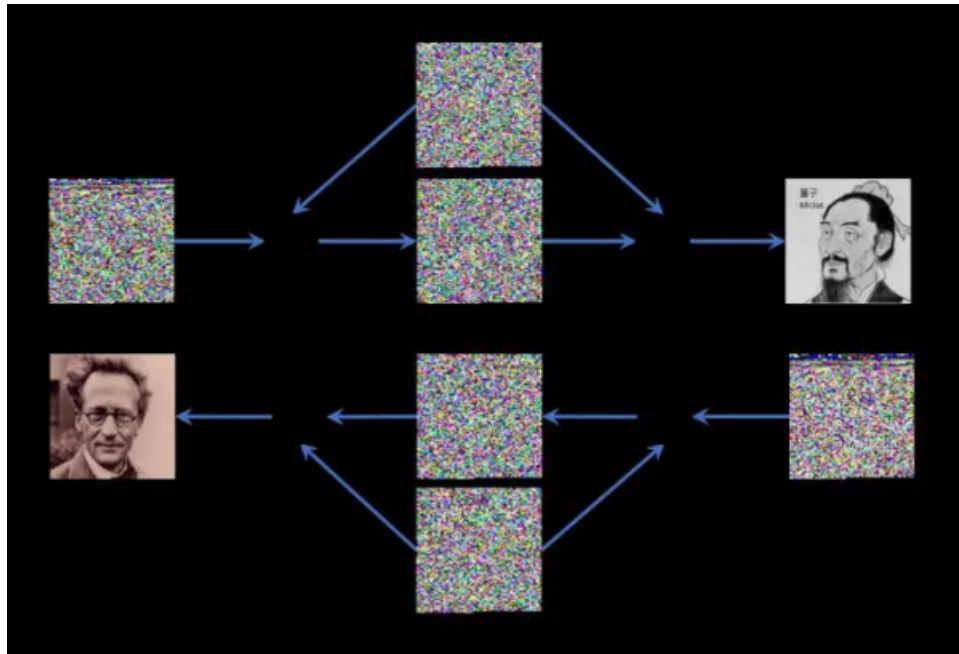


Austria - Cina

Il satellite stabilisce prima una chiave sicura tra se stesso e una stazione di terra, quindi un'altra chiave con un'altra stazione e trasmette le informazioni tra le due.

In questo test, i messaggi erano immagini con dimensioni di file di circa 5 kB, che utilizzavano chiavi quantistiche sicure a 80 kbit per la codifica di un time pad.

Le immagini degli scienziati *Erwin Schrödinger* e *Micius* sono state trasmesse e crittografate attraverso la rete di comunicazione quantistica (Università della Scienza e della Tecnologia della Cina)



Schroedinger e Micius

Un'immagine di *Micius*, lo scienziato cinese del V secolo da cui prende il nome il satellite, è stata inviata da Pechino a Vienna, e la risposta è stata un'immagine di *Erwin Schrödinger*.

Per alzare la posta, gli scienziati hanno quindi condotto una videoconferenza tra le accademie delle scienze cinese e austriaca. Nel corso della chiamata di 75 minuti sono stati trasmessi circa 2 GB di dati, inclusa una chiave quantistica da 560 kbit.

La conferenza è stata anche crittografata utilizzando l'*Advanced Encryption Standard* AES-128, che aggiornava le chiavi *seed* a 128 bit una volta al secondo.

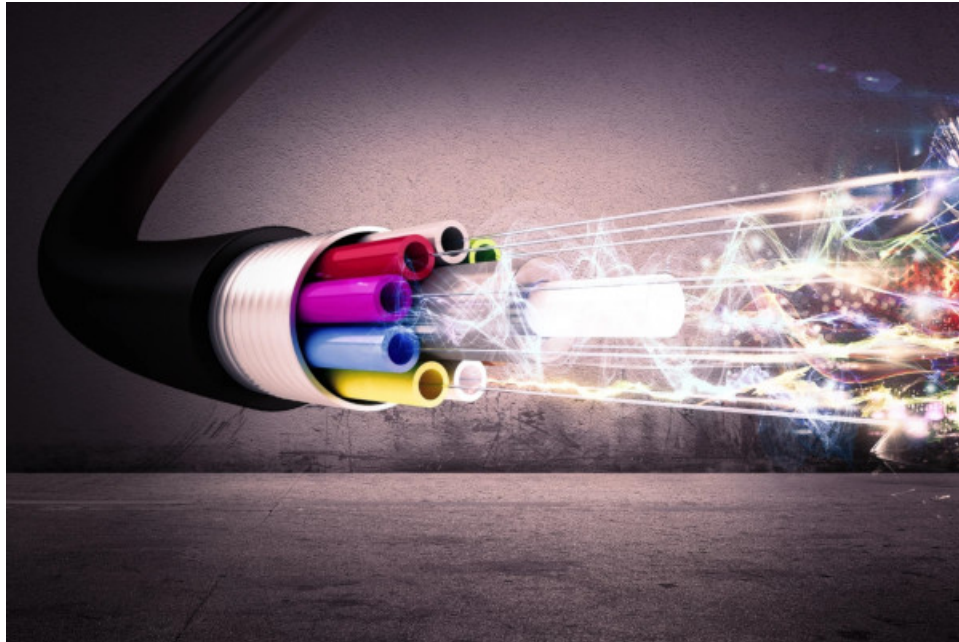
Gli esperimenti sono di buon auspicio per il lancio di reti di comunicazione quantistica su scala globale.

Le reti quantistiche terrestri sono già in uso in alcune aree come la Cina, con fibre in grado di trasmettere dati su una distanza di circa 100 km (62 mi).

Con l'arrivo di satelliti quantistici come *Micius*, un Internet quantistico globale impenetrabilmente sicuro e fulmineo potrebbe essere all'orizzonte.

Un nuovo recente record

Una **Internet quantistica** potrebbe un giorno consentire ai computer quantistici di collaborare e affrontare alcuni problemi giganteschi. Ora il mondo è un passo più vicino a quella realtà, poiché i ricercatori di Toshiba hanno dimostrato possibili le comunicazioni quantistiche inviate su 600 km (373 miglia) di fibra ottica.



Record Toshiba

Ora, quei ricercatori rivendicano il record di distanza per le comunicazioni quantistiche tramite fibra ottica. La svolta che ha consentito di conseguirlo è stata una nuova tecnica di stabilizzazione a doppia banda, che invia due segnali di riferimento ottico insieme ai *qubit* stessi, codificati come ritardo di fase di un debole impulso ottico.

Il primo segnale di riferimento ha una lunghezza d'onda scelta per annullare le fluttuazioni dell'ambiente, mentre il secondo opera sulla stessa lunghezza d'onda dei *qubit* stessi ed è utilizzato per controllare con precisione la fase della luce.

Utilizzando questa tecnica a doppia banda, il team Toshiba è stato in grado di mantenere il segnale quantico costante entro poche decine di nanometri. Ciò a sua volta ha permesso loro di trasmettere i dati su oltre 600 km di fibra ottica, circa sei volte in più rispetto al record precedente.

Tuttavia, non è il più lontano in assoluto: la trasmissione satellitare detiene il record complessivo di oltre 1.200 km (746 miglia), ma un Internet quantistico avrebbe bisogno di un **mix di satelliti e fibre ottiche**.

Il team afferma che il primo utilizzo della tecnologia sarebbe probabilmente per *Quantum Key Distribution (QKD)*. Questa tecnica di crittografia sfrutta la strana regola della fisica quantistica in cui l'atto stesso di osservare la chiave la cambierà, rendendola inutile per un potenziale hacker e avvisando gli utenti autorizzati del tentativo malevolo.

"Negli ultimi anni il QKD è stato utilizzato per proteggere le reti dell'area metropolitana", afferma Andrew Shields, capo della Quantum Technology Division di Toshiba Europe. attraverso paesi e continenti, senza utilizzare nodi intermedi affidabili. Implementato insieme a Satellite QKD, ci consentirà di costruire **una rete globale per comunicazioni protette quantistiche**."

Estratto da "<https://www.electroyou.it/mediawiki/index.php?title=UsersPages:Clavicordo:quantum>"