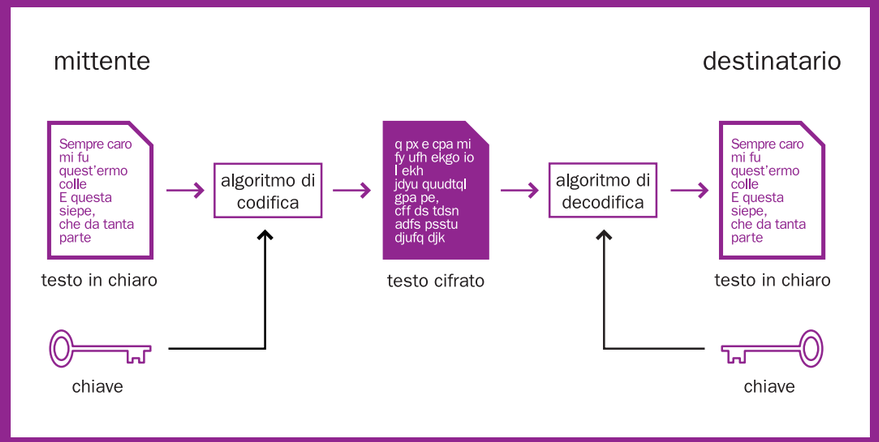
Fotoni e segreti

La meccanica quantistica al servizio della crittografia

di GianCarlo Ghirardi e Francesca Scianitti

Le straordinarie potenzialità dell'applicazione di alcuni aspetti della meccanica quantistica, tra i quali ad esempio l'entanglement (vd. p. 8, ndr), hanno portato alla nascita della moderna teoria quantistica dell'informazione.
Utilizzata oggi per lo scambio di informazioni protette, anche nelle comuni applicazioni del commercio telematico o per la protezione della privacy nell'uso della posta elettronica, la *crittografia* ha origini molto antiche e ha raggiunto nella sua evoluzione livelli elevatissimi, con l'obiettivo di rendere i protocolli di scambio sempre più sicuri. Tuttavia, per quanto il protocollo sia sofisticato, il problema dell'inviolabilità dall'esterno non è mai completamente risolto ed è praticamente impossibile ottenere la certezza della segretezza.
La natura del problema è la seguente. Se due persone – che chiameremo Alice e Bob – vogliono trasmettersi un messaggio senza che nessun'altro sia in grado di leggerne il contenuto, useranno una chiave per cifrare il messaggio, cioè trasformarlo in modo da renderlo irriconoscibile attraverso un processo di codifica (un *algoritmo*). Solo chi è in possesso della chiave può ricostruire il messaggio originale (vd. fig. a).



a.
Per cifrare il testo di un messaggio (il *testo in chiaro*), il mittente lo codifica utilizzando un *algoritmo*, un procedimento generale di scrittura segreta, i cui dettagli sono precisati solo scegliendo una chiave. Applicando insieme *chiave* e algoritmo a un testo in chiaro, questo è trasformato in un *testo cifrato*. Il testo cifrato può essere intercettato da una spia durante la trasmissione al destinatario, ma (almeno nel caso in cui l'algoritmo usato sia sufficientemente raffinato) la spia non dovrebbe essere in grado di decodificarlo. Il destinatario, invece, conoscendo l'algoritmo e la chiave usati dal mittente, può ripristinare il testo in chiaro.

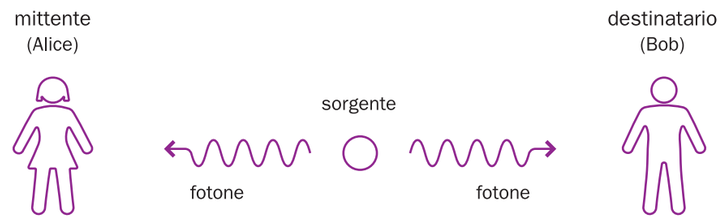
[as] approfondimento

Il principio di indeterminazione di Heisenberg

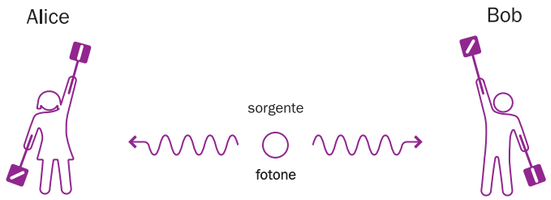
Uno dei principi fondanti della meccanica quantistica è il principio di indeterminazione di Heisenberg del 1927. Esso prevede che esistano grandezze, dette *coniugate*, il cui valore non può mai essere determinato simultaneamente con esattezza, in quanto la misura (più o meno precisa) di uno influisce sull'altro rendendolo (più o meno) casuale e quindi indeterminato. In particolare, il prodotto delle rispettive incertezze di misura deve essere maggiore della costante di Planck h divisa per 4π. Un esempio è dato dalle grandezze posizione e momento (il prodotto tra la massa e la velocità) di una particella: quando si cerca di stabilire precisamente con quale velocità si sta muovendo una particella, inevitabilmente la sua posizione diventa indeterminata. In altre parole, più accuratamente si misura la velocità, meno nota sarà la posizione, visto che il prodotto delle incertezze ha un valore minimo.
Anche gli stati di polarizzazione rettilinea (verticale od orizzontale) e diagonale (a 45° o 135°) sono grandezze coniugate. Di conseguenza, possiamo fare una misura per stabilire se un fotone ha polarizzazione verticale od orizzontale oppure a 45° o a 135°, ma non potremo mai fare una misura che distingua tra tutte e quattro queste possibilità, perché una volta misurato (ad esempio) lo stato di polarizzazione verticale-orizzontale quello a polarizzazione 45°-135° risulta del tutto indeterminato. Per questo, una scelta appropriata per Alice e Bob sui fotoni entangled può essere di usare un filtro verticale e uno a 45°.

L'inviolabilità della comunicazione dipenderà quindi dal modo in cui viene scambiata la chiave e non dal messaggio vero e proprio che, anche se letto dall'esterno, è (praticamente) indecifrabile senza la chiave. Affinché tale sistema sia efficace, Alice e Bob dovranno quindi scambiarsi la chiave di persona, poiché farlo attraverso un altro canale come il telefono o la posta elettronica sarebbe poco sicuro. Questo della "distribuzione delle chiavi" è un problema che può essere risolto secondo protocolli diversi, ma in generale non può essere reso inviolabile senza fare ricorso ai principi della meccanica quantistica. La necessità di attuare lo scambio delle chiavi "a distanza" può essere risolta infatti sfruttando la particolare natura dei fotoni entangled, le cui caratteristiche, ad esempio di polarizzazione, restano correlate anche a distanza, senza che tra i due fotoni vi sia più alcuna interazione dopo la loro creazione.
Il protocollo di scambio delle chiavi proposto da Artur Eckert nel 1991 sfrutta proprio questa natura quantistica dei fotoni e l'entanglement.

Passo 1 (vd. fig. b). Una sorgente emette ogni secondo una coppia di fotoni entangled, che si propagano in direzioni opposte tra un mittente (Alice) e un destinatario (Bob), posti a una distanza qualsiasi dalla sorgente. In generale, lo stato di polarizzazione del sistema dei due fotoni entangled sarà una combinazione lineare (sovrapposizione di stati quantistici) di stati di polarizzazione ortogonali tra loro (ad esempio verticale e orizzontale, oppure a 45° e a 135°, vd. approfondimento).

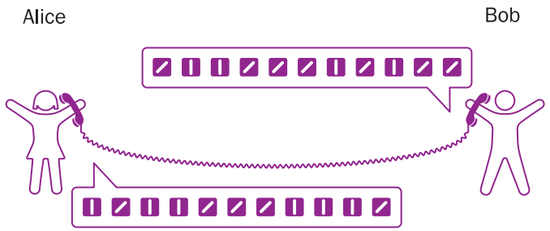


b.



c.

Alice		Bob	
filtro utilizzato	esito della misura	filtro utilizzato	esito della misura
▮	1	◪	0
◪	0	▮	1
▮	1	▮	1
▮	0	◪	1
◪	0	◪	0
◪	1	◪	1
◪	0	▮	1
▮	1	◪	0
▮	0	▮	0
▮	1	◪	1
◪	0	◪	0



d.

Alice		Bob		
filtro utilizzato	esito della misura	filtro utilizzato	esito della misura	chiave
▮	1	◪	0	
◪	0	▮	1	
▮	1	▮	1	1
▮	0	◪	1	
◪	0	◪	0	0
◪	1	◪	1	1
◪	0	▮	1	
▮	1	◪	0	
▮	0	▮	0	0
▮	1	◪	1	
◪	0	◪	0	0

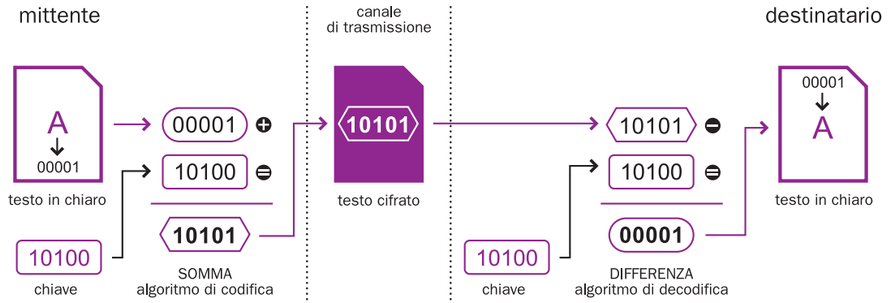
e.

Passo 2 (vd. fig. c). Per generare la chiave comune, Alice e Bob stabiliscono di eseguire una serie di misure di polarizzazione sulle varie coppie di fotoni entangled emesse in successione dalla sorgente, usando arbitrariamente filtri che rivelano se la polarizzazione è verticale o a 45° (indicati nella figura con due differenti palette) e senza comunicarsi la sequenza delle misure che eseguiranno. Indicando con 1 o 0 l'esito della misura (1 se il fotone supera il "test" di misura di polarizzazione – ad esempio il filtro è di tipo "verticale" e il fotone riesce a superarlo – e 0 se non lo supera) la sequenza degli esiti registrati da Alice e Bob sarà una sequenza del tipo 10100101010, ricordando che in ogni misura si ha la stessa probabilità di avere come esito 1 o 0. Nella tabella in figura sono indicati, sia per Alice che per Bob, il tipo di misura effettuata (il filtro utilizzato, verticale o a 45°) e l'esito corrispondente.

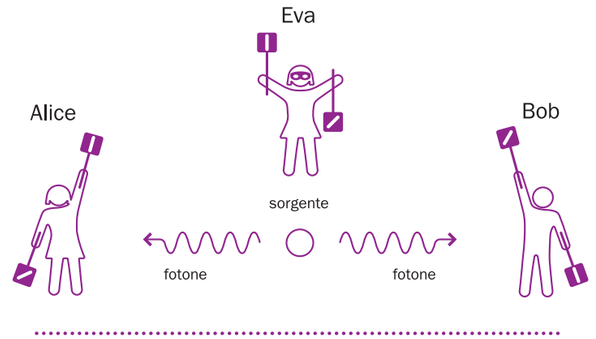
Passo 3 (vd. fig. d). Attraverso un canale di comunicazione tradizionale (per esempio il telefono) Alice e Bob annunciano l'un l'altro la sequenza del tipo di misure eseguite. Avendo eseguito le misure su fotoni entangled, sappiamo con certezza che nei casi in cui Alice e Bob hanno eseguito lo stesso tipo di misura, cioè hanno utilizzato lo stesso filtro, essi hanno anche scritto lo stesso numero.

Passo 4 (vd. fig. e). Eliminando tutti i casi in cui hanno eseguito misure diverse (ovvero in cui i numeri delle rispettive sequenze possono anche differire), Alice e Bob rimangono ciascuno con la stessa sequenza di 0 e 1, che hanno due caratteristiche essenziali: sono assolutamente identiche e la sequenza degli 0 e degli 1 è del tutto casuale. Questa è la loro chiave segreta! In particolare, nella tabella in figura sono evidenziati in grigio i casi in cui Alice e Bob hanno condotto misure diverse. Eliminando questi casi, si ottiene la sequenza "pulita" riportata nella terza colonna, cioè la chiave (10100 nel nostro esempio).

Passo 5 (vd. fig. f). Disponendo della stessa chiave segreta, Alice e Bob possono utilizzarla per trasmettersi un messaggio criptato. Un semplice algoritmo per farlo è quello di tradurre il messaggio in cifre – per esempio associando un numero a ogni lettera del messaggio – e di sommare alle cifre del messaggio le cifre della chiave segreta. L'unico modo per risalire dal testo cifrato a quello in chiaro è di disporre della stessa chiave. Nell'esempio in figura il messaggio da trasmettere è la lettera "A", a cui si è deciso di far corrispondere la sequenza 00001. Analogamente si opera con le altre lettere che compongono il testo in chiaro da trasmettere.



f.



	chiave	chiave finale
1. posto	1	1
2. posto	0	
3. posto	1	1
4. posto	0	
5. posto	0	0

g.

Passo 6 (vd. fig. g). La natura quantistica del fotone implica che una qualsiasi azione da parte di una spia, chiamiamola Eva, mirata a intercettare lo stato di polarizzazione dei fotoni che si propagano tra Alice e Bob, comporta una certa probabilità che gli esiti delle misure effettuate da Alice e Bob risultino diversi, anche quando i due personaggi eseguono la stessa misura. Questo perché, in generale, effettuando una misurazione sul sistema quantistico dei due fotoni entangled, si ha una certa probabilità di distruggere le correlazioni perfette tra loro per misure in direzioni diverse da quella scelta dalla spia (vd. approfondimento p. 10).
Per verificare se Eva sia intervenuta, Alice e Bob si comunicano pubblicamente un certo numero di esiti di misura che compongono la chiave segreta. Per un numero sufficientemente elevato di esiti comunicati (molti più di quelli rappresentati nella tabella dell'esempio in figura), Alice e Bob potranno essere praticamente certi di scoprire se Eva sia intervenuta, perché riscontrerebbero in questo caso almeno un esito discorde, pur avendo eseguito lo stesso tipo di misura. In tal caso dovrebbero ricominciare da capo tutto il procedimento. Altrimenti, rigettando gli esiti enunciati pubblicamente, che a questo punto non sarebbero più segreti, sarà possibile ottenere la chiave segreta da utilizzare nel caso non vi sia stato un intervento di Eva.
Nell'esempio raffigurato in figura, Alice e Bob stabiliscono di comunicarsi i numeri 0 o 1 della chiave segreta alla posizione pari (al secondo e quarto posto). In questo modo, se uno di questi numeri fosse diverso per Alice e Bob, i due personaggi saprebbero di essere stati spiati e potrebbero decidere di ricominciare da capo. Nel caso contrario, utilizzeranno la nuova chiave segreta (la seconda colonna della tabella in figura), più corta della prima, per cifrare e decodificare il messaggio.