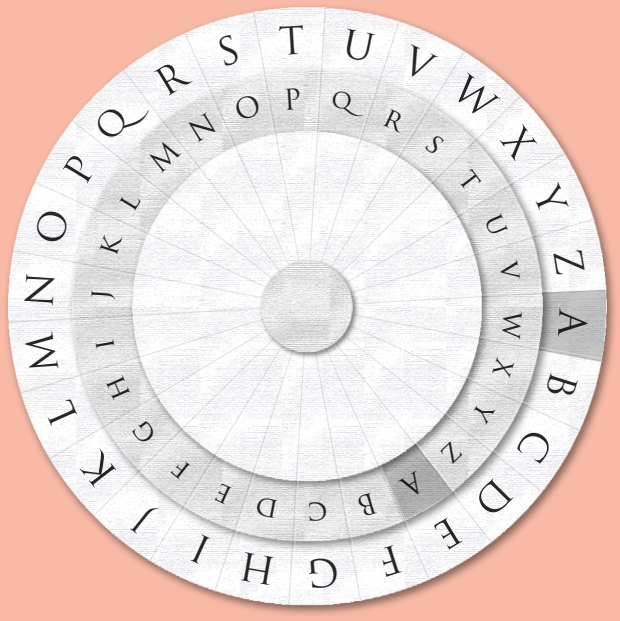
Comunicare nell'era dei quanti

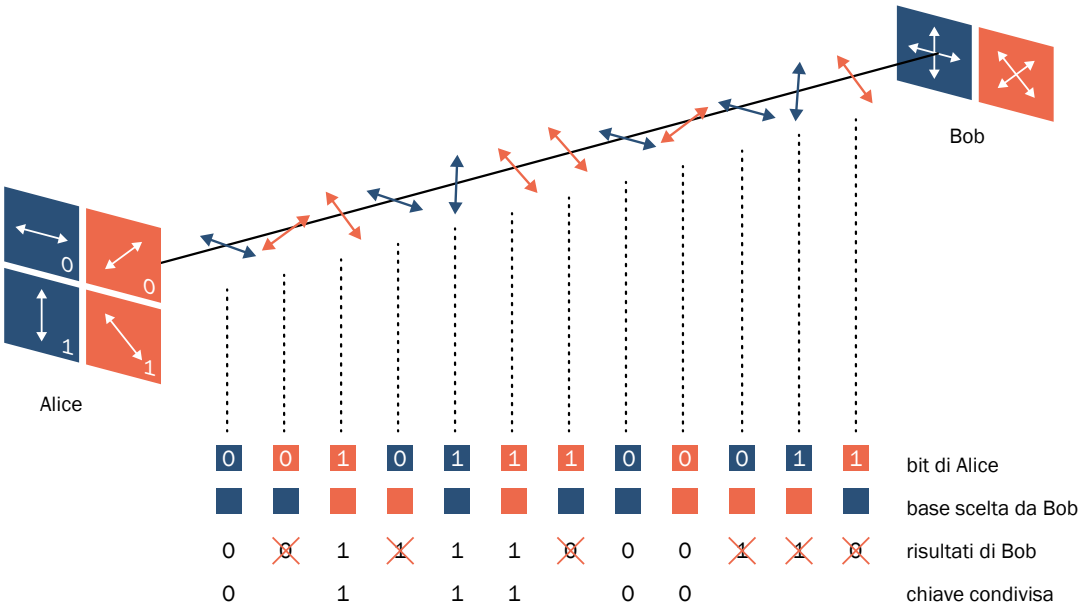
Crittografia, teletrasporto e network quantistici

di Michele Rota, Francesco Basso Basset e Rinaldo Trotta



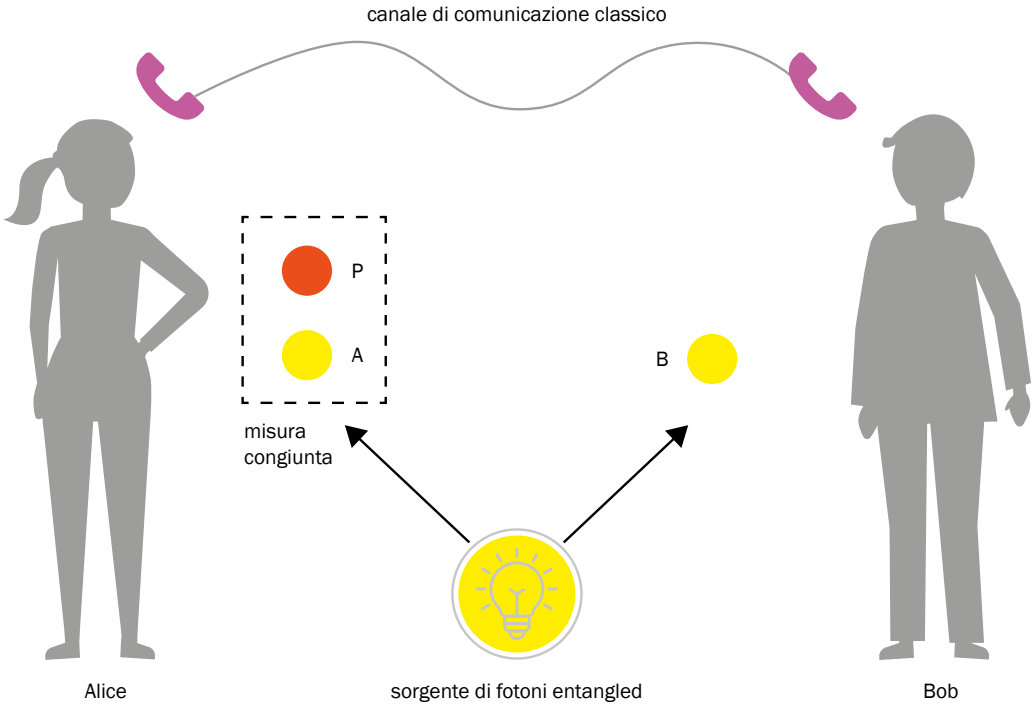
a.
Un esempio di cifrario di Cesare, in cui le lettere dell'alfabeto sono sostituite scorrendo rigidamente l'alfabeto di un numero predefinito di posti. Una ruota fa scorrere due sequenze alfabetiche permettendo la cifratura e la decifratura: a ogni lettera del cerchio interno corrisponde una lettera del cerchio esterno.

La necessità di nascondere o rendere illeggibile un messaggio a occhi indiscreti è stata una preoccupazione della società umana fin dall'invenzione della scrittura: questo ha portato alla nascita della crittografia, dal greco "scrittura nascosta". Uno dei primi metodi di crittografia è attribuito a Giulio Cesare. Nel cifrario di Cesare le singole lettere del messaggio sono sostituite facendo scorrere l'alfabeto di un certo numero di posizioni, il che rende il messaggio apparentemente illeggibile (vd. fig. a). Sapendo di quante lettere spostarsi è però possibile ricostruire il messaggio originale applicando la trasformazione inversa: si tratta di un esempio di crittografia a chiave simmetrica, dove il segreto condiviso, la chiave, in questo caso è il numero di lettere spostate. La teoria dell'informazione, che nel XXI secolo ha dato delle basi rigorose al campo della crittografia, in realtà dimostra che, per evitare che un simile messaggio criptato venga decifrato, occorre impiegare un cifrario di Cesare diverso per ogni lettera. Nell'algoritmo *one-time pad*, che si ispira a questo principio, la sicurezza viene garantita utilizzando una chiave scelta in maniera completamente casuale, non riutilizzabile (*one-time*), e della stessa lunghezza del messaggio. È importante sottolineare che questo algoritmo "classico" di crittografia è teoricamente perfetto, nel senso che la sua sicurezza è comprovata da un teorema matematico dovuto a Claude Shannon. Tuttavia, rimane aperta l'enorme sfida di come scambiare la chiave tra le due parti in maniera sicura.
Una parziale soluzione a questo inconveniente è il metodo della chiave asimmetrica, in cui una chiave pubblica viene usata per cifrare un messaggio e una chiave privata e segreta è usata per poi decifrarlo. Un algoritmo a chiave simmetrica molto importante è l'algoritmo RSA (dalle iniziali degli ideatori Ron Rivest, Adi Shamir e Leonard Adleman) che è oggi alla base della comunicazione crittografata sulle reti informatiche. Questo metodo si affida a un principio di sicurezza computazionale: la fattorizzazione in numeri primi di un intero richiede risorse estremamente maggiori rispetto all'operazione inversa, ossia la moltiplicazione tra due numeri primi. Ad esempio, utilizzando un



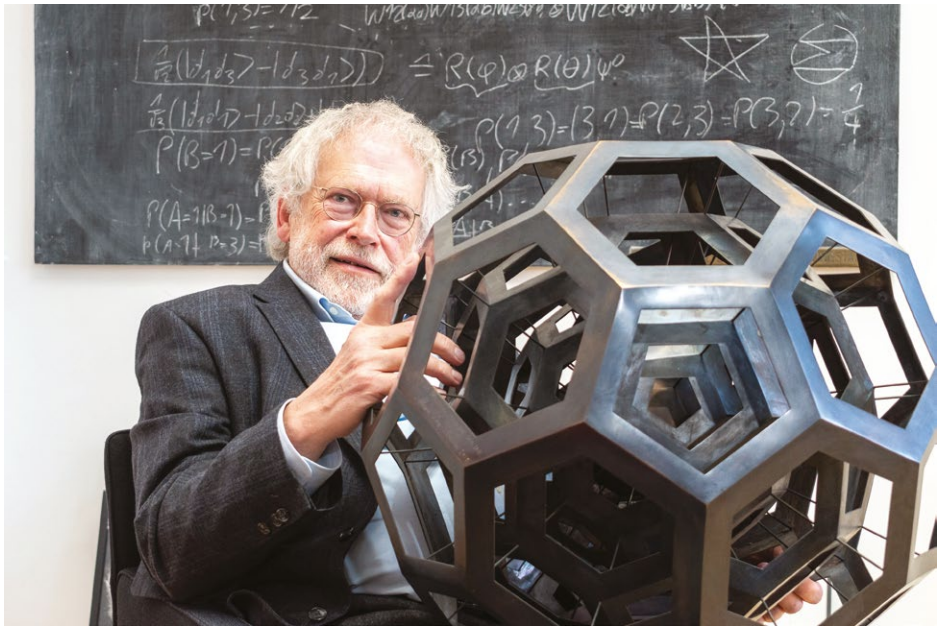
comune algoritmo classico di decodifica, la fattorizzazione di un intero risultante dal prodotto di due numeri primi di tre cifre richiederebbe miliardi di anni. Ma questa sicurezza apparente viene oggi messa in seria discussione dall'avvento della computazione quantistica.
Nel 1994 Peter Shor dimostrò che la fattorizzazione di cui sopra può essere eseguita in una manciata di secondi utilizzando un algoritmo che gira su un computer quantistico. L'avvento delle tecnologie quantistiche pone quindi a rischio la sicurezza dei metodi crittografici moderni, un problema non da poco considerando che già allo stato attuale le perdite stimate per frodi informatiche oscillano tra i 45 e i 654 miliardi di dollari nel solo 2018 (dal Rapporto *Systemic Cyber Risk 2020* del Comitato Europeo per il Rischio Sistemico). La risoluzione di queste difficoltà risiede proprio nella meccanica quantistica e nell'opportunità di guardare in maniera "positiva" ai divieti imposti dalle sue leggi caratteristiche.
È ben noto come la meccanica quantistica limiti le possibilità di intervento su alcune grandezze fisiche del mondo microscopico: è impossibile misurare contemporaneamente due grandezze "coniugate" (come, per esempio, la velocità e posizione di una particella quantistica), osservare uno stato quantistico senza perturbarlo in maniera irreparabile, leggere e copiare uno stato quantistico (*no-cloning*), e la lista dei divieti può continuare. Questa psicologia "negativa", come la definisce Nicolas Gisin, può però essere ribaltata pensando che tali divieti si applichino anche a un malintenzionato, che non può intercettare la chiave segreta senza introdurre errori che ne rivelino la presenza. Proprio questa interpretazione "positiva" dei divieti è alla base della crittografia quantistica e il principio di funzionamento è piuttosto semplice: una chiave segreta viene generata tra due parti trasmettendo un segnale quantistico su un canale in chiaro e codificando i bit della chiave in uno dei suoi gradi di libertà. Comunemente vengono utilizzati fotoni singoli e il loro stato di polarizzazione viene utilizzato per codificare i bit della chiave (vd. fig. b).
Ad ogni passaggio le due parti misurano casualmente lo stato di polarizzazione del singolo fotone e, *a posteriori*, si scambiano informazioni sul tipo di misura effettuata. Quando il tipo di misura coincide, il risultato è aggiunto come bit alla chiave crittografica, altrimenti è scartato. Come detto, le leggi della meccanica quantistica proibiscono di intercettare la chiave senza introdurre errori nella sequenza di bit scambiati, il che offre l'opportunità di verificare una eventuale violazione attraverso confronti mirati. Una volta che la segretezza della chiave viene certificata dalla meccanica quantistica, è possibile utilizzare metodi di crittografia classica, ad esempio *one-time pad*, per scambiare informazioni in maniera completamente sicura.

b.
Esempio del funzionamento di un protocollo di distribuzione di chiave crittografica (il cosiddetto BB84). Alice manda singoli fotoni a Bob, codificando i singoli bit dell'informazione in due "alfabeti" diversi scelti casualmente, dati dalla base della polarizzazione dei fotoni, lineare/orizzontale (blu) e diagonale/anti-diagonale (rosso). Bob riceve i fotoni e li misura scegliendo casualmente la base di misura e segna tutti i risultati ottenuti. Dopo la sessione di trasmissione Alice e Bob confrontano le basi di misura scelte e quando il fotone è stato preparato e misurato nella stessa base mantengono il bit corrispondente che andrà ad aggiungersi alla chiave crittografica. Se i fotoni vengono intercettati e misurati da un "ascoltatore" i risultati delle misure di Bob saranno incongruenti con quelli mandati da Alice e la violazione di sicurezza sarà rivelata.



Esistono già soluzioni commerciali, sviluppate da compagnie come Toshiba e ID Quantique, per lo scambio di chiave quantistica attraverso ordinarie fibre ottiche che raggiungono distanze di alcune centinaia di chilometri. Varie istituzioni di ricerca internazionali hanno realizzato reti dimostrative che coprono distanze maggiori utilizzando stazioni fidate intermedie, e tra esse possiamo annoverare l'iniziativa nazionale Italian Quantum Backbone. Questi progetti di ricerca e sviluppo mirano a realizzare la visione in cui la crittografia quantistica possa inserirsi nella rete di comunicazione globale, collegando diversi nodi mediante fibre ottiche a distanze continentali e intercontinentali e interfacciandosi con satelliti in orbita. Anche in quest'ultimo ambito si riscontra un intenso sviluppo tecnologico, con il satellite cinese Micius che nel 2016 ha dimostrato uno scambio quantistico di chiave segreta su una distanza di 1120 chilometri, sicuro contro eventuali attacchi diretti al satellite stesso.
Una sfida da superare nelle comunicazioni dirette su lunga distanza (si pensi ai 3000 chilometri della dorsale atlantica che connette l'Europa e il Nordamerica) e per la realizzazione in un network globale di comunicazione quantistica è costituita dall'attenuazione del segnale e dall'impossibilità di utilizzare i convenzionali amplificatori ottici, altra conseguenza del teorema di *no-cloning*. Non ci sorprende come la meccanica quantistica ancora una volta offra una soluzione attraverso il celebre protocollo di teletrasporto quantistico. Tramite il teletrasporto quantistico è infatti possibile trasferire fedelmente uno stato quantistico qualsiasi tra due luoghi, senza richiedere che un portatore di informazione in tale stato percorra fisicamente l'intera distanza interposta. Come mostrato in fig. c per la versione fotonica del teletrasporto, il fotone che codifica lo stato quantistico viene fatto "interagire" con un fotone di una coppia di fotoni fortemente correlati tra loro. Il legame tra questi fotoni è talmente forte che qualsiasi "cambiamento" su uno di essi si ripercuote istantaneamente sull'altro, indipendentemente dalla distanza. Questa proprietà, ovvero l'entanglement, permette, con l'ausilio di un canale di comunicazione classico, di trasferire lo stato quantistico sul secondo fotone della coppia e quindi di aumentare le distanze raggiungibili dai protocolli di crittografia.
È possibile fare un ulteriore passo e costruire un ripetitore quantistico in cui è l'entanglement stesso a essere teletrasportato.

c.
Schema del protocollo di teletrasporto quantistico. Alice è in possesso di un fotone (P), il cui stato vuole trasmettere a Bob. Producendo una coppia di fotoni entangled, si fa interagire il fotone di Alice con uno di questi fotoni (A). L'altro fotone entangled (B) è consegnato a Bob. Quando Alice misura lo stato congiunto di P e A, a causa dell'entanglement il fotone di Bob collassa in uno stato collegato con quello di P. Attraverso un canale classico Alice comunica a Bob il risultato della sua misura, e ciò permette a Bob di effettuare un'operazione su B portandolo esattamente nello stato in cui si P trovava all'inizio.



d.
Anton Zeilinger, premio Nobel per la Fisica 2022 insieme a John F. Clauser e Alain Aspect per aver aperto la strada alla scienza dell'informazione quantistica. Il suo gruppo a Innsbruck ha pubblicato nel 1998, in contemporanea al gruppo di Roma di Francesco De Martini, la prima dimostrazione del teletrasporto quantistico descritto in questo articolo.

Una delle proposte principali per realizzare un ripetitore quantistico si basa su un'infrastruttura composta da nodi intermedi, in cui l'entanglement viene teletrasportato a catena fino alle due parti in comunicazione. I nodi possono coinvolgere sia stazioni a terra collegate da fibre ottiche che satelliti in orbita. Con l'ausilio di hardware di memoria volatile (memoria quantistica) che permettono di sincronizzare i diversi nodi della catena, questo protocollo ha la capacità di superare i limiti di attenuazione dei canali di comunicazione ottica. A sottolineare l'importanza di questi concetti ricordiamo come il premio Nobel per la fisica di quest'anno sia stato assegnato a tre pionieri dell'entanglement, Alain Aspect, John Clauser e Anton Zeilinger, che con i loro studi hanno fatto sì che le formidabili proprietà della meccanica quantistica potessero essere applicate alla tecnologia. Lo sviluppo dei ripetitori quantistici presenta nuove sfide tecniche che coinvolgono enti di ricerca e un numero crescente di spin-off universitari e start-up. L'obiettivo principale è quello di realizzare dispositivi in grado di generare in maniera riproducibile miliardi di fotoni singoli o in stati di entanglement al secondo e, allo stesso tempo, di sviluppare componenti in grado di trasferire, manipolare e immagazzinare gli stati quantistici con elevata efficienza, frequenza di operazione e accuratezza. Diverse tecnologie quantistiche si sono dimostrate capaci di soddisfare alcuni dei requisiti ma, allo stato attuale, un ripetitore quantistico funzionale non è stato ancora realizzato. Le ricerche in atto richiedono ancora grandi sforzi, che tuttavia vale la pena sostenere in quanto la realizzazione di un network quantistico su scala globale potrebbe rivoluzionare il nostro modo di comunicare e scambiare informazioni nel prossimo futuro.

Biografia

Francesco Basso Basset è ricercatore presso il Dipartimento di Fisica della Sapienza Università di Roma. Specializzato in spettroscopia ottica, nanotecnologie a semiconduttore e ottica quantistica, la sua attività di ricerca si concentra sullo sviluppo di sorgenti fotoniche a quantum dot e sul loro impiego nell'informazione e comunicazione quantistica.

Michele Rota è assegnista di ricerca nel Dipartimento di Fisica della Sapienza Università di Roma, dove ha conseguito il dottorato di ricerca in fisica nel 2021. Si occupa di esperimenti di ottica per la comunicazione in network quantistici e dello sviluppo di nuove sorgenti di luce entangled basate su quantum dots.

Rinaldo Trotta è professore associato presso il Dipartimento di Fisica della Sapienza Università di Roma, dove coordina il gruppo di ricerca Nanophotonics. I suoi interessi spaziano dalla fisica dei semiconduttori nanostrutturati al campo dell'informazione e comunicazione quantistica.

10.23801/asimmetrie.2022.33.7