IstitutoVeneto
diScienzeLettere
edArti

LA COMUNICAZIONE QUANTISTICA PER GLI USI QUOTIDIANI

di Paolo Villoresi*

Le comunicazioni quantistiche sono uno dei settori più interessanti e promettenti delle tecnologie quantistiche. Esse hanno attirato e concentrato molte sperimentazioni e investimenti in tutto il mondo, e hanno progressivamente conquistato ampio spazio in campo applicativo anche per la vita di tutti i giorni. L'Università di Padova non manca di fare la sua parte attiva in questo settore. A partire dal 2003 all'interno del Dipartimento di Ingegneria dell'Informazione è stato costituito il gruppo QuantumFuture, dove fisici e ingegneri operano fianco a fianco sulle ricerche nelle comunicazioni quantistiche. Inoltre, dal 2020 presso l'Ateneo patavino è stato attivato il *Padua Quantum Technologies Research Center*, qtech.unipd.it, nel quale operano anche matematici e chimici.

Un esempio concreto di applicazione delle comunicazioni quantistiche negli usi quotidiani avvenne proprio a Padova il 12 febbraio 2021: ci fu una dimostrazione pubblica utilizzando gli apparati, sviluppati dal gruppo QuantumFuture, per generare e misurare stati quantistici e scambiarli, sfruttando il collegamento in fibra ottica dell'Ateneo, che connette i Dipartimenti e il Centro di Calcolo. Nella dimostrazione sono state scambiate delle chiavi numeriche grazie al protocollo di distribuzione quantistica delle chiavi (QKD - Quantum Key Distribution) conosciuto come BB84. Attraverso chiavi crittografiche di questo tipo, il socio Rosario Rizzuto, all'epoca Rettore dell'Università, ha inviato al socio Bruno Chiarellotto, Direttore del Dipartimento di Matematica, la lettera rivolta all'Ateneo e riportata di seguito, con lo scopo di introdurre le tecnologie quantistiche, spiegarne l'origine, gli sviluppi patavini e le potenzialità.

800 1222·2022 ANNI

UNIVERSITÀ DEGLI STUDI DI PADOVA

Il Rettore

Padova, 12 febbraio 2021

Care colleghe e colleghi docenti e del personale tecnico e amministrativo. Care studentesse e studenti,

con la trasmissione di questo documento si inaugura il primo tratto della Rete Quantistica dell'Università degli Studi di Padova, il quale congiunge tramite fibra ottica la sede dei Servizi Informatici e Telematici dell'Università in Via San Francesco con il Dipartimento di Matematica in Via Trieste. Con questa rete è possibile effettuare uno scambio di chiavi crittografiche la cui sicurezza è garantita dai princìpi fondamentali della meccanica quantistica, e che poi possono essere usate per l'autenticazione o la criptazione delle comunicazioni. Ad esempio, la trasmissione del presente documento è autenticata tramite queste chiavi ed è quindi impossibile che esso arrivi a destinazione manomesso da intrusi.

Le tecnologie quantistiche sono un fiorente campo di ricerca, che negli ultimi anni ha attirato l'attenzione di accademie e industrie di tutto il mondo. Padova è all'avanguardia, avendo investito da oltre un decennio sulla ricerca e sviluppo di soluzioni che applichino la meccanica quantistica per andare oltre ciò che la fisica classica può fare. Nel campo della sicurezza informatica, il risultato odierno è un passo importante per rendere invulnerabili le nostre comunicazioni, prima all'interno dell'Ateneo e, in futuro, in una Rete Quantistica Italiana estesa su tutto il territorio nazionale.

I vantaggi offerti da questi sviluppi non si limitano alle comunicazioni. Per questo l'Università ha dato il via ad un nuovo Centro di Ateneo per le Tecnologie Quantistiche che stimolerà la sinergia fra vari Dipartimenti e la collaborazione all'interno di un folto gruppo di brillanti ricercatrici e ricercatori per portare le tecnologie quantistiche verso nuove direzioni.

Con la trasmissione autenticata di questo documento, l'Università degli Studi di Padova dimostra ancora una volta di essere pronta per le sfide del futuro.

Ringrazio tutti voi per la cortese attenzione e porgo i miei,

Cordiali saluti

Il Rettore

Rosario Rizzuto

Questo documento è un esempio usato allo scopo della dimostrazione della Rete Quantistica in data 12 Febbraio 2021 e non ha validità ufficiale.

Palazzo Bo, via VIII febbraio 2 35122 Padova, Italy tel. +39 049 8273001, fax +39 049 8273009, rettore@unipd.it

Lettera del Rettore di Padova all'Ateneo, distribuita per la dimostrazione, che introduce le tecnologie quantistica e le sue applicazioni.

La particolarità di questa trasmissione è che è stata autenticata, ovvero il destinatario ha ricevuto una conferma basata sulla verifica di una chiave numerica che era nota solo ai

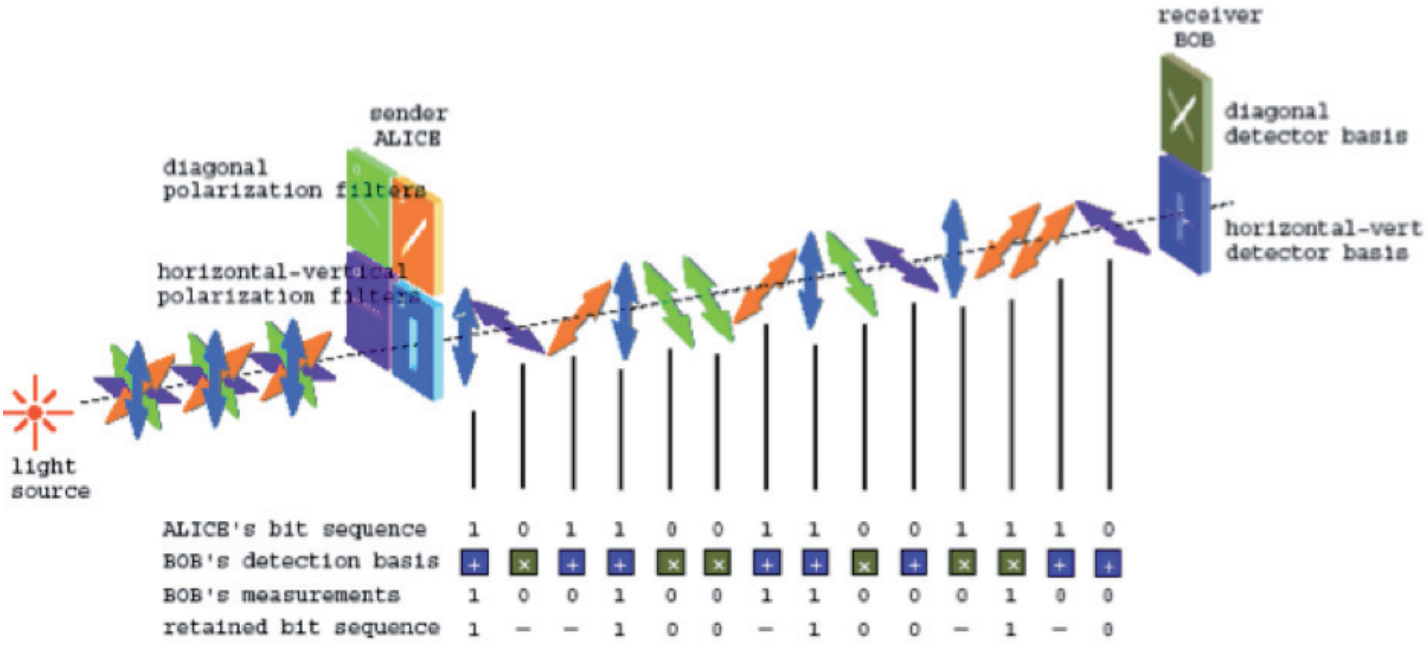
due interlocutori e che ha attestato l'autenticità del mittente. È stato anche possibile inviare delle immagini, come ad esempio un'immagine, presa col telescopio di Quantum Future, che è stato possibile autenticare e rendere fruibile solo al destinatario legittimo, mentre a eventuali origliatori sarebbe apparsa come un'immagine caotica. Inoltre, i due interlocutori hanno potuto dialogare con una chat sia audio che video, avendo assicurata la protezione della comunicazione attraverso una chiave sicura.

In sostanza, il sistema di QKD utilizzato consente ai due interlocutori di disporre di una chiave crittografica, i cui usi comprendono l'autenticazione, la verifica dell'integrità del messaggio e la cifratura di un file, che può essere poi diffuso in un canale non protetto come per esempio il telefono o Internet. Lo scopo della QKD è quindi quello di rendere sicure le comunicazioni e si inquadra nella ricerca di soluzioni per contrastare il crimine digitale, o *cyber-crime*.

Allo stesso tempo, la tecnica si basa sullo scambio di stati quantistici e permette la sperimentazione di nuovi paradigmi di comunicazione. Questo ambito tecnologico è di fatto molto recente: i primi protocolli sono della prima metà degli anni 80 del '900. Tuttavia, la sua potenzialità è stata dimostrata con una serie di esperimenti scientifici più recenti, grazie ai quali si è anche attestata la fattibilità tecnologica. Su questa base la Commissione Europea si è mossa con decisione e a partire da quattro anni fa ha spinto a un cambiamento tecnologico europeo in campi come il calcolo ad alte prestazioni, le comunicazioni sicure e la metrologia, sintetizzata con lo slogan: *The future is quantum*.

Nelle comunicazioni quantistiche si sfrutta la luce e in particolare la sua rappresentazione come quanti di energia, detti anche fotoni, proposti da Einstein per spiegare l'effetto fotoelettrico nel 1905, per il quale ricevette il premio Nobel nel 1921. La quantizzazione dell'energia rivoluzionò la nostra comprensione della natura della luce e dell'interazione tra radiazione e materia, e stimolò la nascita della meccanica quantistica, la teoria che ci ha permesso di comprendere il microcosmo. Grazie a questa comprensione è stato possibile scoprire molti effetti di estrema importanza sia concettuale, come le teorie che hanno unificato le forze, sia pratica, con l'ideazione di molte applicazioni che hanno aperto le porte a grandi sviluppi come il transistor, il laser, i metodi di indagine dei materiali, di predizione di fenomeni e di studio di nuove strutture della materia, composti, sistemi di nanoelettronica, farmaci etc.

Il protocollo per lo scambio di chiavi BB84 consta nel preparare e inviare, da parte del trasmettitore, convenzionalmente chiamato Alice, un singolo fotone alla volta in uno stato quantistico che rappresenta una direzione tra le quattro possibili. Queste direzioni consistono in quattro diverse polarizzazioni del fotone, orizzontale/verticale (primo sistema di riferimento) oppure diagonale/anti-diagonale (secondo sistema di riferimento), che vengono scelte casualmente, invio per invio. Esse sono indicate nella figura con quattro colori diversi. Questo treno di fotoni, chiamati QUBIT, viene inviato lungo un canale che non deve alterare lo stato del fotone e raccolto da un ricevitore, convenzionalmente chiamato Bob, dove avviene la misura quantistica secondo i due sistemi di riferimento, ancora una volta scelti a caso.

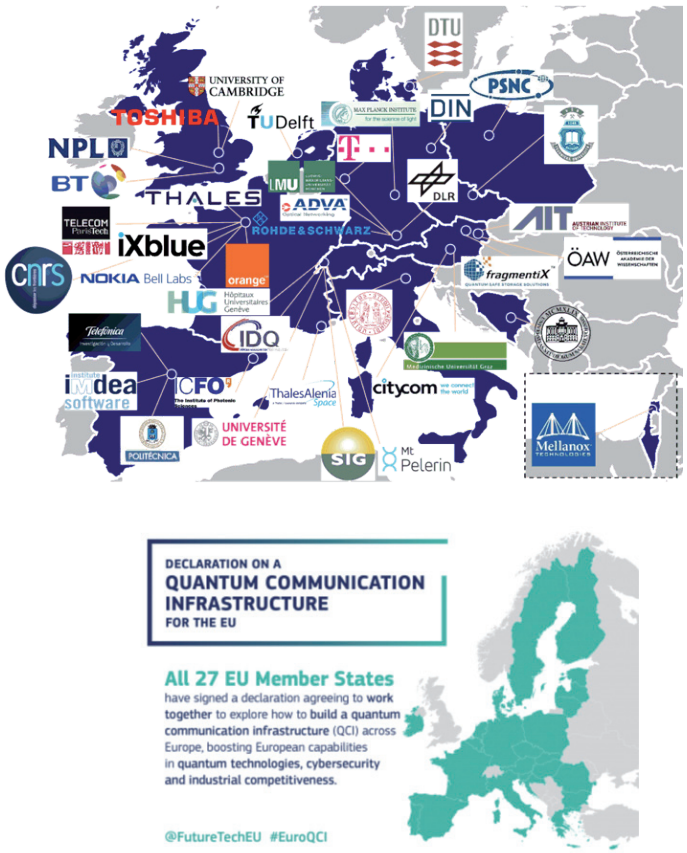


La distribuzione quantistica della chiave QKD secondo il protocollo BB84, che utilizza quattro stati quantistici del fotone, con diverse polarizzazioni.

Nel 50% dei casi, i sistemi di riferimento di Alice e Bob coincidono. In questi casi c'è una correlazione precisa tra la scelta fatta nella preparazione e il risultato della misura effettuata, dando origine a una sequenza di bit (1 e 0) da usare per la chiave. La forza di questo protocollo sta nel contrastare possibili origliatori: chi cerca di inserirsi e vuole fare una misura in una posizione intermedia cambia lo stato e introduce degli errori. La quantificazione di questi errori, QBER, è un parametro cruciale che ha una soglia limite oltre la quale l'applicazione del protocollo non è possibile, ma al di sotto della quale permette di eliminare qualsiasi informazione condivisa con l'esterno grazie a un protocollo che si chiama *privacy amplification*. Sottolineiamo che lo scambio di singoli fotoni rappresenta la più fondamentale correlazione tra sistemi, essendo basata su particelle elementari.

Lo stato di sviluppo delle comunicazioni quantistiche e di questo scambio di chiavi ha raggiunto ormai la scala planetaria. In Europa da oltre un anno opera il progetto OpenQKD, con oltre 40 partner (vedi pannello in alto) rivolto a dimostrazioni sia in fibra che spazio libero. L'Università di Padova, unico membro italiano, ha in carico delle dimostrazioni per mettere in sicurezza l'informazione sul funzionamento degli orologi installati nei satelliti tipo GNSS e di avvalorare una tecnica nella quale i qubit viaggiano prima in spazio libero e poi in fibra. OpenQKD tra i suoi scopi si rivolge alla protezione di dati sanitari e finanziari e di trasmissioni governative. Il passo successivo in programma in Europa è la realizzazione di un'infrastruttura per le comunicazioni sicure (QCI) sottoscritta da tutti i 27 Paesi membri, basata sia su canali in fibra che spaziali.

La Cina è stata particolarmente attiva nello sviluppo della tecnica QKD nell'ultimo decennio, con la realizzazione di una dorsale tra Pechino e Shanghai di 2000 km, e anche con il lancio del satellite Micius, dal nome di uno scienziato cinese di epoca antica, che ha permesso di coprire grandi distanze e in particolare di dimostrare la comunicazione sicura tra due continenti.



Il progetto OpenQID per sviluppare testbed di QKD in Europa e l'iniziativa QCI firmata da tutti i 27 Stati membri.

Oltre a queste applicazioni nelle comunicazioni, lo scambio di stati quantistici è il metodo su cui si baserà il quantum internet, che scambierà stati quantistici tra computer quantistici, dispositivi come memorie, misuratori, analogamente a come il sistema internet che conosciamo opera con i dati.

Bibliografia essenziale

S. Pirandola et al, *Advances in quantum cryptography*, «Adv. Opt. Photonics» 12, 1012 (2020).

S. Wehner, D. Elkouss, R. Hanson, *Quantum internet: A vision for the road ahead*, «Science» 362 (2018).

S.-K. Liao et al, *Satellite-to-ground quantum key distribution*, «Nature» 549, 43–47 (2017).

S.-K. Liao et al, *Satellite-Relayed Intercontinental Quantum Network,* «Phys. Rev. Lett.» 120, 030501 (2018).

J. G. Ren et al, *Ground-to-satellite quantum teleportation*, «Nature» 549, 70–73 (2017).

J. Yin et al, *Satellite-based entanglement distribution over 1200 kilometers*, «Science» 356, 1140–1144 (2017).

P. Villoresi et al, *Experimental verification of the feasibility of a quantum channel between space and Earth*, «New J. Phys.» 10, 033038 (2008).

D. Bacco, M. Canale, N. Laurenti, G. Vallone, P. Villoresi, *Experimental quantum key distribution with finite-key security analysis for noisy channels*, «Nature» Commun. 4, 2363 (2013).

G. Vallone et al, *Experimental Satellite Quantum Communications*, «Phys. Rev. Lett.» 115, 040502 (2015).

G. Vallone et al, *Interference at the Single Photon Level Along Satellite-Ground Channels*, «Phys. Rev. Lett.» 116, 253601 (2016).

F. Vedovato et al, *Extending Wheeler's delayed-choice experiment to space*, «Science», Adv. 3, e1701180 (2017).

M. Avesani, D. G. Marangon, G. Vallone, P. Villoresi, *Source-device-independent heterodyne-based quantum random number generator at 17 Gbps*, «Nature» Commun. 9, 5365 (2018).

M. Avesani et al, *Resource-effective quantum key distribution: a field trial in Padua city center*, «Opt. Lett.» 46, 2848 (2021).

M. Avesani et al, *Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics*, «Nature» Quantum Inf. 7, 93 (2021).

*Paolo Villoresi è professore ordinario di Fisica nell'Università di Padova e socio corrispondente dell'Istituto Veneto di Scienze, Lettere ed Arti