



UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Sicurezza dei Sistemi e delle Reti Informatiche

PRESENTAZIONE DIDATTICA DELLA CRITTOGRAFIA QUANTISTICA E DEI CONCETTI COLLEGATI

Relatrice

Prof.ssa Laura Citrini

Tesi di Laurea di

Filippo Corsi

Matricola n. 671071

Anno Accademico 2006-2007

Indice

Introduzione	5
Caratteristiche e limiti della crittografia.....	7
<i>Sicurezza nella Crittografia.....</i>	<i>7</i>
<i>One-Time Pad.....</i>	<i>8</i>
<i>Crittografia Quantistica.....</i>	<i>10</i>
Introduzione alla fisica classica.....	12
<i>La natura della luce, l'esperimento di Young e le teorie successive</i>	<i>12</i>
<i>Alcune osservazioni sulla fisica classica.....</i>	<i>14</i>
<i>Cristalli Birifrangenti</i>	<i>22</i>
Introduzione alla fisica quantistica	24
<i>La notazione di Dirac (o notazione bra-ket).....</i>	<i>27</i>
<i>Il principio di sovrapposizione.</i>	<i>27</i>
<i>L'entanglement quantistico.....</i>	<i>28</i>
<i>Il paradosso EPR.....</i>	<i>29</i>
<i>Il Teorema di Bell.....</i>	<i>30</i>
Introduzione storica.....	32
<i>La moneta quantistica di Weisner</i>	<i>32</i>
QKD – Quantum Key Distribution	34
<i>Protocollo BB84</i>	<i>34</i>
<i>Il protocollo</i>	<i>34</i>
<i>Correzione errori e Privacy Amplification</i>	<i>39</i>
<i>Strategie di intercettazione</i>	<i>41</i>
<i>Protocollo E91</i>	<i>42</i>
<i>Oblivious Transfer.....</i>	<i>44</i>
<i>Il protocollo</i>	<i>44</i>
QKD ed algoritmi di cifratura tradizionali.....	47
<i>QKD e One Time Pad: sicurezza incondizionata.....</i>	<i>47</i>
<i>QKD e schemi di cifratura computazionalmente sicuri</i>	<i>47</i>
Conclusioni.....	49
Appendici.....	51
<i>A. Protocollo Diffie Hellman</i>	<i>51</i>
<i>B. Cenni alla computazione quantistica</i>	<i>53</i>
<i>C. Postulati fondamentali della meccanica quantistica.</i>	<i>55</i>
<i>Valori medi di grandezze fisiche.....</i>	<i>58</i>
<i>D. Note Matematiche</i>	<i>59</i>
<i>Definizione di operatore</i>	<i>59</i>
<i>Notazione Bra e Ket</i>	<i>61</i>

Bibliografia.....62

Introduzione

La necessità di proteggere le comunicazioni, in particolare in ambito militare e commerciale, ha richiesto fin dall'antichità lo sviluppo di tecniche crittografiche, inizialmente per garantire la segretezza dei contenuti e più recentemente per assicurare anche l'integrità dei messaggi e l'autenticazione delle parti.

La storia della crittologia è sempre stata caratterizzata dal confronto tra i crittografi, il cui compito è quello di proteggere le informazioni, ed i crittoanalisti, impegnati a scoprire o alterare i messaggi.

Una prima grossolana classificazione degli algoritmi crittografici è la seguente, basata principalmente sul fatto che si utilizzino una o due chiavi:

La crittografia simmetrica, anche detta crittografia convenzionale o crittografia a chiave unica si basa su uno schema formato da cinque elementi:

- Testo in chiaro: il messaggio originale, che si vuole trasmettere o archiviare in modo segreto;
- Algoritmo di crittografia: l'insieme di procedure di sostituzione e trasposizione applicate al testo in chiaro;
- Chiave segreta: parametro dell'algoritmo di crittografia, indipendente dal testo in chiaro, modifica l'output dell'algoritmo.
- Testo cifrato: il messaggio trasformato, prodotto dall'applicazione dell'algoritmo di crittografia con la chiave al testo in chiaro.
- Algoritmo di decrittografia: l'inverso dell'algoritmo di crittografia, consente di riprodurre il testo in chiaro a partire dalla chiave e dal testo cifrato.

Gli algoritmi simmetrici si basano su alcuni assunti, tra cui il fatto che la chiave segreta sia condivisa tra mittente e destinatario in modo sicuro e che l'algoritmo di crittografia sia invece pubblico e noto quindi anche a potenziali attaccanti.

Nei sistemi a chiave asimmetrica si utilizzano invece due chiavi, diverse ma correlate, una per cifrare (pubblica) e l'altra per decifrare (privata).

Gli algoritmi a chiave pubblica, quale ad esempio RSA o ElGamal, basano la loro efficacia e sicurezza su problemi computazionalmente difficili, quali la scomposizione in fattori primi di numeri di grandi dimensioni.

Essi non richiedono uno scambio iniziale di chiavi segrete come richiesto negli algoritmi simmetrici, in quanto ogni utente genera la propria coppia di chiavi da solo, ma in ogni caso la loro sicurezza non può essere matematicamente provata in quanto la difficoltà nel calcolare la chiave privata a partire da quella pubblica non è stata dimostrata.

In questa tesi vogliamo presentare un nuovo tipo di crittografia, la **crittografia quantistica** che consente di avere un livello di sicurezza arbitrariamente elevato ed assolutamente inviolabile fintanto che si dimostrino valide le leggi della meccanica quantistica e dei principali aspetti di fisica e matematica che riguardano tale argomento.

Caratteristiche e limiti della crittografia

Sicurezza nella Crittografia

Prima di affrontare gli schemi di crittografia quantistica è opportuno ricordare le definizioni di sicurezza dei sistemi di cifratura classici (con classici ci si riferisce a tutti i sistemi, a chiave pubblica e privata, non basati su assunti quantistici).

Uno schema crittografico viene definito come **computazionalmente sicuro** quando soddisfa entrambi i seguenti criteri:

- Il costo necessario a violare il testo cifrato supera il valore delle informazioni crittografate
- Il tempo richiesto per violare il testo cifrato supera la vita utile delle informazioni

In realtà risulta difficile valutare se un algoritmo soddisfa pienamente i due criteri indicati, a causa sia dell'incremento costante della potenza di elaborazione dei calcolatori che rende possibili attacchi a forza bruta in tempi "brevi" rispetto al momento in cui il cifrario è stato pensato o ai parametri utilizzati per implementarlo, sia a causa della costante evoluzione delle tecniche crittanalitiche, che consentono di portare attacchi al testo cifrato da direzioni inaspettate.

In contrapposizione alla definizione precedente uno schema crittografico è invece detto **incondizionatamente sicuro** se, indipendentemente dalla quantità di testo cifrato e dal tempo a disposizione, non è possibile decrittografare il testo in alcun modo a meno di avere la chiave corretta: semplicemente il testo cifrato non contiene alcuna informazione che renda possibile una analisi di qualunque tipo. Le caratteristiche matematiche di un cifrario del genere sono state enunciate da Shannon¹ negli anni '40, in particolare servirà ricordare che l'entropia contenuta in un testo cifrato non può essere maggiore di quella presente nella chiave usata per cifrarlo, da cui si deduce che condizione necessaria (ma non sufficiente) per ottenere una assoluta sicurezza è l'utilizzo di una chiave casuale non riutilizzabile di lunghezza pari al messaggio.

¹ C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28, 1949

One-Time Pad

L'unico cifrario incondizionatamente sicuro attualmente conosciuto è il **One-Time Pad**: tale sistema richiede una chiave casuale non riutilizzabile lunga tanto quanto il messaggio da inviare, ogni bit del testo in chiaro viene messo in XOR con il corrispondente bit della chiave per formare il testo cifrato. Per le proprietà dello XOR, la decrittografia si esegue effettuando la stessa operazione bit a bit tra il testo cifrato e la stessa chiave.

In breve, per la crittografia:

$$c_i = p_i \oplus k_i$$

mentre per la decrittografia:

$$p_i = c_i \oplus k_i$$

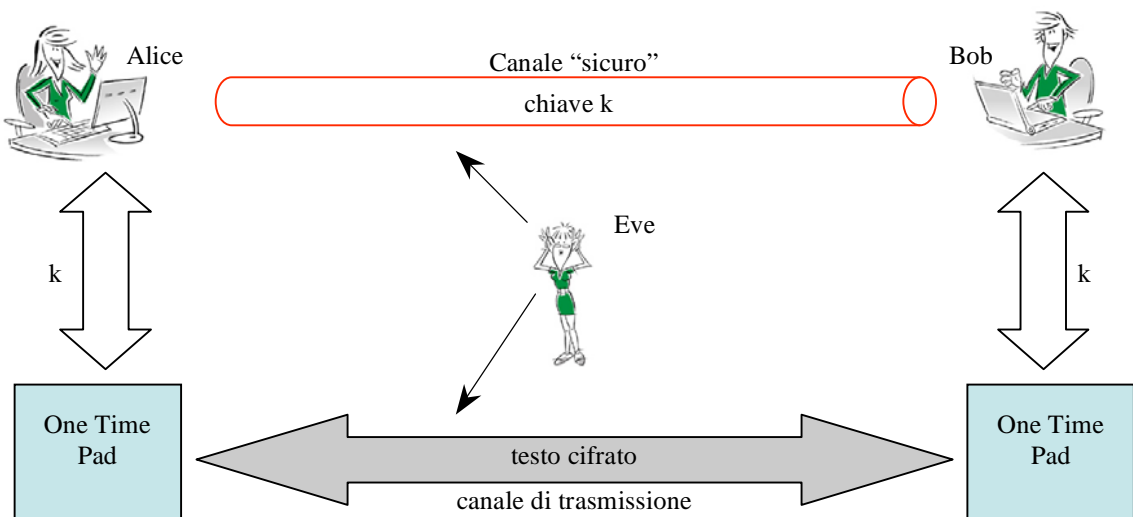
dove

p_i = i-esima cifra binaria del testo in chiaro (plaintext)

c_i = i-esima cifra binaria del testo cifrato (ciphertext)

k_i = i-esima cifra binaria della chiave (key)

\oplus = simbolo dell'operatore di OR esclusivo (XOR)



Questo schema, se la chiave è scelta come una sequenza realmente casuale e non viene mai riutilizzata, è assolutamente inviolabile in quanto produce un testo cifrato che non ha nessuna relazione statistica con il testo in chiaro che lo ha generato e non contiene quindi alcuna informazione sul *plaintext* stesso.

Nonostante l'assoluta inviolabilità di questo procedimento esso non viene praticamente mai adottato nella pratica a causa di un fondamentale problema: se fosse possibile distribuire in modo assolutamente sicuro chiavi di lunghezza arbitraria tra due soggetti ogni volta che questo si renda necessario, lo stesso canale "sicuro" potrebbe essere utilizzato per trasmettere direttamente il messaggio, rendendo superflua la crittografia medesima.

Infatti nella crittografia classica, secondo il principio di Kerckhoffs² un crittosistema dovrebbe rimanere sicuro anche se tutto il sistema, ad eccezione della chiave, è di pubblico dominio: questo implica che è sempre possibile per un attaccante (convenzionalmente chiamato Eve dal termine inglese *eavesdrop* – ascoltare di nascosto) intercettare il canale di comunicazione e quindi ottenere il testo cifrato; da notare che è considerato ammissibile che l'intercettazione sia passiva, ovvero senza interferenza, in modo che mittente e destinatario (chiamati convenzionalmente Alice e Bob) non sappiano se la comunicazione è stata ascoltata o meno da una terza parte non autorizzata.

La distribuzione delle chiavi (*key distribution*) deve essere considerata sicura a priori. Questo può non essere un grave problema se l'algoritmo crittografico prevede l'utilizzo di una chiave una volta per tutte (ad esempio nel DES), infatti in questo caso gli utenti potrebbero spendere molte risorse per avere un buon livello di sicurezza. Se però, come nel one-time pad, ogni messaggio richiede una nuova chiave, i costi di distribuzione delle chiavi sarebbero proibitivi, questo è il motivo per cui tale algoritmo viene usato solo raramente ed in circostanze che richiedono estrema segretezza, ad esempio in comunicazioni diplomatiche.

La domanda di avere una distribuzione delle chiavi con un alto livello di sicurezza ha però due possibili soluzioni, una basata sulla matematica ed una basata sulla fisica: la crittografia a chiave pubblica e la *quantum key distribution*. È importante ricordare che l'approccio a chiave pubblica, sul tipo dello scambio di chiavi Diffie-Hellman³, dipende ancora dalla difficoltà del calcolo di certe funzioni matematiche e quindi, potenzialmente, potrebbe in futuro venire invalidato da nuove scoperte in campo matematico e non solo⁴...

² Auguste Kerckhoffs, "La cryptographie militaire", Journal des sciences militaires, vol. IX, pp. 5–38, Gennaio 1883, pp. 161–191, Febbraio 1883.

³ Una descrizione del protocollo Diffie-Hellman è riportata in appendice

⁴ In appendice si trova una breve introduzione al quantum computing ed al possibile utilizzo di questa tecnologia per "rompere" i più noti cifrari a chiave pubblica.

Crittografia Quantistica

I contributi dati dalla meccanica quantistica alla crittografia sono duplici e di segno opposto.

Da un lato grazie all'introduzione di concetti quali il *quantum computing*, un nuovo paradigma di calcolo in grado teoricamente di effettuare calcoli che oggi hanno una complessità esponenziale in un tempo polinomiale, vengono minati alla base i presupposti di efficacia degli attuali algoritmi crittografici a chiave pubblica.

Dall'altro lato le stesse idee permettono, grazie alle proprietà fisiche delle particelle subatomiche, di costruire dei canali quantistici per la trasmissione dei dati assolutamente sicuri e che hanno inoltre la straordinaria proprietà di permettere la scoperta di eventuali estranei che tentassero di intercettare i dati in essi contenuti.

La crittografia quantistica (*Quantum Cryptography*) fornisce una soluzione al problema di distribuire chiavi segrete, da utilizzare per la cifratura di dati, da trasmettere poi su canali convenzionali, in questo senso è più corretto parlare di *Quantum Key Distribution*, o QKD. Come verrà mostrato più avanti, le leggi della meccanica quantistica applicate alla trasmissione di informazioni sicure garantiscono la rilevazione dell'attività di intercettazione dalle parti attive sul canale, basata su principi fisici e non su assunti computazionali, garantendo a questi schemi la perfetta sicurezza e l'inviolabilità delle comunicazioni.

Per poter utilizzare la QKD le due parti devono condividere un canale di comunicazione quantistico: questo può essere monodirezionale anche se alcune implementazioni prevedono una comunicazione (e quindi un canale) bidirezionale; serviranno quindi delle apparecchiature che consentano di inviare e rilevare le particelle e inoltre Alice e Bob dovranno essersi preventivamente accordati per comunicare su di un canale tradizionale, su cui scambiarsi delle informazioni in chiaro (in seguito verranno precisati meglio questi requisiti).

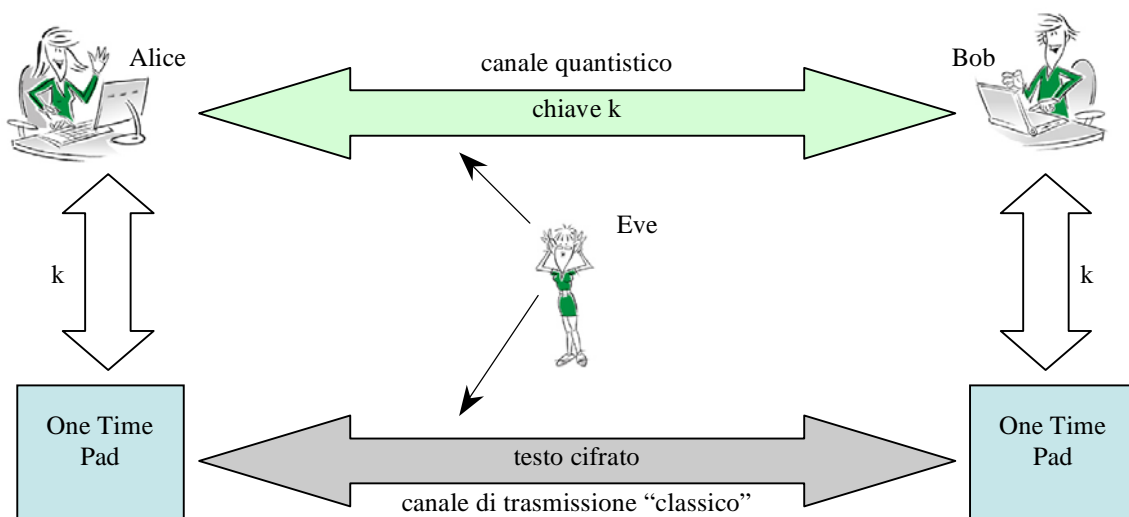
Lo schema di massima della QKD è il seguente:

- Alice e Bob si scambiano fotoni sulla fibra ottica che li collega direttamente.
- Dopo di che si scambiano alcune informazioni sul canale classico.
- Alla fine di questo processo essi si trovano a condividere una chiave segreta di lunghezza arbitraria che non può essere stata intercettata da Eve oppure, se Eve stessa fosse riuscita ad avere anche solo una parte della chiave, Alice e Bob sanno che questo è avvenuto e quindi "buttano" la chiave e ne trasmettono una nuova.

Si assume che l'attaccante Eve abbia le seguenti opzioni:

- Fare tutto ciò che le è fisicamente concesso sul canale quantistico.
- Intercettare passivamente il contenuto del canale tradizionale (vengono escluse in questa fase le possibilità di interruzione della comunicazione e di alterazione del contenuto del messaggio).

È fondamentale notare alcuni aspetti dello schema precedente: è possibile che Eve intercetti la chiave segreta, ma Alice e Bob hanno la certezza di avere questa informazione e possono prendere quindi adeguate contromisure; il protocollo non può essere usato per scambiarsi direttamente dati, ma solo chiavi poiché solo *dopo* la trasmissione si può sapere se questa è stata intercettata o meno: se la chiave è compromessa se ne può generare e trasmettere una nuova mentre sarebbe un problema se ad essere acquisiti fossero i dati.



Le modalità attraverso cui è possibile effettuare questo tipo di scambio di informazioni sicure è l'argomento di questo lavoro.

Introduzione alla fisica classica

Nella meccanica classica la posizione di un punto o di una particella è descritta da un vettore $\mathbf{x}=\mathbf{x}(t)$ che indica le sue coordinate in un sistema di riferimento dato, in funzione del tempo t tale che soddisfi un sistema di equazioni differenziali, le *equazioni del moto*.

Un classico problema fisico consiste nel determinare il moto del punto, ovvero la funzione $\mathbf{x}(t)$, una volta noto il suo valore e quello di alcune sue derivate nell'*istante iniziale* $t = t_0$.

Le equazioni del moto hanno, in condizioni normali, una e una sola soluzione che verifichi le condizioni iniziali. Questo significa che il moto della particella, ovvero la sua posizione e la sua velocità in ogni istante, sono determinabili dalle informazioni che abbiamo sulla particella stessa in un dato istante. Per questo motivo si dice che la meccanica classica è *deterministica*: tutto, nel suo ambito, viene *univocamente determinato* dalle condizioni iniziali. Questo modello, valido per tutti i sistemi macroscopici, non funziona nei sistemi molto piccoli, ad esempio per le particelle elementari, che sono invece governate da leggi di natura probabilistica.

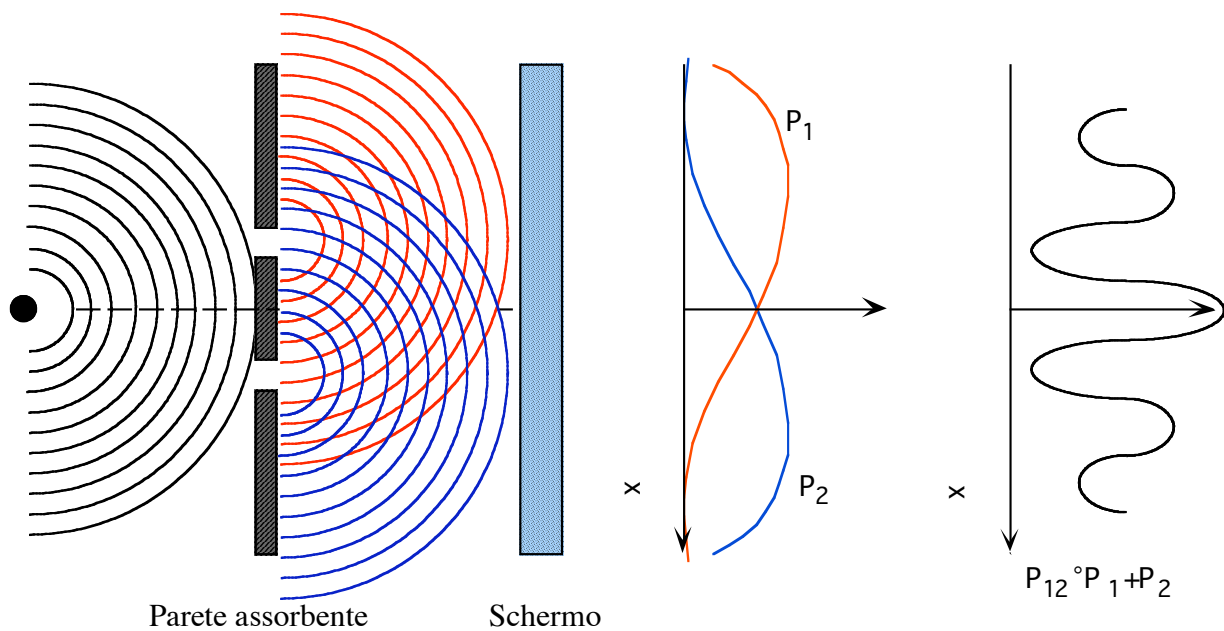
Questo è l'oggetto della fisica quantistica.

La natura della luce, l'esperimento di Young e le teorie successive

Alla fine del XVIII secolo era in corso tra gli scienziati un dibattito sulla natura della luce: ci si chiedeva in particolare se la luce avesse natura ondulatoria o se fosse piuttosto composta di minuscole particelle. Per i sostenitori della teoria delle particelle la luce sarebbe stata composta da un flusso di piccolissimi elementi che avrebbero attraversato lo spazio in linea retta, colpendo gli oggetti e "illuminandoli", mentre secondo la teoria ondulatoria la luce sarebbe stata trasportata come un'onda, in analogia ad esempio alle onde che si formano sulla superficie di uno stagno quando vi si getta un sasso.

La questione venne risolta a favore della teoria ondulatoria nel 1803 dal fisico Thomas Young che dimostrò, facendo passare un fascio luminoso attraverso uno schermo sul quale era stata praticata una fenditura molto sottile, che questo usciva dalla fenditura formando delle figure di diffrazione tipiche delle onde. Questo primo esperimento, pur interessante, venne contestato dai sostenitori della teoria corpuscolare, il cui esponente più autorevole era certamente Newton, in quanto esso

avrebbe potuto essere interpretato come il risultato di “urti” delle particelle luminose con i bordi della fenditura, con conseguente deviazione dall’asse di propagazione originale. La variante più nota dell’esperimento, che eliminò anche i dubbi degli scettici circa la natura della luce, richiedeva che il fascio passasse contemporaneamente attraverso due fenditure vicine: questa configurazione permetteva di osservare, oltre alla diffrazione, anche delle figure di interferenza in cui le onde



luminose si rafforzavano o annullavano a vicenda in un modo incompatibile con le ipotesi corpuscolari.

Sessanta anni dopo, nel 1864, Maxwell dimostrò che sono i campi elettrico e magnetico a propagarsi nello spazio, dando un fondamento matematico agli esperimenti di Young e fornendo delle prova alla teoria che considera la luce come un’onda elettromagnetica.

Un ulteriore, fondamentale, passo avanti nella spiegazione della natura della luce arrivò in articolo del 1905 *Un punto di vista euristico sulla creazione e assorbimento della luce*, in cui Einstein postulò l’esistenza dei quanti di luce. L’idea era che l’energia delle onde elettromagnetiche descritte da Maxwell non fosse distribuita con continuità nello spazio, ma piuttosto che essa fosse il multiplo di una quantità discreta. A questo quanto di energia venne dato il nome di **fotone** (dal greco φως "phos", che significa *Luce*), una particella indivisibile, di massa e carica nulle.

Einstein mostrò come i processi che prevedono lo scambio di energia tra radiazione e materia fossero compatibili con questa nuova teoria e gli esperimenti successivi sull’effetto fotoelettrico

– il fenomeno in cui delle superfici metalliche colpite da onde elettromagnetiche emettono degli elettroni – confermarono l'ipotesi dell'esistenza dei quanti di luce, tanto da fruttargli l'assegnazione del premio Nobel nel 1921.

Nonostante l'apparente contraddizione, per Einstein l'esistenza dei quanti non era in contrasto con le teorie espresse da Maxwell, che rimasero un punto di riferimento anche per le ricerche successive, quando le energie da analizzare erano notevolmente maggiori di quelle di un singolo quanto. Infatti, analogamente ad un gas che ha un comportamento semplice e "continuo" nonostante sia composto da un numero elevatissimo di atomi che si muovono in modo caotico ed irregolare, un tipico fascio luminoso risulta composto da un numero di fotoni tanto elevato da avere l'apparenza di una distribuzione continua di energia.

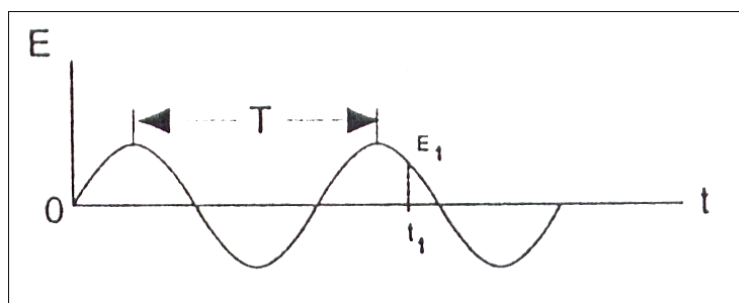
Alcune osservazioni sulla fisica classica

Al fine di rendere più chiari i concetti che verranno esposti in seguito, in particolare le proprietà di polarizzazione delle onde elettromagnetiche (e quindi anche della luce) si procederà ad illustrare alcuni richiami di fisica. Le osservazioni che verranno esposte, in particolare sulle proprietà di filtri e cristalli, sono valide fino a quando vengono presi in considerazione fasci di luce abbastanza intensi da permettere di adottare il punto di vista classico, che prevede che la radiazione sia distribuita uniformemente nello spazio.

Si supponga di avere una carica elettrica che si muove di moto periodico lungo un segmento. Tale carica irraggerà onde elettromagnetiche nello spazio circostante caratterizzate dalla stessa frequenza con cui oscilla.

Un'onda elettromagnetica consiste di due vettori di campo, perpendicolari tra loro e rispetto alla direzione di propagazione dell'onda. Questi due vettori rappresentano rispettivamente il campo magnetico **H** e quello elettrico **E**. La velocità di propagazione nel vuoto di onde di questo tipo è di circa 300.000 Km/s e viene indicata convenzionalmente con c (velocità della luce).

Con riferimento al campo elettrico, esso può essere studiato osservando l'evoluzione della sua intensità, direzione e verso nel tempo, in un certo punto dello spazio, ottenendo un grafico sinusoidale come il seguente



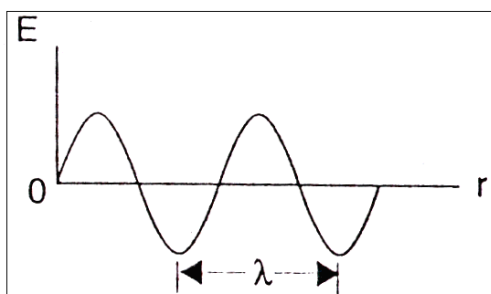
il tempo T che intercorre tra due punti di massimo è il periodo di oscillazione, ed è lo stesso della carica che genera il campo.

L'esempio mostrato in figura illustra un caso molto semplice, in cui la frequenza è costante (ovvero che, nel caso di una radiazione luminosa, si abbia un colore puro) e che oscilli in un piano ben definito, cioè che abbia una precisa e definita polarizzazione piana – concetto che verrà chiarito più avanti. Nella realtà il campo può variare in modo arbitrario nello spazio e nel tempo, in orientamento ed ampiezza, fermo restando il vincolo di perpendicolarità rispetto alla direzione di propagazione dell'onda.

L'inverso del periodo T è la frequenza dell'onda:

$$\nu = \frac{1}{T}$$

che indica il numero di oscillazioni al secondo del campo.



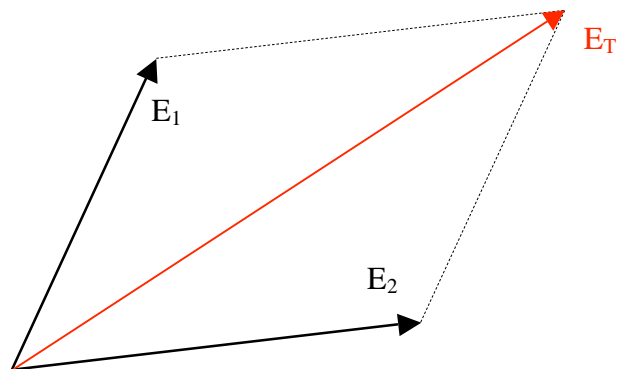
La velocità di un'onda si può allora esprimere come il prodotto tra la distanza λ coperta in un periodo per il numero di oscillazioni al secondo (la frequenza). La relazione tra lunghezza d'onda, frequenza e velocità della luce si può allora esprimere come:

$$\lambda \nu = c$$

Il punto fondamentale di questo tipo di processi ondulatori è la linearità delle equazioni che li descrivono, ovvero la possibilità di combinare linearmente più campi presenti nella stessa regione di spazio, secondo la nota regola del parallelogramma.

Se ad esempio in punto dello spazio, in un certo istante, sono presenti due campi elettrici $E_1(r,t)$ ed $E_2(r,t)$, i loro effetti si sommano vettorialmente per ottenere un nuovo campo

$$E_T = E_1(r,t) + E_2(r,t).$$



Per comprendere alcuni fenomeni che verranno illustrati in seguito, è opportuno precisare che risulta inoltre sempre possibile decomporre un vettore campo elettrico in due componenti tra loro ortogonali.

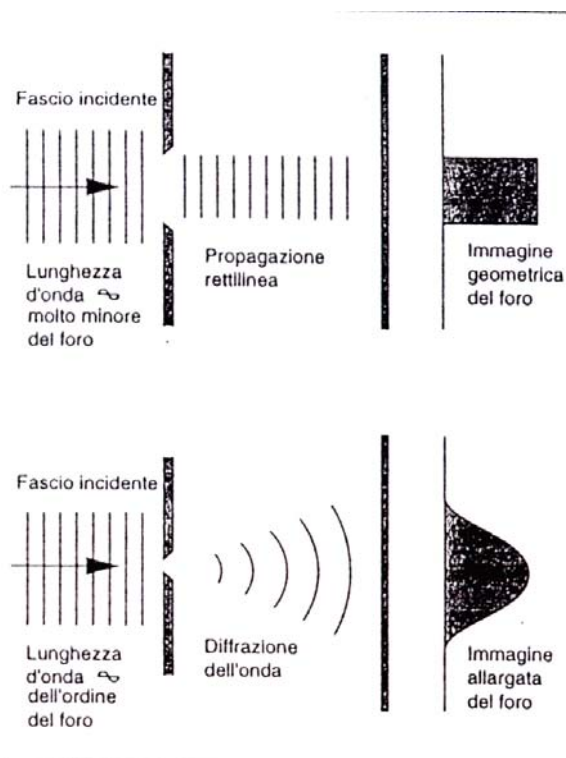
Si osservano in natura dei fenomeni ondulatori, quali la **diffrazione** e l'**interferenza**.

La diffrazione è il fenomeno che vede un'onda aggirare gli ostacoli, poiché ogni punto della perturbazione ondosa diventa a sua volta origine di nuove onde (principio di Huygens).

L'interferenza è un effetto prodotto dalla sovrapposizione di due o più treni d'onde che si propagano simultaneamente in una stessa regione dello spazio. Si hanno due possibili tipi di interferenza: costruttiva quando le onde si rafforzano reciprocamente e distruttiva quando invece si elidono a vicenda.

Questi fenomeni sono strettamente legati al rapporto tra la lunghezza d'onda e le dimensioni degli ostacoli che l'onda stessa incontra durante la sua propagazione. Per mostrare come cambi il comportamento delle onde al variare di tale rapporto si farà riferimento ai fenomeni luminosi ed alla formazione delle ombre.

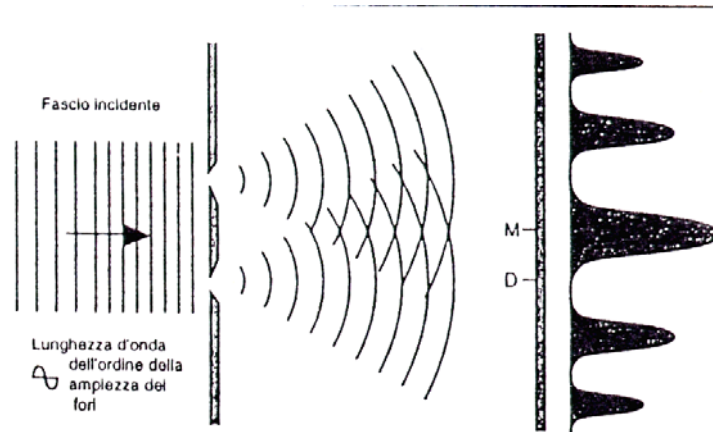
Si ipotizzi di illuminare uno schermo su cui è stato praticato un foro:



se il foro è molto più grande della lunghezza d'onda, allora la luce seguirà le leggi dell'ottica geometrica: le traiettorie dei raggi luminosi saranno rettilinee.

Se invece il foro ha dimensioni dello stesso ordine di grandezza della lunghezza d'onda, si osservano dei fenomeni di diffrazione, l'ombra si allarga.

Per illustrare il fenomeno dell'interferenza, sullo schermo verranno praticati due fori:



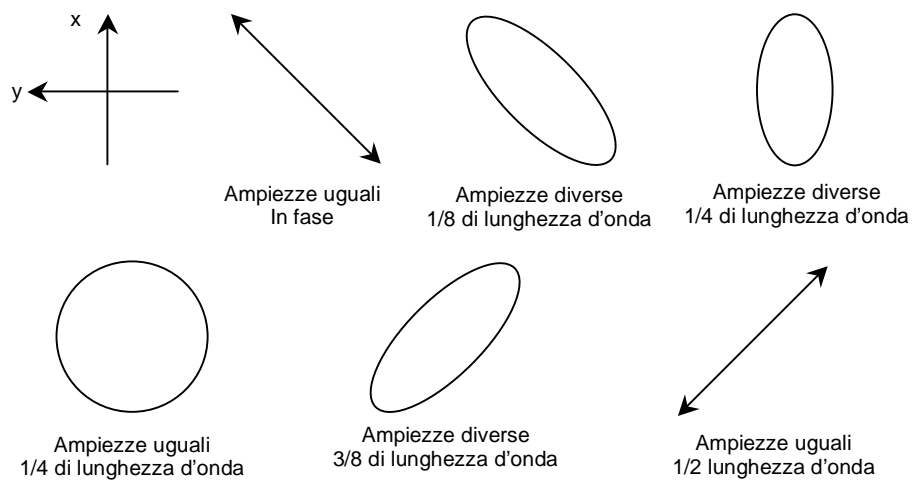
Nota: si tratta proprio degli esperimenti di Young.

Le onde che si formano interferiscono fra di loro nella regione dello schermo. In alcuni punti esse si rafforzano, in altre si sottraggono fino ad annullarsi.

Sommando, sempre secondo la regola del parallelogramma, campi che sono orientati in modo diverso nello spazio o con differenze di fase si possono ottenere tre tipologie di stati di polarizzazione:

- Piano, nel caso in cui si combinino tra loro due campi ortogonali, uguali in fase ed ampiezza, oppure con una differenza di fase pari a mezza lunghezza d'onda.
- Circolare, se l'estremo del vettore, visto da un osservatore verso cui si propaga l'onda, descriva nel tempo una circonferenza in senso orario o antiorario. Questo accade quando i due campi sono tra loro ortogonali, hanno uguale ampiezza ma sono sfasati di un quarto di lunghezza d'onda.
- Ellittico, in cui il vettore E, osservato in un dato punto, nel tempo descrive una ellisse; questo accade nel caso in cui i due campi abbiano ampiezze diverse, anche in questo caso si distingue tra polarizzazione ellittica destrorsa o sinistrorsa.

La figura mostra la visione frontale dei vari tipi di campi ottenibili variando ampiezza e lunghezza d'onda di due vettori (orizzontale e verticale), il verso di avanzamento si suppone uscente dal foglio.

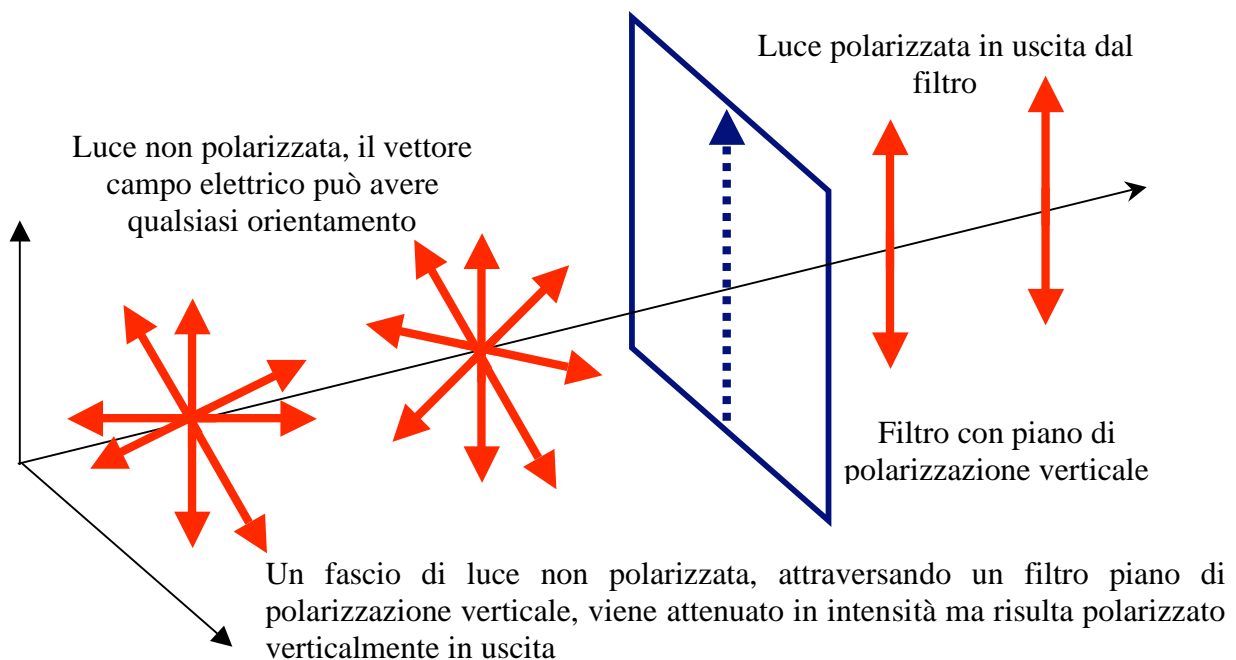


Per motivi connessi ai meccanismi di funzionamento della crittografia quantistica, si utilizzeranno esclusivamente gli stati di polarizzazione lineare e circolare. Si menziona inoltre anche il caso in cui il vettore E, in un dato punto, varia nel tempo in tutte le direzioni, mantenendosi perpendicolare alla direzione di propagazione, in tal caso si parla di onda non polarizzata.

Filtri Polarizzatori

Osservando nello specifico i fenomeni luminosi si nota come la maggior parte delle sorgenti di luce, come il sole, una sbarra di metallo incandescente o il filamento di una lampadina, emettono radiazioni che variano continuamente in frequenza, fase, ampiezza e polarizzazione. Il motivo per cui questo avviene è semplicemente dovuto al fatto che le sorgenti (atomi e molecole) di tali emissioni, che contribuiscono a formare l'onda luminosa, sono moltissime ed indipendenti tra loro e quindi il campo risultante dalla somma vettoriale di tutte le singole emissioni varia in modo imprevedibile da punto a punto e da istante a istante: in particolare si rileva che tale campo non possiede uno stato di polarizzazione definito.

È tuttavia possibile polarizzare un fascio luminoso utilizzando un filtro polarizzatore, ovvero un materiale che può essere attraversato solo dalle radiazioni che hanno una precisa polarizzazione piana. L'esempio più semplice di filtro di questo tipo è rappresentato dal film polaroid, una sottile lastra di materiale plastico usata anche per la realizzazione delle lenti degli occhiali da sole.



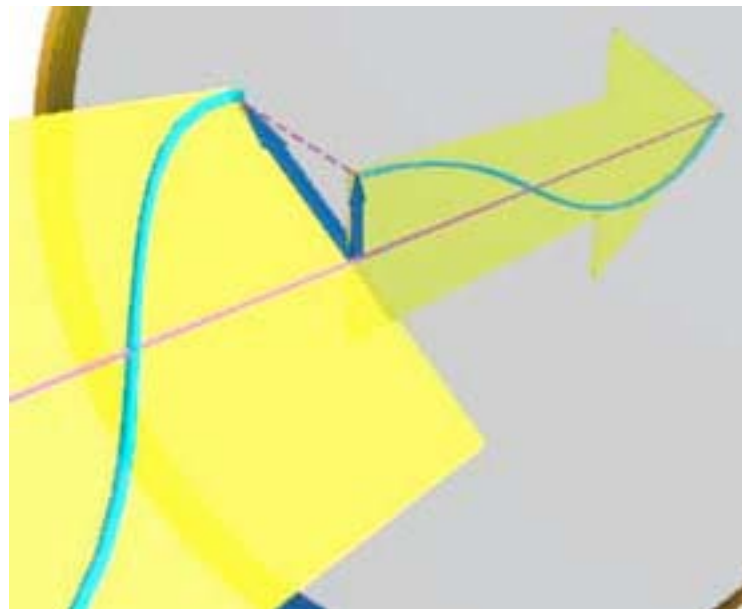
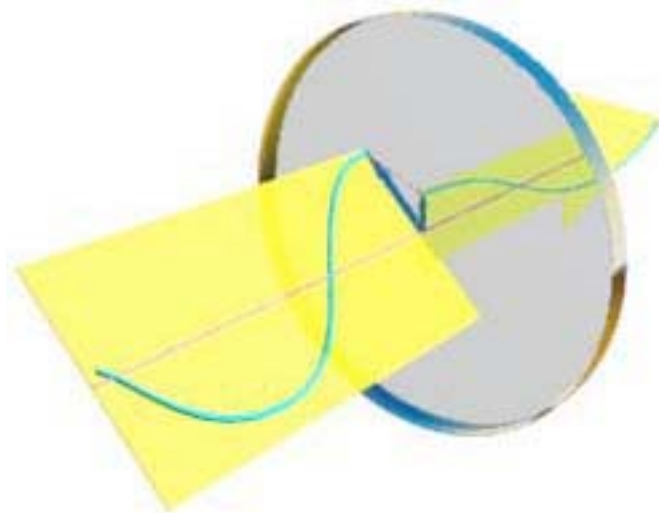
Nell'immagine si vede un fascio luminoso non polarizzato che attraversa un filtro polaroid orientato verticalmente: in uscita passa solo una frazione della luce incidente, ma questa risulta polarizzata secondo l'orientamento del filtro.

Si supponga adesso di disporre di un fascio di luce già polarizzato (ad esempio verticalmente) e di farlo passare attraverso un altro filtro polaroid. Facendo ruotare il filtro si osserverà come l'intensità della luce⁵ che lo attraversa vari in funzione dell'orientamento: il massimo di trasmissione si avrà quando il piano caratteristico del filtro coincide con la polarizzazione del fascio luminoso in ingresso (verticale, nell'esempio) mentre il massimo dell'assorbimento della luce, ovvero il buio totale, si otterrà quando il piano del filtro sarà perpendicolare a quello di polarizzazione della luce (orizzontale in questo caso). Nelle angolazioni intermedie l'intensità luminosa risulterà attenuata secondo modalità che sono espresse dalla legge di Malus, che lega l'intensità luminosa trasmessa I_T a quella incidente I_0 secondo la formula:

$$I_T = I_0 \cos^2 \theta$$

in cui θ rappresenta l'angolo tra il piano di polarizzazione che caratterizza la luce incidente ed il filtro.

⁵ L'intensità luminosa è proporzionale al quadrato del campo

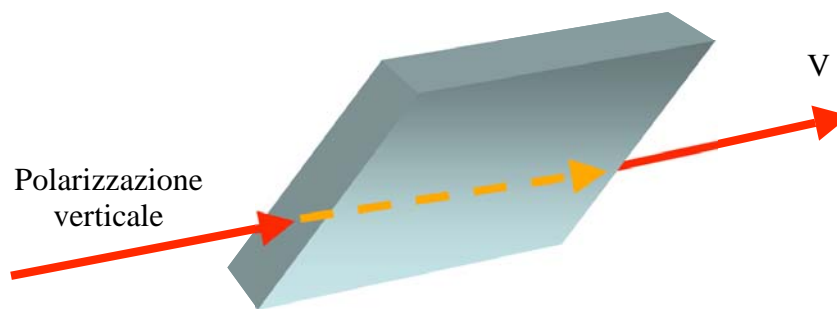


La legge di Malus appena enunciata può essere spiegata in base alle osservazioni fatte precedentemente sulla natura vettoriale dei campi: la scomposizione di un campo a polarizzazione piana lungo due assi ortogonali, secondo la regola del parallelogramma, viene combinata con il fatto che un filtro polarizzatore consente il passaggio solo alla componente parallela al suo piano di polarizzazione e con l'osservazione che l'intensità luminosa dipende dal quadrato del campo.

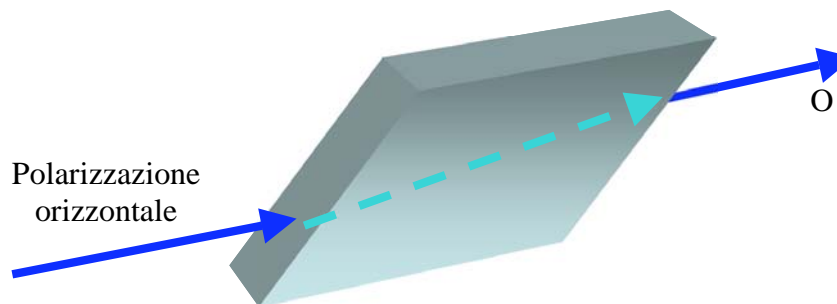
Cristalli Birifrangenti

Un'altra classe di materiali che hanno la capacità di influenzare la propagazione della luce al loro interno è costituita dai cristalli birifrangenti. Questi oggetti, come i filtri polaroid, hanno una struttura *otticamente anisotropa*, ovvero reagiscono in modo differente a seconda della direzione e polarizzazione della luce incidente. Un esempio di materiale di questo tipo è costituito da cristalli di calcite opportunamente tagliati rispetto i loro piani reticolari.

Inviando un raggio luminoso ad un cristallo birifrangente, si osserva un comportamento peculiare: se il raggio è polarizzato verticalmente esso attraversa il cristallo senza subire variazioni;

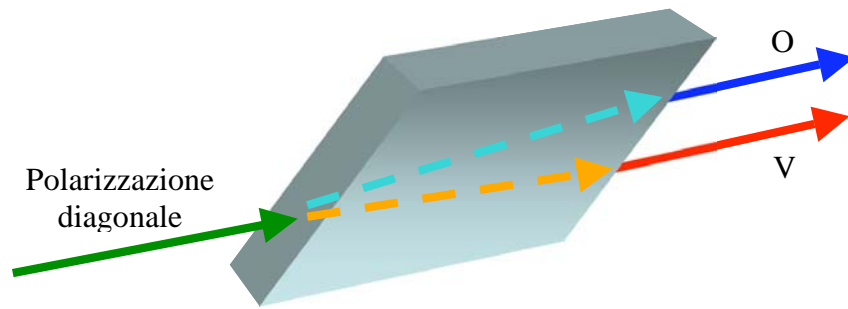


se invece esso è polarizzato orizzontalmente, viene deflesso verso l'alto all'interno del cristallo ed esce dall'altro lato con un ulteriore cambiamento di direzione che lo riporta ad essere parallelo al raggio incidente ma spostato di una quantità proporzionale allo spessore del cristallo.



In entrambi i casi i raggi luminosi mantengono il loro piano di polarizzazione originale.

Particolarmente interessante si rivela il caso in cui il raggio incidente abbia ancora una polarizzazione piana che non sia né verticale né orizzontale ma, ad esempio, diagonale a 45° . In questo caso il raggio si divide in due parti (nello specifico di uguale intensità) caratterizzate da avere rispettivamente polarizzazione verticale (indeflesso, detto raggio ordinario) e polarizzazione orizzontale (deflesso, detto raggio straordinario).



A differenza dei filtri polarizzatori quindi i cristalli birifrangenti non assorbono una parte del fascio che li attraversa, ma lo scompongono nelle due componenti orizzontale e verticale (che risulteranno attenuate in proporzione all'angolo di polarizzazione del fascio incidente).

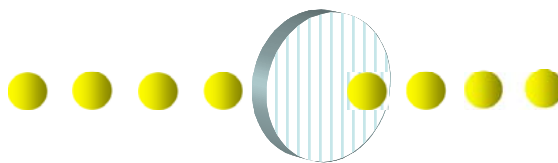
Introduzione alla fisica quantistica

Nella parte precedente si sono riportate alcune considerazioni sulle onde elettromagnetiche, analizzate esclusivamente dal punto di vista classico. In questo paragrafo si analizzeranno gli stessi fenomeni, tenendo conto anche della natura corpuscolare della radiazione, che deve essere quindi assimilata ad un flusso di particelle: i fotoni.

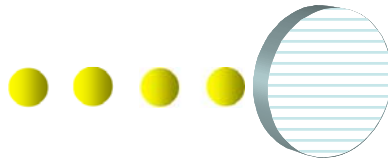
Si consideri un fascio di luce monocromatico di frequenza ν e polarizzato, ad esempio verticalmente, e si supponga di dirigerlo verso un filtro il cui piano di polarizzazione non coincida con quello del fascio: l'intensità luminosa in uscita dal filtro risulterà attenuata rispetto a quella in ingresso. Si supponga inoltre che il fascio sia talmente debole da fare in modo che l'energia che investe il filtro in un certo intervallo di tempo, ad esempio un secondo, sia esattamente pari a quella di un quanto, ovvero $h\nu$ (ove h è la costante di Planck), in altri termini possiamo affermare che un singolo fotone raggiunge il filtro ogni secondo. Allora, poiché per la legge di Malus l'energia in uscita risulta ridotta di un fattore pari a $\cos^2\theta$ rispetto all'energia incidente e poiché un fotone è indivisibile, l'unica spiegazione all'attenuazione dell'intensità in uscita è che alcuni fotoni vengano fermati dal filtro mentre altri lo attraversano indisturbati e che la frazione di quelli bloccati sia esattamente proporzionale a quanto mostrato dalla legge di Malus.

Nelle immagini seguenti vengono esemplificati i comportamenti di una sequenza di fotoni singoli polarizzati verticalmente che vengono inviati verso filtri con diversi piani di polarizzazione.

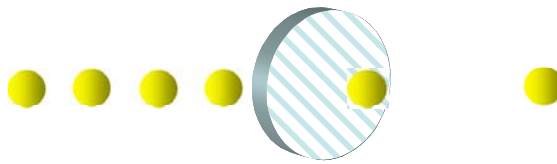
Se anche il filtro è orientato verticalmente, tutti i fotoni incidenti vengono rilevati anche dopo il filtro.



Se il filtro è orientato orizzontalmente, tutti i fotoni incidenti vengono bloccati e nessuno viene rilevato dopo il filtro.

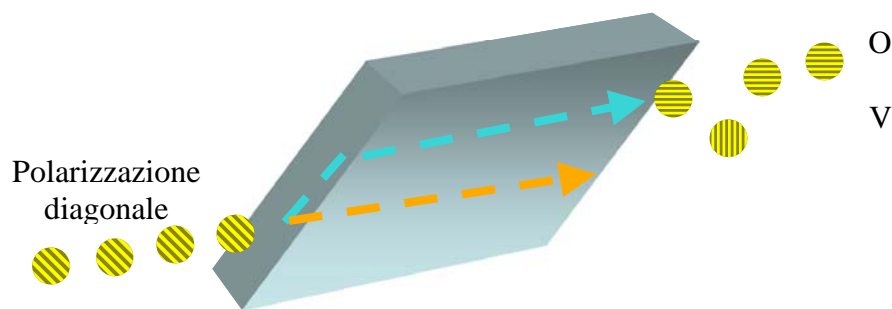


Se il filtro ha un orientamento di 45° , allora la metà dei fotoni, a caso, lo attraversa e viene rilevato mentre l'altra metà viene bloccata.



Questo ultimo caso riveste particolare importanza ai fini della trattazione successiva della crittografia quantistica e quindi risulta importante precisarne ulteriormente due aspetti: il primo riguarda il fatto che un evento quantistico (e quindi microscopico) possa venire amplificato fino a renderlo percepibile a livello macroscopico. Il secondo punto riguarda la genuina casualità dell'evento "la metà dei fotoni attraversa il filtro", alcuni fenomeni quantistici sono intrinsecamente aleatori: non è possibile stabilire a priori se l'evento "attraversamento del filtro" si verificherà o meno. Tra l'altro, se si accetta che la teoria quantistica sia corretta e completa, è letteralmente sbagliato pensare che, sia pure in un modo sconosciuto, i singoli fotoni possiedano, prima di attraversare il filtro, una qualche caratteristica peculiare che consenta loro di superare il filtraggio o meno.

Un fenomeno analogo si osserva sostituendo ai filtri i cristalli birifrangenti:

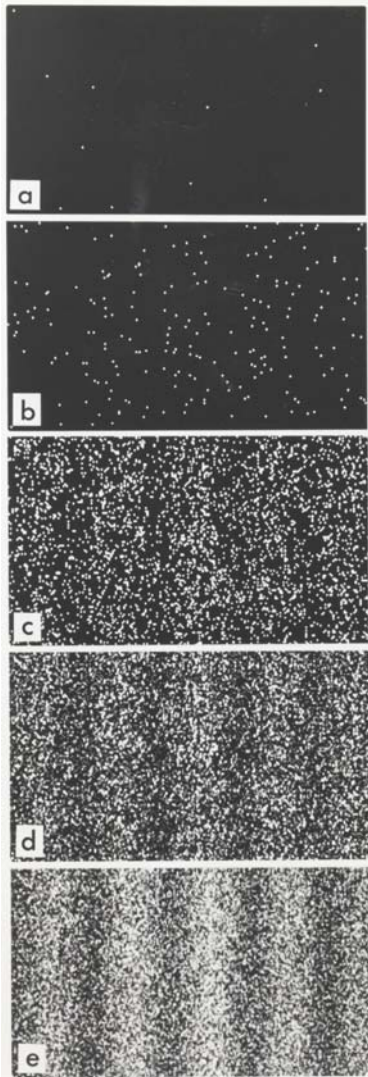


Ogni fotone andrà ad attivare un rivelatore posto lungo il cammino ordinario o straordinario, la traiettoria indeflessa verrà rilevata con una probabilità di $\cos^2\phi$ mentre il cammino straordinario sarà rilevato nei casi rimanenti, ovvero con una probabilità pari a $(1 - \cos^2\phi)$. Anche stavolta, se

la teoria è ritenuta vera e completa, non risulta lecito pensare che i fotoni abbiano qualche proprietà individuale che determinerà il loro percorso nell'attraversamento del cristallo.

Anche i fenomeni di diffrazione ed interferenza devono essere reinterpretati dal punto di vista quantistico: la figura a campana tipica della diffrazione si forma solo grazie all'apporto di molti fotoni, ognuno di essi colpisce il rivelatore in un punto preciso e la densità risulterà maggiore in quella regione dove un maggior numero di essi va ad incidere, sempre secondo principi probabilistici.

L'interferenza deve essere rivista come una distribuzione probabilistica di fotoni: le aree in cui l'intensità luminosa risulta più elevata sono quelle in cui il maggior numero di fotoni raggiungono lo schermo, mentre le zone in cui il campo elettrico è nullo, le cosiddette zone di interferenza negativa, sono quelle che le particelle non raggiungono mai.



Un aspetto particolarmente significativo del fenomeno dell'interferenza visto dal punto di vista quantistico è dato dal fatto che il formarsi della tipica figura "ad onde" non è da interpretarsi come il risultato di una serie di urti tra fotoni ma come manifestazione di proprietà che i fotoni stessi possiedono, indipendentemente gli uni dagli altri: un esperimento in cui un solo fotone alla volta viene emesso, inviato verso uno schermo su cui sono state praticate due fenditure ed infine rilevato su una lastra fotografica evidenzia come la figura di interferenza si formi quale contributo di molte particelle che agiscono in modo indipendente, senza alcuna correlazione tra loro. Questo comportamento decisamente controintuitivo è stato verificato anche con particelle diverse dai fotoni e dotate di massa e carica elettrica, quali ad esempio gli elettroni.

Nell'immagine a lato, risultato di un'esperimento condotto da Tanamura, si osserva l'evoluzione nel tempo di tale esperimento e di come i singoli fotoni sembrano disporsi casualmente sulla lastra ma anche come, al crescere del numero di fotoni registrati, l'immagine assuma sempre più i contorni delle onde tipiche dell'interferenza. Il numero dei fotoni è di 10 (a), 200 (b), 6000 (c), 40000 (d), 140000 (e).

La notazione di Dirac (o notazione bra-ket)

Viene introdotta adesso una notazione dovuta a Dirac, che verrà usata estesamente nel seguito, efficace per rappresentare gli stati di un sistema quantistico. Quando lo stato del sistema corrisponde ad una definita proprietà, si userà per indicarlo il simbolo $|\dots\rangle$ che rappresenta il vettore di stato del sistema, mettendo al posto dei puntini una lettera, un simbolo o una breve frase che specifichi la proprietà posseduta dal sistema. La polarizzazione di un fotone sarà rappresentata in questa notazione come $|\updownarrow\rangle$ o $|V\rangle$ se verticale, con $|\leftrightarrow\rangle$ o $|O\rangle$ se orizzontale mentre gli stati di polarizzazione diagonali saranno rappresentati con $|D\rangle$ o, più specificamente con i simboli $|\nearrow\rangle, |\searrow\rangle, |45\rangle, |135\rangle$.

Il principio di sovrapposizione.

Gli stati di polarizzazione si possono combinare linearmente, ovvero moltiplicare per un numero e poi sommare tra loro, ottenendo come risultato un nuovo stato. La prima conseguenza di questo è la possibilità di definire un certo stato di polarizzazione (in termini di ampiezza di probabilità) in una base.

Ad esempio la combinazione lineare di uno stato $|\updownarrow\rangle$ con uno $|\leftrightarrow\rangle$ fornisce come risultato uno stato $|\nearrow\rangle$, nello specifico:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\updownarrow\rangle + \frac{1}{\sqrt{2}}|\leftrightarrow\rangle$$

Esprimendo questo concetto in termini più formali, lo stato di polarizzazione è definito come un vettore in uno spazio di Hilbert (uno spazio vettoriale bidimensionale complesso, su cui è definita una operazione di prodotto interno). Gli elementi di una base ortonormale in questo spazio sono indicati con $|0\rangle$ e $|1\rangle$ ed un vettore normalizzato può quindi essere rappresentato come

$$|Y\rangle = a|0\rangle + b|1\rangle, \text{ con } |a|^2 + |b|^2 = 1$$

dove $a, b \in \mathbf{C}$. Questa notazione non significa che il valore dello stato di polarizzazione assume un valore compreso tra 0 e 1 ma piuttosto che esso si trova in una sovrapposizione coerente di entrambi gli stati e che, misurando $|Y\rangle$ si ottiene un risultato non deterministico: la probabilità di

ottenere il risultato $|0\rangle$ è pari ad $|a|^2$, mentre la probabilità di ottenere $|1\rangle$ è $|b|^2$. Naturalmente la somma delle probabilità individuali dei due eventi mutuamente esclusivi è 1, in accordo con il fatto che essi sono gli unici eventi che è possibile osservare.

La notazione di Dirac consente di definire completamente lo stato di una particella e la teoria prevede che per la particella stessa non sia possibile alcuna ulteriore specificazione circa lo stato. La natura genuinamente casuale dei processi quantistici è quindi implicata, oltre che dalle evidenze sperimentali, dall'assunzione che la teoria sia completa, ovvero che la specificazione del vettore di stato rappresenti l'informazione più completa (in teoria, non solo in pratica) su un dato sistema fisico e quindi che non sia possibile conoscere nulla oltre al vettore stesso. Una volta specificato il vettore di stato è possibile calcolare le probabilità che un fotone superi un test di polarizzazione, ma questa informazione è l'unica cosa che è possibile conoscere circa il processo di misura stesso.

L'entanglement quantistico

Il fenomeno dell' *entanglement* (o correlazione quantistica), privo di un equivalente nella fisica classica, si ha quando ogni stato quantico di un insieme di due o più sistemi fisici dipende dagli stati di ciascuno dei sistemi che compongono l'insieme, anche se essi sono separati spazialmente. In particolare, è possibile preparare un sistema costituito da una coppia di particelle tali che, anche senza necessità di misurazione, si sappia che esse hanno un valore "opposto" di una certa proprietà osservabile, (ad esempio la polarizzazione di due fotoni $|\uparrow\rangle_e|\leftrightarrow\rangle$): anche allontanando indefinitamente tra loro le due particelle esse manterranno questa relazione e pertanto, quando si effettui la misurazione della polarizzazione su di una di esse in una base arbitraria, anche la funzione d'onda dell'altra particella collasserà in un valore preciso in modo che sia conservata la relazione. Per illustrare il concetto di *entanglement* in termini più formali, si immagini un sistema composto da due fotoni, indicati dai numeri 1 e 2: nel caso in cui entrambi siano polarizzati orizzontalmente un tale sistema sarà associato allo stato $|\Phi\rangle = |1, \leftrightarrow\rangle|2, \leftrightarrow\rangle$ mentre se si assume che entrambi siano polarizzati verticalmente lo stato del sistema sarà $|\Lambda\rangle = |1, \uparrow\rangle|2, \uparrow\rangle$. Per quanto visto nei paragrafi precedenti risulta chiaro pensare a quali saranno gli esiti di eventuali misurazioni di queste particelle, in particolare si noti che in entrambi i casi i fotoni avranno probabilità 1/2 di passare un test di polarizzazione diagonale a 45° mentre dei test nelle basi orizzontali o verticali avranno un esito certo.

Per il principio di sovrapposizione risulta però possibile anche un altro stato che sia la combinazione lineare dei precedenti, ovvero:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\leftrightarrow\rangle) = \frac{1}{\sqrt{2}}|1, \uparrow\rangle|2, \uparrow\rangle + \frac{1}{\sqrt{2}}|1, \leftrightarrow\rangle|2, \leftrightarrow\rangle$$

Nello stato $|\Psi\rangle$ nessuno dei due fotoni ha la proprietà di essere polarizzato verticalmente o orizzontalmente in quanto la probabilità di superare un test di polarizzazione (verticale o orizzontale) è pari al quadrato del coefficiente dello stato in cui si trova e tale valore è di 1/2 per entrambi i fotoni, in entrambe le basi. Sviluppando i calcoli necessari a stabilire le probabilità di superare un test di polarizzazione diagonale (45° o 135°) si ottiene ancora una probabilità di 1/2 e lo stesso avviene per qualsiasi base, scelta arbitrariamente. La prima implicazione dell'*entanglement* è quindi che i singoli costituenti dello stato non possiedono più alcuna proprietà individuale, in quanto non esiste alcuna proprietà osservabile di polarizzazione per nessuno di essi di cui possa prevedersi il risultato con certezza. Misurando però uno solo dei fotoni lungo una direzione arbitraria si ottiene che se esso supera il test anche l'altro, che prima non aveva alcuna proprietà di polarizzazione, risulta polarizzato lungo la stessa direzione del primo. Analogamente se il primo fotone non supera il test, l'altro risulterà polarizzato nella direzione perpendicolare.

Riassumendo: prima della misurazione nessuno degli elementi *entangled* che compongono lo stato composto ha una specifica proprietà osservabile, misurando un elemento si ottiene che anche l'altro "acquisisce" istantaneamente una proprietà.

Il paradosso EPR

Il punto centrale del fenomeno dell'*entanglement* è che la teoria quantistica prevede che l'interazione tra le due particelle avvenga istantaneamente, qualunque sia la distanza che le separa. Questa sorta di azione istantanea a distanza è stata per lungo tempo fonte di imbarazzo per gli scienziati in quanto sembra violare i principi della teoria della relatività, in particolare il cosiddetto "principio di località" per cui ciò che avviene nel luogo *A* non può avere alcuna relazione con quanto accade nel luogo *B* se *A* e *B* sono separati da una distanza *l* tale che $l > c\Delta t$ (eventi oltre il cono di luce) ed il "principio di causalità" secondo il quale nessuna trasformazione relativistica può capovolgere la relazione tra causa ed effetto (ovviamente la causa precede sempre l'effetto).

Il paradosso di Einstein, Podolsky e Rosen (EPR) è un esperimento ideale, proposto dagli autori nel 1935⁶, pensato allo scopo di dimostrare che la teoria quantistica era fondamentalmente incompleta. Le leggi della meccanica quantistica stabiliscono che la funzione d'onda determina le probabilità associate all'esito di un esperimento e che la funzione d'onda stessa contiene tutta l'informazione possibile sullo stato quantistico del sistema in esame. Einstein ed altri scienziati ritenevano invece che le previsioni della meccanica quantistica fossero corrette, ma solo come risultato di distribuzioni statistiche di altre proprietà sconosciute associate alle particelle. L'esperimento si basa sulla apparente contraddizione tra i principi relativistici di località e di causalità ed il fenomeno dell'entanglement per arrivare alla conclusione che dovevano esserci delle "variabili nascoste", non previste dalla meccanica quantistica stessa.

Si consideri un sistema composto da due particelle, distanti nello spazio, che sia nello stato *entangled* esposto nel precedente paragrafo:

$$|\Psi, t\rangle = \frac{1}{\sqrt{2}}|1, \uparrow\rangle|2, \uparrow\rangle + \frac{1}{\sqrt{2}}|1, \leftrightarrow\rangle|2, \leftrightarrow\rangle$$

Al tempo t si sottopone il fotone 1 che si trova nella regione dello spazio A ad una misura di polarizzazione piana lungo la verticale. Si supponga che il fotone superi il test. Per quanto visto l'effetto della misura è quello di ridurre lo stato del sistema, al tempo $t+dt$ a:

$$|\Psi, t+dt\rangle = |1, \uparrow\rangle|2, \uparrow\rangle$$

A questo punto l'osservatore che si trova in A e che ha eseguito la misura ha la certezza che il fotone 2 supererebbe un analogo test di polarizzazione verticale, senza bisogno di compiere alcuna ulteriore azione. In altre parole immediatamente dopo la misura in A del fotone 1, il fotone 2 possiede un elemento di realtà fisica (la polarizzazione verticale) che prima non aveva.

Il paradosso EPR si basa sul principio di località per affermare che l'azione sul fotone 1 nella regione A non può aver creato questo elemento di realtà sul fotone 2. Di conseguenza è possibile concludere che il fotone 2 doveva possedere la proprietà di superare con certezza un test di polarizzazione verticale anche prima ed indipendentemente dalla misura sul fotone 1 (e quindi che la teoria quantistica è incompleta).

Il Teorema di Bell

Nonostante il fatto che le contraddizioni evidenziate dal paradosso EPR fossero state risolte dopo un breve periodo dal fisico Niels Bohr e che fosse accertato che alcuni fenomeni quantistici sono

⁶ Einstein, A.; Podolsky, B.; and Rosen, N. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* **47**, 777-780, 1935.

genuinamente non locali, l'ipotesi che potessero esistere delle "variabili nascoste" in grado di spiegare i fenomeni quantistici in modo più accurato continuò ad avere un certo credito presso molti scienziati almeno fino a quando Bell non dimostrò il teorema che porta anche il suo nome (detto anche Disuguaglianza di Bell) che può riassumersi dicendo che qualsiasi teoria locale, che assume che determinate coppie di particelle correlate separate ed inviate verso rivelatori lontani abbiano proprietà definite anche prima di essere sottoposte a test, non può riprodurre la distribuzione probabilistica prevista dalla meccanica quantistica allorché si considerino non solo misure "simmetriche/opposte" ma anche test su posizioni intermedie.

Introduzione storica

La moneta quantistica di Wiesner

L'inizio della storia della crittografia quantistica risale alla fine degli anni sessanta del secolo scorso quando Stephen Wiesner propose in un manoscritto, pubblicato successivamente nel 1983⁷, due concetti che si rivelarono fondamentali: il "multiplexing channel", sviluppato poi nel protocollo "oblivious transfer" da Rabin e l'idea di *moneta quantistica*, una banconota le cui caratteristiche la rendessero fisicamente impossibile da falsificare.

Il denaro quantistico di Wiesner si basava sulla fisica dei fotoni, in particolare sulle proprietà di polarizzazione.

L'idea esposta prevede che ogni banconota contenga oltre al tradizionale numero di serie univoco anche venti "trappole di luce", dei meccanismi in grado di conservare un singolo fotone, precedentemente polarizzato casualmente in una delle due basi: $(0^\circ, 90^\circ)$ o $(45^\circ, 135^\circ)$.

La banca mantiene un archivio, ovviamente segreto, in cui per ogni banconota viene registrato il relativo numero di serie e lo specifico orientamento ($0^\circ, 45^\circ, 90^\circ, 135^\circ$) dei fotoni contenuti nelle trappole di luce.

Un eventuale falsario per contraffare una banconota non può semplicemente produrne una con un numero di serie ed una sequenza di polarizzazione arbitrari perché questa sarebbe scoperta immediatamente ad un controllo, non comparando nell'elenco della banca, ma dovrebbe tentare di copiarne una autentica.

Per realizzare un buon falso egli dovrebbe misurare la sequenza di venti polarizzazioni, copiare il numero di serie e quindi inserire nella copia i fotoni correttamente orientati nelle trappole di luce.

La sicurezza della moneta quantistica si basa proprio sulla difficoltà di misurazione della polarizzazione dei fotoni: se il falsario non è in grado di osservarla con precisione non può chiaramente riprodurla in modo corretto. Il solo modo che ha il falsario di ottenere informazioni sui fotoni è quello di usare un filtro polarizzatore. Supponiamo ad esempio che il falsario usi un filtro orientato verticalmente per verificare quali informazioni possa ottenere: il fotone potrebbe essere orientato nello stesso modo ed uscire oppure potrebbe essere orientato orizzontalmente ed essere bloccato dal filtro, in questi due casi l'informazione ottenuta sarebbe corretta ma il fotone potrebbe anche essere stato inserito nella trappola di luce con uno dei due orientamenti diagonali,

⁷ Wiesner, "Conjugate Coding", *Sigact News* 15, 1983

in questo caso avrebbe una probabilità del 50% di superare il filtro ed essere creduto verticale o una identica probabilità di essere bloccato e quindi ritenuto orizzontale. Il problema vero del falsario consiste nel fatto che per misurare con certezza la polarizzazione del fotone è necessario usare il corretto orientamento del filtro ma è proprio per ottenere questa informazione che la misurazione stessa viene effettuata!

L'impossibilità di avere informazioni complete sulla polarizzazione dei fotoni, conseguenza del principio di indeterminazione di Heisenberg, non creano però alcuna difficoltà alla banca che voglia controllare l'autenticità della banconota: disponendo a priori delle informazioni sul contenuto delle trappole di luce, ottenute tramite il numero di serie, si può usare per ognuna di esse un filtro orientato nella giusta base, smascherando così anche il falsario ingenuo che avesse inserito nella banconota contraffatta dei fotoni con una polarizzazione arbitraria. Se invece la banconota supera il controllo può essere rimessa in circolazione reinserendovi i fotoni appropriati.

Pur essendo irrealizzabile, non è noto infatti alcun modo di conservare per lunghi periodi un fotone nello stesso stato di polarizzazione, la moneta quantistica fornì lo spunto per ulteriori sviluppi negli anni successivi basati sulla possibilità di trasmettere delle informazioni in modo assolutamente sicuro, sfruttando proprio le proprietà della fisica quantistica.

Nel 1979 Charles Bennet e Brassard si basarono sui concetti esposti da Wiesner per ideare un sistema di distribuzione delle chiavi tale da garantire l'assoluta sicurezza, nel 1984 pubblicarono il protocollo oggi conosciuto come "BB84"⁸.

⁸ C.H. Bennet, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", International Conference on Computers, Systems & Signal Processing, 1984

QKD – Quantum Key Distribution

La *quantum key distribution*, o QKD, è una tecnica per generare e scambiare in modo assolutamente sicuro delle chiavi segrete per uso crittografico tra due soggetti, sfruttando le particelle elementari e basandosi sulle leggi della fisica quantistica.

La QKD è quindi un modo per risolvere il problema della generazione e dello scambio di chiavi segrete, di lunghezza arbitraria, destinate ad essere utilizzate in algoritmi crittografici su canali convenzionali. Questo sistema permette di evitare l'utilizzo di algoritmi crittografici asimmetrici, basati su assunti matematici fino ad ora non provati e quindi potenzialmente oggetto di attacchi.

Protocollo BB84

Il primo esempio di protocollo basato su assunzioni quantistiche è stato proposto nel 1984 da Charles Bennett e Gilles Brassard⁹ da cui il nome di BB84. Facendo riferimento al testo in nota utilizzeremo la polarizzazione lineare dei fotoni per illustrare la tecnica di distribuzione della chiave, precisando che è però possibile applicare gli stessi principi anche usando basi circolari o sfruttando proprietà di angolo di fase.

Assumiamo che le due parti, convenzionalmente chiamate Alice e Bob, abbiano accesso a due canali, uno quantistico ed uno pubblico.

Il protocollo

Per illustrare il protocollo consideriamo degli impulsi di luce polarizzata, ciascun impulso è composto da un singolo fotone ed ogni fotone potrà essere polarizzato verticalmente o orizzontalmente: nella notazione di Dirac indicheremo questi stati rispettivamente con $|\updownarrow\rangle$ e $|\leftrightarrow\rangle$.

Per trasmettere informazioni stabiliamo arbitrariamente un sistema di codifica, ad esempio $|\updownarrow\rangle$ vale 0 e $|\leftrightarrow\rangle$ vale 1, per cui Alice e Bob potranno comunicare semplicemente inviandosi delle sequenze di impulsi.

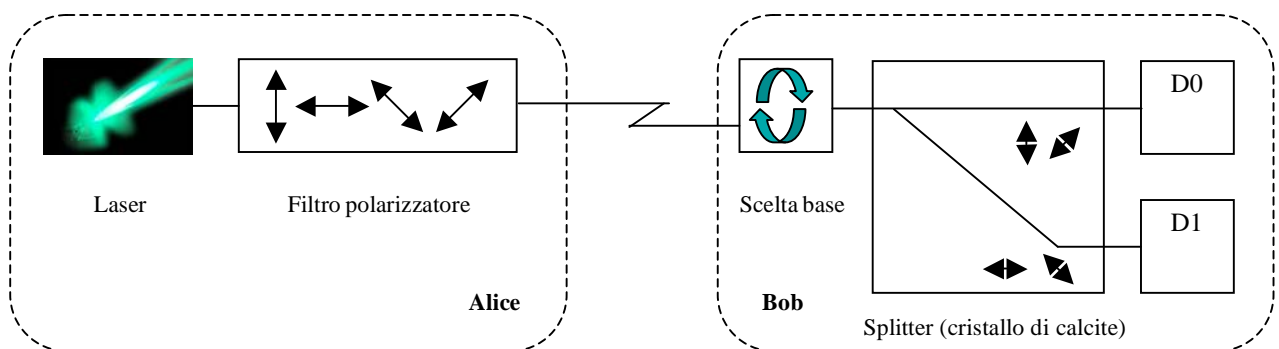
⁹ C.H. Bennet, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", International Conference on Computers, Systems & Signal Processing, 1984

Se ad esempio Alice inviasse una sequenza di impulsi come:

$$|\leftrightarrow\rangle, |\updownarrow\rangle, |\leftrightarrow\rangle, |\updownarrow\rangle, |\updownarrow\rangle, |\leftrightarrow\rangle, |\leftrightarrow\rangle, |\updownarrow\rangle,$$

Bob interpreterebbe questa sequenza come il numero binario 10100110. I due stati indicati formano una base dello spazio di Hilbert, che verrà detta base orizzontale-verticale ed indicata con il simbolo \oplus .

Alice decide di trasmettere i valori 0 e 1 con pari probabilità, come richiesto dalla casualità della chiave da condividere. Per ricevere il messaggio, Bob utilizza un dispositivo, ad esempio un cristallo birifrangente di calcite, in grado di misurare la polarizzazione di un fotone in ingresso e di inoltrarlo in modo deterministico lungo due diversi cammini: in linea retta se polarizzato verticalmente oppure traslato se polarizzato orizzontalmente fino a fargli raggiungere una coppia di rilevatori (*detector*) che si attivano indicando quindi la ricezione di uno 0 o di un 1 nella base scelta. Come conseguenza di possibili disturbi lungo il canale di trasmissione o di problemi nei sensori, potrebbe verificarsi una mancata ricezione di alcuni bit di informazione (nella realtà questa situazione si verifica abbastanza spesso), in questo caso Bob informerà Alice della mancata ricezione ed il bit non sarà utilizzato. Alla fine solo una frazione dei bit inviati sarà stata ricevuta correttamente ma gli altri saranno effettivamente condivisi tra Alice e Bob. A causa di questa limitazione il sistema indicato non è utilizzabile per l'invio diretto di un messaggio dato mentre può essere utile per scambiarsi una chiave crittografica che abbia come unici requisiti casualità e confidenzialità.



Schema di polarizzazione: il trasmittente, Alice, invia singoli fotoni polarizzati a Bob. La polarizzazione è controllata da un filtro che permette la scelta tra i quattro possibili stati. Bob può orientare il proprio sistema di ricezione in una delle due basi, lungo gli assi o lungo le diagonali, il filtro consente quindi il passaggio o meno del fotone che può essere rilevato dai detector e quindi interpretato come uno 0 o un 1.

In realtà, per quanto visto fino a questo punto il sistema è decisamente insicuro: un attaccante potrebbe intercettare gli impulsi trasmessi da Alice, misurarli ed inviarne di identici a Bob. In questo caso Eve avrebbe la certezza di avere accesso alla chiave condivisa.

Una strategia per ottenere la confidenzialità prevede l'aggiunta di una ulteriore scelta casuale durante l'invio: Alice potrà polarizzare i fotoni trasmessi sia nella base \oplus indicata in precedenza, sia in un'altra base diagonale \otimes in cui $|\nearrow\rangle$ rappresenta uno 0 e $|\searrow\rangle$ rappresenta un 1. Come prima, Alice invierà 0 o 1 con la stessa probabilità. Anche Bob potrà scegliere se misurare i fotoni in arrivo nella base rettilinea o in quella diagonale. Questo accorgimento consente di ottenere la sicurezza grazie ad un principio fondamentale della meccanica quantistica: l'indeterminazione. Un fotone inviato in una base e misurato nell'altra ha una probabilità di $\frac{1}{2}$ di essere riconosciuto come 0 o come 1, indipendentemente dal suo valore iniziale: il risultato è cioè puramente casuale e non esiste alcuna altra proprietà del fotone che consenta di prevedere quale percorso seguirà.

Se Alice sceglie casualmente la base in cui trasmettere e mantiene segreta l'informazione non c'è modo per Eve di sapere se la base che usa per le misurazioni sia corretta o meno. Ogni volta che la base usata non è la stessa di Alice il risultato sarà casuale e quindi per ogni fotone intercettato Eve non può sapere se il risultato è corretto o meno.

Questa proprietà spiega anche il motivo per cui è necessario utilizzare impulsi contenenti un singolo fotone: se venisse trasmesso un impulso contenente più fotoni, sarebbe possibile per Eve effettuare diverse misurazioni e confrontare i risultati, due risultati diversi per lo stesso impulso indicherebbero che la base è sbagliata e l'attaccante potrebbe semplicemente non inoltrare il risultato senza generare errori. Fino a che viene inviato un solo fotone, Eve non ha altre opzioni se non misurarli ed inviare a Bob il risultato dell'osservazione (intercept-resend), questo comportamento introduce degli errori che possono essere poi verificati da Alice e Bob che saranno quindi coscienti della presenza di un ascoltatore sul canale.

Nella tabella seguente è fornito un esempio di applicazione del protocollo illustrato: Alice sceglie in modo casuale sia una base (\oplus o \otimes) che un valore del bit (0 o 1) da inviare, e quindi invia un fotone opportunamente polarizzato a Bob. Bob sceglie a sua volta una base in modo casuale ed osserva sul detector il valore del bit corrispondente. Questi bit formano la *chiave grezza*. Alice e Bob si comunicano quindi, su un canale pubblico in chiaro le rispettive basi, scartando tutti i bit in cui esse non coincidono. Il risultato è detto *sifted key* (chiave raffinata). Per verificare che non si siano verificati episodi di origliamento si scelgono dei bit a caso tra quelli

rimanenti e li si confronta, scartandoli. Nell'esempio non ci sono difformità, il che indica che la trasmissione è sicura. I bit rimasti sono la chiave condivisa.

Base di Alice	\oplus	\oplus	\otimes	\otimes	\oplus	\otimes	\otimes	\oplus	\oplus	\otimes
bit inviato	1	1	0	1	0	0	1	0	0	1
Alice invia	$ \leftrightarrow\rangle$	$ \leftrightarrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$	$ \updownarrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$	$ \updownarrow\rangle$	$ \updownarrow\rangle$	$ \searrow\rangle$
Base di Bob	\otimes	\oplus	\oplus	\otimes	\otimes	\otimes	\oplus	\oplus	\oplus	\otimes
bit ricevuto	1	1	1	1	0	0	1	0	0	1
Stessa base ?	NO	SI	NO	SI	NO	SI	NO	SI	SI	SI
Alice conserva bit		1		1		0		0	0	
Bob conserva bit		1		1		0		0	0	
Bit di verifica (scelti arbitrariamente)		NO		SI		NO		NO	SI	
Chiave		1				0		0		

Il protocollo BB84 può essere riassunto nei seguenti punti:

1. Alice sceglie casualmente sia la base che il valore del bit e trasmette a Bob sul canale quantistico il corrispondente fotone polarizzato. Per ogni invio Alice memorizza e mantiene segreta la sua scelta.
2. Bob sceglie casualmente (in modo indipendente da Alice) la base in cui effettuare la misurazione ed osserva, nella base scelta, il fotone ricevuto oppure la mancanza di ricezione dovuta a perdite sul canale. Per ogni ricezione Bob memorizza e mantiene segreti sia la base utilizzata che il valore osservato. L'insieme delle registrazioni forma la chiave grezza.
3. Usando il canale di comunicazione pubblico non quantistico, Bob segnala ad Alice quali basi ha utilizzato per le misurazioni, ma non i risultati ottenuti.
4. Allo stesso modo Alice comunica a Bob le basi usate per le trasmissioni. Entrambi scartano tutti i bit in cui le basi non coincidono. I valori rimanenti formano la chiave setacciata o *sifted key*. Viene effettuata una prima stima statistica degli errori presenti nella trasmissione, se la stima è minore di un valore di soglia, la chiave viene accettata, altrimenti tutta la trasmissione viene cancellata e ripetuta con nuovi valori casuali.

5. Per trasformare le loro stringhe, parzialmente inficiate da errori e potenzialmente non sicure, in chiavi segrete condivise Alice e Bob devono effettuare alcune ulteriori verifiche: stimare il tasso di errore della trasmissione e valutare se le comunicazioni hanno subito origliamento. Sono quindi richieste delle procedure per individuare e correggere tutti gli errori e ridurre ad un valore piccolo a piacere l'informazione ottenuta da Eve. Nella pratica i valori di alcuni bit, scelti in modo casuale, vengono verificati sul canale di comunicazione pubblico da Alice e Bob per verificarne la corrispondenza e quindi scartati. La sequenza di bit rimanente è la chiave segreta.

Si può notare come, anche in assenza di *eavesdropping* ed errori di trasmissione, la chiave grezza contenga in media un 25% di bit sbagliati. Infatti nel 50% dei casi la base di Bob sarà diversa da quella di Alice e quando si usa la base sbagliata per la misurazione, il risultato sarà errato nel 50% dei casi. Un tasso di errore del 25% è troppo elevato per essere corretto efficacemente con dei codici a correzione di errore classici ed è per questo che sono stati introdotti i passi 3 e 4 per eliminare tutti gli errori dovuti all'uso di basi non corrette da parte di Bob. È importante notare come in queste comunicazioni sul canale pubblico Eve non ottenga alcuna informazione sulla composizione della chiave.

Correzione errori e Privacy Amplification

Analizziamo adesso con un maggiore livello di dettaglio le procedure necessarie per la riconciliazione delle chiavi, a partire dalla *sifted key* fino ad arrivare alla chiave condivisa.

Abbiamo assunto che Eve possa ascoltare il contenuto del canale pubblico (ma non modificarlo) e quindi tutti i messaggi scambiati dovranno essere strutturati in modo da fornire ad Eve il minor numero di informazioni possibili.

Il protocollo di correzione è stato esposto per la prima volta da Bennett ed altri, nel 1992¹⁰ e permette di riparare sia gli errori di trasmissione che quelli dovuti ad una intercettazione.

Alice e Bob devono essersi preventivamente accordati su alcuni parametri: un valore k per suddividere le stringhe in loro possesso in blocchi di k bit ciascuno ed una permutazione casuale da applicare ai blocchi (per randomizzare la posizione degli errori all'interno dei blocchi). La dimensione k dei blocchi dovrebbe essere scelta in funzione del tasso di errore atteso, in modo tale che sia improbabile che ogni blocco contenga più di un errore, tale funzione non è stata ancora definita esattamente quindi viene utilizzata una dimensione stabilita in base a prove empiriche basate sulle apparecchiature impiegate. Un sistema valido potrebbe essere quello di “sacrificare” inizialmente un campione di bit presi casualmente dalla *sifted key* per verificare l'incidenza degli errori ed inferire quindi la dimensione ottimale del blocco.

Per ogni blocco Alice e Bob confrontano la parità. Se la parità concorda i blocchi vengono temporaneamente accettati, altrimenti viene effettuata da entrambi una ricerca bisettiva sul blocco, calcolando $\log(k)$ parità dei sottoblocchi fino a trovare e correggere il bit sbagliato. Per impedire di fornire informazioni ad Eve si procede quindi a scartare l'ultimo bit del blocco.

Per eliminare gli errori rimanenti, dovuti alla presenza nei blocchi di un numero pari di bit scorretti, si itera il procedimento (permutazione e controllo di parità) più volte con dimensioni crescenti dei blocchi fino a che si stima che il numero di errori rimasti sia molto basso.

Questo approccio, basato sul confronto di parità presenta comunque notevoli inconvenienti, tra tutti il più significativo appare essere lo spreco di informazione necessario al completamento dell'algoritmo. Infatti, ipotizzando la presenza di due soli errori ed una suddivisione della stringa in k blocchi, la probabilità che questi non siano rilevati è pari ad $1/k$ con uno spreco di k bit.

Per questi motivi è stata proposta un'altra strategia in cui, allo stesso costo di l bit, si ottiene una probabilità di mancata rilevazione di errori di 2^{-k} ed inoltre la probabilità non è correlata al numero ed alla posizione degli errori stessi.

¹⁰ C.H. Bennet, F. Bessette, G. Brassard, L. Salvail, J. Smolin “Experimental Quantum cryptography”, Journal of Cryptology, vol. 5, 1992

Ad ogni iterazione il confronto sulla parità viene effettuato su un sottoinsieme casuale dell'intera stringa, comunicato sul canale pubblico. Se le sottostringhe di Alice e Bob differiscono la parità dei due sarà diversa con probabilità di $1/2$; se viene rilevata questa differenza allora verrà avviata una ricerca bisettiva sul sottoinsieme, fino a trovare e correggere l'errore. Anche in questo caso l'ultimo bit della sottostringa viene scartato per prevenire perdite di informazione nei confronti di Eve. Naturalmente ogni sottoinsieme viene stabilito in base ad una diversa scelta casuale delle posizioni dei bit.

Alice e Bob non possono sapere con certezza quando tutti gli errori saranno stati corretti e quindi dovranno continuare a confrontare sottoinsiemi, ottenendo sempre risultati positivi, fino ad avere una bassissima probabilità di avere errori non rilevati nelle rispettive stringhe.

A questo punto i due condividono una chiave corretta ma solo parzialmente segreta. Si può quindi procedere a ridurre l'informazione in possesso di Eve fino a renderla arbitrariamente piccola ed ottenere quindi una chiave sicura. Questo processo è noto come *privacy amplification*¹¹. Dal numero di errori presenti nella *sifted key* è possibile stimare l'informazione nota ad Eve, ovvero il numero di bit corretti di cui è in possesso. Alice e Bob si accordano su di un sottoinsieme casuale di posizioni di bit rispetto alla chiave condivisa (già depurata dagli errori), Eve potrebbe conoscere la parità di questo sottoinsieme solo se conoscesse tutti i bit che lo compongono e questo evento è altamente improbabile. Quindi Alice e Bob possono usare questa parità come primo bit di una nuova, assolutamente sicura, chiave finale. Infatti scegliendo un numero di sottoinsiemi indipendenti approssimativamente uguale alla dimensione della chiave condivisa meno il numero di bit che si stima Eve possa conoscere, Alice e Bob ottengono un equivalente numero di bit condivisi: la chiave finale, condivisa ed assolutamente sicura. La tecnica di *privacy amplification* miscela le informazioni che Eve conosce con altre che non può sapere, diluendo la sua conoscenza.

Ai fini del corretto funzionamento dell'algoritmo è opportuno fare alcune ulteriori osservazioni:

- Il canale di comunicazione deve garantire autenticazione, in modo tale da non consentire attacchi di tipo *man in the middle*, in cui Eve impersona Bob con Alice e viceversa.
- Per autenticare il canale è comunque necessario che Alice e Bob condividano una (breve) chiave segreta convenzionale. In tal senso è corretto parlare di protocollo di accrescimento di chiave crittografica.

¹¹ C.H. Bennet, G. Brassard, M. Robert "Privacy amplification by public discussion", Siam Journal, vol.17, 1988

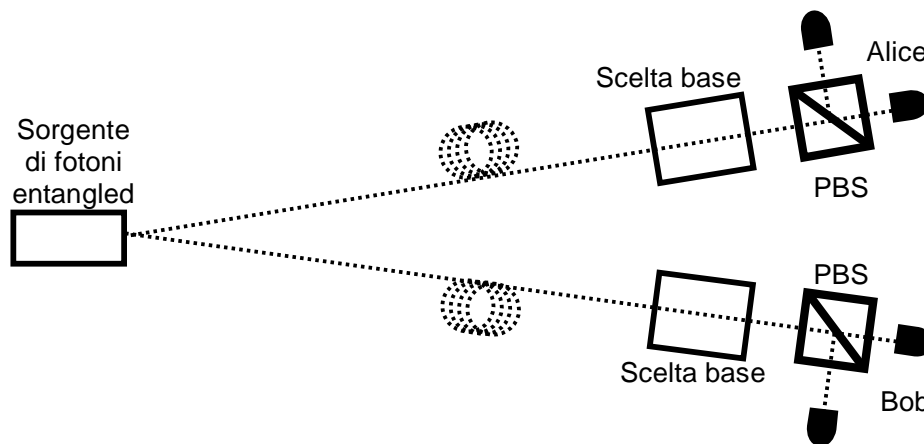
Strategie di intercettazione

Oltre alla strategia intercept-resend precedentemente illustrata Eve ha altre opzioni a disposizione per cercare di ottenere informazioni. In particolare l'attacco *beamsplitting* (divisione del raggio) dipende dal fatto che gli impulsi trasmessi normalmente non sono realmente dei singoli fotoni polarizzati, ma dei deboli impulsi di luce laser monocromatica. Utilizzando uno specchio semiargentato Eve devia una frazione dell'impulso luminoso, lasciandone passare una parte inalterata verso Bob che non si accorgerebbe di nulla. Se l'impulso fosse molto debole, ovvero contenesse pochissimi fotoni, Eve dovrebbe conservare i fotoni per poi misurarli *dopo* l'annuncio pubblico delle basi scelte da Alice. Attualmente non è però noto alcun metodo per conservare fotoni polarizzati. Nel caso di misurazione immediata in una base arbitraria Eve non potrebbe comunque ottenere una frazione significativa di informazioni. Un problema di sicurezza decisamente maggiore si porrebbe invece nel caso in cui l'impulso fosse abbastanza intenso da consentire ad Eve di deviare un numero di fotoni sufficiente a misurare correttamente la loro polarizzazione, anche senza conoscerne a priori la base corretta. Fortunatamente questa circostanza è talmente improbabile da non costituire un serio rischio per la sicurezza, inoltre il sistema di *privacy amplification* già visto può limitare superiormente la quantità di informazioni in possesso di Eve fino a renderla arbitrariamente bassa.

Protocollo E91

Un interessante algoritmo di QKD è stato proposto da Arthur Ekert nel 1991¹², basandosi sul paradosso EPR.

Si attiva una sorgente che emette coppie di fotoni entangled, uno dei quali diretto verso Alice e l'altro verso Bob. Entrambi, attraverso filtri polarizzatori e PBS, effettuano misure della polarizzazione in basi casuali e indipendenti tra loro.



Nella prima variante di tale protocollo, strettamente derivata da BB84, dopo la trasmissione la sorgente annuncia pubblicamente le basi usate (rettilinea o diagonale) ed Alice e Bob scartano immediatamente i bit in cui le misurazioni sono state fatte nella base incompatibile, in seguito eseguono gli stessi passaggi di controllo e correzione errori di BB84. A patto che la sorgente sia affidabile, ovvero non sia in mano ad Eve, tale protocollo è altrettanto sicuro di quello proposto da Bennett e Brassard. Infatti se le basi scelte sono corrette, il valore misurato da entrambi sarà identico mentre se le basi sono scorrelate tra loro, i risultati delle misurazioni saranno casuali e scorrelati.

La seconda variante del protocollo si appoggia invece alla disuguaglianza di Bell: i fotoni *entangled* vengono polarizzati in modo casuale in *tre* basi non ortogonali differenti (rettilinea, diagonale e circolare). In questo caso i risultati delle misurazioni fatte lungo le basi non coincidenti non vengono scartati a priori ma servono per fare un test basato sulla disuguaglianza di Bell, ad esempio per controllare che i due fotoni ricevuti siano realmente *entangled*.

¹² A. Ekert, "Quantum Cryptography based on Bell's Theorem", Physical Review Letters Vol. 67, N. 6, 5 Agosto 1991

Un eavesdropper non può ottenere informazioni da un singolo fotone in transito, semplicemente perché esso non contiene alcuna informazione: l'informazione stessa “diviene in essere” solo dopo che essi sono stati misurati dai legittimi destinatari.

Un'altra strategia possibile con cui Eve potrebbe tentare di ottenere informazioni potrebbe consistere nell'alterazione della sorgente in modo che essa non emetta più due soli fotoni ma tre (misurando poi il terzo fotone senza influenzare quelli diretti ai legittimi destinatari), anche in questo caso una semplice misurazione della lunghezza d'onda dei fotoni da parte di Alice e Bob permetterebbe di rilevare una riduzione di energia e quindi di smascherare Eve.

Oblivious Transfer

Nel suo ormai celebre articolo, Wiesner introdusse non solo l'idea che la meccanica quantistica potesse essere usata a scopi crittografici ma anche uno "strumento" crittografico che chiamò *conjugate coding*. Esso venne reinventato una decina di anni dopo da Even, Goldreich e Lempel che lo chiamarono "one-out-of-two Oblivious Transfer" dal nome di un altro metodo simile pubblicato da Rabin e noto come "Oblivious Transfer"¹³.

In un Oblivious Transfer, Alice invia un messaggio a Bob che lo riceve con una probabilità del 50% (tale probabilità non è controllabile dalle parti). Alice non sa se Bob ha ricevuto o meno il messaggio.

Analogamente, in un one-out-of-two Oblivious Transfer, Alice ha due messaggi, m_0 e m_1 che invia a Bob in modo tale che egli possa decidere di riceverne uno a sua scelta, ma non entrambi. Alice ignora quale dei due messaggi sia stato effettivamente ricevuto da Bob.

Lo scopo del protocollo è quello di fare in modo che le due parti non possano ottenere più informazioni di quelle consentite, indipendentemente da eventuali comportamenti fraudolenti ed evitando di fornire informazioni ad un eventuale attaccante.

Il protocollo

Siano b_0 e b_1 i due messaggi (binari) che Alice deve inviare a Bob e sia n il triplo della lunghezza in bit dei messaggi.

I passi richiesti per completare il protocollo sono i seguenti:

1. Questo passo deve essere ripetuto n volte:
 - Alice sceglie un bit casuale r_i
 - Alice sceglie, sempre in modo casuale, una base di trasmissione (\oplus , \otimes)
 - Alice invia a Bob un fotone π_i polarizzato nella base scelta
 - Bob sceglie casualmente una base di ricezione (\oplus , \otimes)
 - Bob misura il fotone in arrivo nella base scelta

¹³ M. Rabin "How to exchange secrets with oblivious transfer" *Technical report TR-81, Aiken Computation Lab, Harvard University, 1981*

- Bob imposta un bit r'_i in base al valore ottenuto dalla misurazione e segnala ad Alice l'avvenuta ricezione di un fotone
2. Alice annuncia l'elenco delle basi scelte per l'invio a Bob
 3. Bob seleziona casualmente due sottoinsiemi I_0, I_1 dei bit ricevuti, disgiunti, aventi entrambi cardinalità pari ad $n/3$ ed in cui tutti gli elementi appartenenti ad I_0 hanno la caratteristica di essere stati misurati nella stessa base in cui Alice li ha inviati. Bob annuncia gli elementi dei due insiemi ad Alice, senza però indicare quale dei due è l'insieme contenente solo le misurazioni coerenti
 4. Alice riceve i due insiemi, calcola e trasmette a Bob $J_0 = b_0 \oplus I_0$ e $J_1 = b_1 \oplus I_1$.
 5. Bob riceve i due insiemi ed ottiene il messaggio $b = J_0 \oplus I_0$

Intuitivamente, Alice sceglie in modo casuale una sequenza di n bit $r_1 r_2 \dots r_n$ e li invia a Bob codificando ciascun bit in una delle due basi tra loro coniugate, come nel protocollo BB84. Bob sceglie arbitrariamente una base in cui effettuare la ricezione. Quando le basi usate da Alice e da Bob coincidono il bit ricevuto è corretto, altrimenti il risultato è del tutto casuale.

Alice annuncia quindi a Bob le basi di polarizzazione scelte, consentendo a quest'ultimo di costruirsi due insiemi di cui solo uno contiene solo bit misurati nelle basi corrette e li inoltra entrambi ad Alice (che non sa quale dei due insiemi è quello valido). Alice effettua lo xor binario di ognuno dei messaggi con una delle stringhe ricevute e manda il risultato della computazione a Bob al quale non resta che effettuare ancora uno xor per ottenere uno dei due messaggi, come illustrato nello schema seguente:

Alice vuole inviare i due messaggi $b_0=(\mathbf{1,0,1})$ e $b_1=(1,1,0)$, Bob vuole ricevere $b_c = b_0$									
Base scelta casualmente da Alice	\oplus	\oplus	\otimes	\otimes	\oplus	\otimes	\otimes	\oplus	\oplus
Bit scelto casualmente da Alice	1	1	0	1	0	0	1	0	0
Fotone inviato da Alice	$ \leftrightarrow\rangle$	$ \leftrightarrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$	$ \updownarrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$	$ \updownarrow\rangle$	$ \updownarrow\rangle$
Base scelta casualmente da Bob	\otimes	\oplus	\oplus	\otimes	\otimes	\otimes	\oplus	\oplus	\oplus
Bit misurato da Bob	1	1	1	1	0	0	1	0	0
Stessa base ?	NO	SI	NO	SI	NO	SI	NO	SI	SI
Bit che appartiene ad I_0 (scelta arbitraria)		SI		SI					SI
Bit che appartiene ad I_1 (scelta arbitraria)	SI		SI				SI		
Bob comunica ad Alice $I_0=(1,1,0), I_1=(1,1,1)$									

Alice calcola e trasmette $J_0 = I_0 \oplus b_0 = (1,1,0) \oplus (1,0,1) = (0,1,1)$ e $J_1 = I_1 \oplus b_1 = (1,1,1) \oplus (1,1,0) = (0,0,1)$

Bob riceve le due stringhe e calcola $b_0 = J_0 \oplus I_0 = (0,1,1) \oplus (1,1,0) = \mathbf{(1,0,1)}$

QKD ed algoritmi di cifratura tradizionali

Come illustrato nei capitoli precedenti, la crittografia quantistica è in realtà un insieme di metodi per la distribuzione sicura di chiavi, da utilizzare poi per la codifica con algoritmi crittografici simmetrici, che traggono beneficio dalla possibilità di utilizzare le chiavi assolutamente casuali e riservate così ottenute.

QKD e One Time Pad: sicurezza incondizionata

Quando le chiavi scambiate tramite QKD sono utilizzate con un cifrario di tipo One Time Pad per la cifratura e l'autenticazione è possibile garantire una trasmissione di dati su di un canale convenzionale punto-a-punto incondizionatamente sicura: le chiavi generate e scambiate tramite un canale quantistico sono genuinamente casuali e la loro riservatezza e integrità può essere matematicamente provata ed il loro abbinamento con One Time Pad, anch'esso incondizionatamente sicuro, garantisce tale proprietà

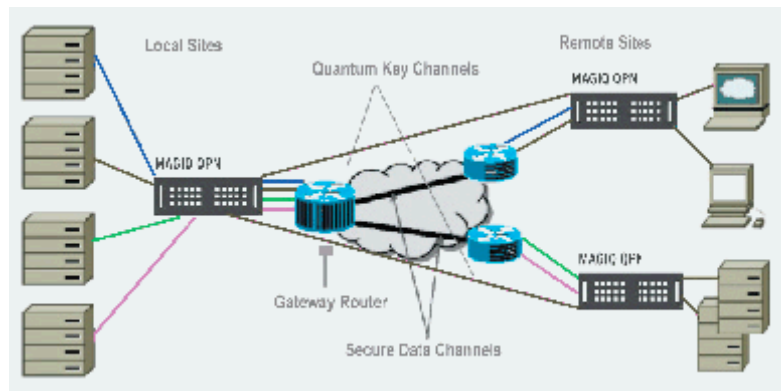
Anche se l'abbinamento di un sistema di QKD con l'algoritmo One Time Pad garantisce un livello di sicurezza assolutamente inviolabile esso si rivela di difficile applicabilità a causa della grande quantità di informazioni che devono essere scartate durante la fase di *key agreement* per garantire l'integrità delle comunicazioni e che porterebbe, in applicazioni reali, a risultati inaccettabili sul piano prestazionale.

QKD e schemi di cifratura computazionalmente sicuri

Per ovviare in parte a questo inconveniente la soluzione adottata dai produttori di sistemi di QKD commerciali IdQuantique e MagiQ è stata quella di utilizzare le chiavi condivise ottenute sul canale quantistico per cifrare con algoritmi simmetrici tipo AES le grandi quantità di dati da trasmettere poi sul canale convenzionale. Questa soluzione permette anche di realizzare delle connessioni cifrate VPN, ad esempio interfacciando i sistemi di scambio chiavi QKD con IPSEC.

Nell'immagine seguente è mostrato un possibile schema di funzionamento di una rete basata su fibre ottiche che colleghi diversi siti remoti tramite una VPN su IPSEC basata sul dispositivo

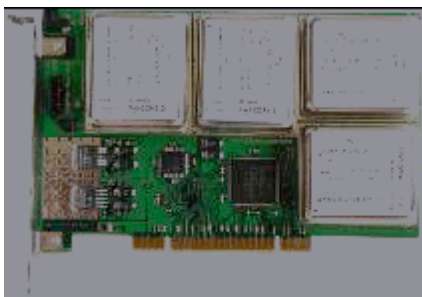
MagiQ QPN Security Gateway 7505, in grado di creare ed utilizzare fino a 100 chiavi al secondo da applicare ad algoritmi crittografici standard quali 3DES ed AES a 256 bit.



Chiaramente la sicurezza dei dati scambiati tramite un collegamento di questo tipo non può essere maggiore di quella dell'algoritmo utilizzato, e quindi dipendente dai seguenti quattro fattori:

1. La sicurezza della chiave (ovvero se essa può essere nota ad un attaccante)
2. Il numero di blocchi cifrati con la stessa chiave (tasso di rinnovo della chiave)
3. La lunghezza del modulo della chiave (56 bit per DES, 128, 192, 256 bit per AES)
4. La sicurezza dell'algoritmo simmetrico di cifratura applicato.

Gli ultimi due fattori sono puramente dipendenti dal sistema di cifratura e non dal modo in cui le chiavi vengono scambiate tra le parti. I primi due fattori, d'altra parte, dipendono strettamente proprio dalla scelta del metodo di scambio delle chiavi e la possibilità, offerta dalla QKD, di avere chiavi assolutamente casuali e private rinnovabili con elevatissima frequenza porta ad un consistente miglioramento della sicurezza complessiva del collegamento rispetto a tecniche che non ne facciano uso.



Nell'immagine a fianco un esempio di scheda PCI, compatibile con i principali sistemi operativi desktop, per la generazione di numeri realmente casuali basata sui principi della meccanica quantistica e prodotta dalla svizzera IdQuantique.

Conclusioni

Da quanto visto sui protocolli e sulle procedure della crittografia quantistica (o più correttamente *quantum key distribution*), per mezzo dei quali è possibile trasmettere in modo assolutamente sicuro delle chiavi segrete, è possibile effettuare un raffronto con la crittografia “classica” per verificare i punti di forza e di debolezza di entrambe le tecnologie.

Innanzitutto la QKD non può essere usata direttamente per trasmettere messaggi cifrati, né per archiviare contenuti segreti, mentre è estremamente sicura nella trasmissione di chiavi segrete di lunghezza arbitraria da applicare poi ad algoritmi crittografici non quantistici per la trasmissione o l’archiviazione sicure di messaggi.

Per il resto si tenterà un confronto basandosi su vari parametri di valutazione tra i sistemi a chiave pubblica/privata (P/PK) e la QKD.

- Le risorse necessarie ad implementare un sistema QKD sono indubbiamente più onerose, richiedendo sempre e comunque un sistema hardware dedicato, mentre P/PK è implementata in software su molti sistemi diversi.
- QKD è assolutamente sicura, sarebbe violabile solo violando le stesse leggi fisiche che ne stanno alla base. P/PK si basa su assunti computazionali non dimostrati, problemi che oggi sono ritenuti intrattabili potrebbero rivelarsi molto più semplici in seguito a nuove scoperte matematiche.
- P/PK richiede di aumentare costantemente la lunghezza delle chiavi di cifratura per resistere ad attacchi a forza bruta portati con sistemi sempre più efficaci, mentre la sicurezza di QKD, basandosi su principi fisici, non richiede aggiornamenti.
- QKD ad oggi può funzionare solo con collegamenti diretti tra le parti e su distanze relativamente brevi, mentre la sua controparte classica funziona a qualunque distanza e su qualunque tipo di rete.
- L’impossibilità di conservare fotoni polarizzati per periodi di tempo di lunghezza arbitraria richiede che le due parti della QKD siano connesse contemporaneamente, P/PK non ha questa limitazione.

La possibilità che in un futuro non troppo lontano vengano realizzati dei *quantum computer* con prestazioni sufficienti per far funzionare gli algoritmi (già noti) per risolvere in tempo polinomiale, tra gli altri, i problemi della fattorizzazione e del logaritmo discreto, attualmente alla base delle più diffuse procedure di crittografia utilizzate in ogni campo fa in modo che la crittografia quantistica rivesta un particolare interesse sia in ambito commerciale che militare, è quindi ragionevole aspettarsi un suo notevole sviluppo.

La sua proprietà peculiare, ovvero la possibilità di scoprire (e quindi neutralizzare) un eventuale ascoltatore, le conferisce un livello di sicurezza che non trova una controparte nei sistemi convenzionali e questo rende la crittografia quantistica una soluzione ideale per le applicazioni di trasmissione dati con elevati requisiti di sicurezza.

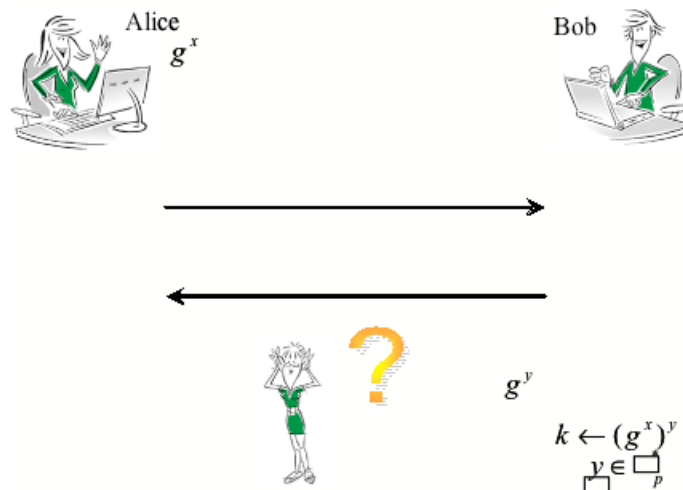
Alcuni problemi sono ancora oggetto di studio, in particolare devono essere ancora superate le difficoltà nell'integrazione con infrastrutture di rete esistenti che mitigherebbero il limite delle distanze raggiungibili dalle comunicazioni punto-a-punto. Quando queste difficoltà saranno superate la crittografia quantistica entrerà prepotentemente nelle applicazioni di sicurezza di massa, prima affiancando e poi probabilmente sostituendo gli attuali algoritmi di crittografia asimmetrica nelle situazioni in cui sia richiesta la massima sicurezza.

Appendici

A. Protocollo Diffie Hellman

Uno dei limiti più significativi della crittografia simmetrica è dato dal fatto che, dovendo comunicare con molte persone, è necessario disporre di un gran numero di chiavi diverse da scambiarsi preventivamente in modo sicuro e da custodire gelosamente per evitare rischi alla riservatezza ed all'integrità delle informazioni scambiate.

Gli albori della crittografia a chiave pubblica risalgono al 1976 quando Whitfield Diffie e Martin Hellman pubblicarono l'articolo "New Directions in Cryptography"¹⁴ nel quale illustravano una soluzione a questo problema mediante l'introduzione di un protocollo per l'accordo su una chiave segreta che desse la possibilità a due interlocutori che hanno a disposizione solo una linea non sicura di accordarsi senza che essa possa essere carpita da un ascoltatore non autorizzato.



Il protocollo Diffie Hellman originale si basa sulle proprietà dei gruppi finiti e richiede i seguenti passi:

- Alice e Bob si accordano su un numero primo "grande" p e su un altro numero g che sia generatore del gruppo \mathbb{Z}_p^* . Sia p che g sono costanti pubbliche del protocollo e si suppone che esse siano note a tutte le parti, inclusa Eve.

¹⁴ Whitfield Diffie, Martin Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, Novembre 1976

- Alice sceglie un numero x casuale appartenente a \mathbb{Z}_p^* , ovvero un numero compreso nell'intervallo $1..p-1$, poi calcola $g^x \bmod p$ e quindi invia il risultato a Bob.
- Bob a sua volta sceglie un numero casuale y appartenente a \mathbb{Z}_p^* , calcola $g^y \bmod p$ e quindi invia il risultato ad Alice.
- Adesso entrambi calcolano separatamente lo stesso valore $k = g^{xy} \bmod p$ a partire dai numeri che ciascuno di loro ha ricevuto dall'altro e dal valore casuale che hanno scelto: per Alice $k = (g^y)^x$ mentre per Bob $k = (g^x)^y$.
- Entrambi sono in possesso del valore k che può essere usato come chiave segreta per le comunicazioni successive.

Eve conosce p , g , e g^y ma non x o y . Il calcolo del valore di g^{xy} a partire dai valori in suo possesso è noto come problema di Diffie Hellman e, se p e g sono scelti correttamente, non è noto alcun algoritmo per calcolarlo efficientemente. $x \in \mathbb{Z}_p^*$ e quindi Eve non è in grado di calcolare il valore di k . Il modo più efficiente consiste nel cercare di ottenere x a partire da g^x ma anche questo metodo è considerato “difficile” e prende il nome di problema del logaritmo discreto.

B. Cenni alla computazione quantistica

Negli elaboratori convenzionali l'unità di misura dell'informazione è il bit, che può assumere solo due valori logici: 0 o 1. Tipicamente negli attuali computer lo stato di un bit è identificato dalla presenza o assenza di carica elettrica.

L'unità di misura dell'informazione nei quantum computer (QC) è invece il qubit. Un qubit è ancora un sistema a due stati, rappresentati nella notazione di Dirac come $|0\rangle$ e $|1\rangle$, mentre un bit può trovarsi solo nei due stati distinti 0 e 1 il qubit può contenere anche una loro sovrapposizione coerente. Si tratta di un terzo stato che non ha un analogo nell'informazione classica in cui il qubit rappresenta sia 0 che 1 contemporaneamente.

Formalmente quindi un qubit è rappresentato come un vettore in uno spazio di Hilbert dove, prendendo come elementi di una base ortonormale proprio $|0\rangle$ e $|1\rangle$, un generico vettore normalizzato può essere rappresentato come:

$$|Y\rangle = a|0\rangle + b|1\rangle, \text{ con } |a|^2 + |b|^2 = 1$$

con $a, b \in \mathbf{C}$. Lo stato di sovrapposizione implica il fatto che misurando $|Y\rangle$ si ottiene un risultato non deterministico dove la probabilità di ottenere il risultato $|0\rangle$ è pari ad $|a|^2$, mentre la probabilità di ottenere $|1\rangle$ è $|b|^2$.

Una caratteristica peculiare dei qubit è data dal fatto che un gruppo di essi può trovarsi in uno stato *entangled*, mostrando così un livello di correlazione che permette di operare su uno di essi, modificando però simultaneamente lo stato di un numero arbitrario di essi, ottenendo una forma di parallelismo estremamente potente.

La possibilità di gestire contemporaneamente un certo numero di qubit correlati e sovrapposti (quantum register) permette di sviluppare algoritmi efficienti per problemi che, nella teoria dell'informazione classica, hanno invece complessità superpolinomiale.

Si consideri ad esempio un computer "classico" che operi su un registro di 3 bit. In ogni momento i bit del registro sono in uno stato ben definito, ad esempio 101. In un quantum computer invece i qubit possono trovarsi in una sovrapposizione di stati, essendo il registro descritto da una funzione d'onda del tipo:

$$|\psi\rangle = \alpha|000\rangle + \beta|001\rangle + \gamma|010\rangle + \delta|011\rangle + \varepsilon|100\rangle + \phi|101\rangle + \varphi|110\rangle + \lambda|111\rangle$$

in cui i valori $\alpha, \beta, \gamma, \dots, \lambda$ sono numeri complessi il cui modulo al quadrato indica la probabilità di misurare il qubit nel relativo stato. Di conseguenza la probabilità di misurare il registro nello stato 010 è pari a $|\gamma|^2$.

Un registro composto da n qubit può quindi contenere *contemporaneamente* 2^n valori contro il singolo stato di un registro “classico”. Un ipotetico computer quantistico con un singolo registro composto da 300 qubit potrebbe contenere un numero di stati pari a circa 10^{90} , un valore più grande del numero di atomi dell’universo: è facile immaginare quale possa essere la potenza di un simile calcolatore.

La fattorizzazione degli interi è un problema ritenuto ingestibile dai computer tradizionali quando il numero N da scomporre sia il prodotto di due primi di grandi dimensioni (come nella chiave pubblica di RSA) in quanto gli algoritmi per risolverlo hanno complessità esponenziale: gli algoritmi noti più efficienti hanno infatti complessità $O((\log N)^k)$.

Se il numero N è composto da n cifre binarie, un quantum computer con registri di almeno $2n$ qubit è in grado di scomporlo in fattori primi in un tempo polinomiale utilizzando l’algoritmo di Shor¹⁵, con lo stesso metodo è possibile risolvere anche il problema collegato detto del logaritmo discreto, alla base della sicurezza del protocollo Diffie-Hellman.

Per motivi tecnologici, dovuti alla difficoltà di mantenere diverse particelle in uno stato di sovrapposizione coerente, ad oggi i prototipi di computer quantistici effettivamente realizzati utilizzano registri da pochissimi qubit (nel febbraio 2007 la canadese D-Wave Systems Inc ha mostrato un modello dotato di 16 qubit) e quindi non costituiscono una minaccia significativa alla sicurezza degli algoritmi crittografici a chiave pubblica ed agli schemi di firma digitale ma appare evidente come questi possano, in un futuro non troppo lontano, rendere obsoleto l’uso di sistemi di crittografia a chiave pubblica e quindi la necessità di trovare delle alternative resistenti a questo tipo di attacchi.

¹⁵ P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Novembre 1994

C. Postulati fondamentali della meccanica quantistica.

1.

Il moto e tutte le proprietà di un sistema fisico in un determinato stato dinamico sono descritte da una quantità ausiliaria detta **funzione d'onda** $\psi(\xi, t)$. Questa funzione è complessa, monodroma e continua di un insieme completo di coordinate indipendenti del sistema, che denotiamo collettivamente con il simbolo ξ , e del tempo. La variabile ξ individua i punti di uno spazio astratto, chiamato *spazio delle configurazioni*. Si useranno i termini *funzione d'onda* e *stato* come sinonimi.

Questo postulato implica una dipendenza di ξ dal tempo. Questo significa che in un certo istante, il sistema non occupa un punto preciso dello spazio delle configurazioni (la "traiettoria" della fisica classica) o, più esattamente, tutto funziona come se esso non avesse una traiettoria precisa e definibile. Il concetto di descrizione completa del sistema, intesa nel senso della meccanica classica, non ha più valore e quindi la descrizione di un sistema è intrinsecamente incompleta.

2.

In ogni istante l'integrale

$$\int_a^b |\psi(\xi, t)|^2 d\xi$$

è proporzionale alla probabilità che, nello stato descritto da ψ , il sistema si trovi all'interno del volume di spazio delle configurazioni limitato da a e b .

Questo postulato stabilisce il significato fisico della funzione d'onda. Non è possibile misurare sperimentalmente, in un dato istante ed in un dato punto dello spazio delle configurazioni, l'esistenza di solo una parte del sistema fisico: l'osservazione indica solo se l'intero sistema si trova in un punto o meno.

Nel caso in cui l'integrale

$$\int_{-\infty}^{+\infty} |\psi(\xi, t)|^2 d\xi$$

converga, si deduce che la funzione $\psi(\xi, t)$ tende a zero rapidamente per $|\xi| \rightarrow \infty$, cioè il sistema in quel dato istante è soggetto a forze che ne confinano il moto (ovvero le possibili posizioni) all'interno di un volume finito dello spazio delle configurazioni. In tal caso si dice che il moto del sistema è *finito*, o anche che il sistema si trova in uno **stato legato**. La funzione ψ in questo caso è normalizzabile ed il quadrato del modulo della funzione normalizzata all'unità coincide con la densità di probabilità della variabile ξ in quel dato istante. La funzione stessa $\psi(\xi, t)$ viene allora detta **ampiezza di probabilità**.

3.

Vale il principio di sovrapposizione degli stati, per cui:

- Se la funzione d'onda viene moltiplicata per un numero complesso scelto arbitrariamente e diverso da zero, la nuova funzione descrive lo stesso stato del sistema.
- Se a determinate condizioni il sistema può esistere in due stati distinti ψ_1 e ψ_2 , allora esso può esistere, sotto le stesse condizioni, anche in ogni altro stato del tipo:

$$a_1\psi_1 + a_2\psi_2$$

dove a_1 e a_2 sono numeri complessi arbitrari.

Il principio di sovrapposizione implica l'ammissibilità di stati del sistema in cui qualche grandezza fisica non è definita. Per esempio la combinazione lineare di due onde piane non è esprimibile come una terza, singola, onda piana. Una particella descritta da tale combinazione lineare non può avere un valore preciso ed univoco della quantità di moto e dell'energia. Da questa affermazione si ottiene che il risultato di una misurazione della quantità di moto eseguita su una particella in questo stato è **intrinsecamente non prevedibile**. Possiamo al massimo aspettarci che la funzione d'onda descriva la distribuzione di probabilità di tali risultati.

Il principio di sovrapposizione prescrive la sovrapposibilità delle ampiezze di probabilità, ma non delle densità di probabilità. Da questo si ottiene che in uno stato che sia la sovrapposizione di altri, come ad esempio

$$\psi = a_1\psi_1 + a_2\psi_2$$

la densità di probabilità, che si ottiene come

$$|\psi|^2 = |a_1|^2 |\psi_1|^2 + |a_2|^2 |\psi_2|^2 + \underline{a^* b \psi_1^* \psi_2 + a b^* \psi_1 \psi_2^*}$$

non è una semplice combinazione lineare delle densità di probabilità date, ma contiene dei termini di interferenza. Questa osservazione ha profonde conseguenze, in quanto rende inapplicabile ai fenomeni quantistici la statistica classica, in cui si combinano direttamente le distribuzioni di probabilità di eventi distinti.

4.

Lo stato di moto libero, ovvero non soggetto a forze, di una particella non relativistica avente massa m , quantità di moto p ed energia $E=p^2/2m$ è descritto da una onda piana:

$$\psi_k(r, t) = Ae^{i(k \cdot r - \omega t)}$$

dove

$\omega = E/\hbar$ e $k = p/\hbar$. \hbar è l'unità atomica di momento angolare definita come:

$$\hbar = \frac{h}{2\pi} \approx 1.0546 \cdot 10^{-34} J \cdot s$$

e h è la costante di Planck.

L'ipotesi che una particella libera avente una quantità di moto definita sia descritta da un'onda piana è necessaria per spiegare il comportamento ondulatorio delle particelle stesse (esperimenti di diffrazione). È stato mostrato sperimentalmente che alla particella deve essere associata un'onda di lunghezza $\lambda = \frac{2\pi\hbar}{p}$ e che la relazione $E = \hbar\omega$ (con ω frequenza angolare) deve

valere non solo per un fotone, ma per qualsiasi particella.

Valori medi di grandezze fisiche

In base ai postulati fondamentali precedentemente enunciati abbiamo stabilito che, in generale, una data grandezza fisica non abbia un valore specifico quando si trova in un determinato stato, ma piuttosto che essa abbia una distribuzione probabilistica di valori che si presenteranno come risultato di una osservazione. Risulta interessante allora calcolare il valore medio di una grandezza.

Inizialmente, per semplificare, effettueremo il calcolo del valore medio in un dato istante, in particolare porremo quindi $t = 0$ per poter omettere ovunque la dipendenza dal tempo.

Si supporrà inoltre di essere in uno stato legato, in modo che la funzione d'onda normalizzata $\psi(\xi, t)$ fornisca direttamente le densità di probabilità. Si farà riferimento ad una singola particella, descritta da una funzione $\psi(r)$.

Il valore medio della coordinata r può quindi essere calcolato direttamente come:

$$\langle r \rangle = \int r |\psi(r)|^2 dr \equiv \int \psi^*(r) \cdot r \psi(r) dr$$

in cui $\langle r \rangle$ indica un vettore i cui componenti sono i valori medi delle coordinate x , y e z .

Ricorrendo ancora alle definizioni di teoria della probabilità possiamo ottenere immediatamente anche il valore medio di una qualsiasi funzione di r :

$$\langle f(r) \rangle = \int \psi^*(r) \cdot f(r) \cdot \psi(r) dr$$

[passaggi ulteriori che includono operatore differenziale e trasformate di Fourier sulla quantità di moto per arrivare a...]

Si può concludere che per una qualsiasi grandezza fisica F che sia una somma di funzioni $F_1(r) + F_2(p)$, il valore medio nello stato $\psi(r)$ è dato dall'integrale

$$\langle F \rangle = \int \psi^*(r) \hat{F} \psi(r) dr$$

dove \hat{F} è un operatore, in generale differenziale, definito da:

$$\hat{F} = F_1(r) + F_2(-i\hbar\nabla)$$

D. Note Matematiche

Definizione di operatore

Un operatore è definito su di un insieme di funzioni da una legge che associa a ciascuna funzione dell'insieme una funzione presa dall'insieme stesso. Operatori definiti su insiemi diversi di funzioni devono essere considerati diversi.

Operatori che coinvolgono una derivazione, vengono detti *operatori differenziali*, operatori che coinvolgono una integrazione vengono detti *operatori integrali*. Gli *operatori integro-differenziali* coinvolgono entrambe le operazioni.

Un tipo di operatori integrali sono i *funzionali*. Essi associano un numero a ciascuna funzione appartenente all'insieme su cui sono definiti. Un esempio particolare di funzionale è l'integrale di sovrapposizione cioè il seguente:

$$\langle \phi | \psi \rangle = \int \phi^*(\xi) \cdot \psi(\xi) d\xi$$

in cui, per una data funzione ϕ , il numero $\langle \phi | \psi \rangle$ è un funzionale lineare delle funzioni ψ . Questo integrale è probabilmente più noto con il nome di **prodotto scalare**.

Proprietà

Gli operatori che descrivono grandezze fisiche vengono detti *osservabili* e godono di due proprietà fondamentali.

L'azione di un operatore osservabile su di una funzione d'onda non può violare il principio di sovrapposizione. Affinché questo non accada occorre che l'operatore sia lineare:

$$\hat{F}(a\psi_1 + b\psi_2) = a\hat{F}(\psi_1) + b\hat{F}(\psi_2)$$

Il valore medio di un operatore osservabile deve essere un numero reale. Presa una funzione d'onda $\psi + \alpha\phi$, con α numero complesso arbitrario, si ottiene:

$$\langle F \rangle = \langle \psi | \hat{F}\psi \rangle + \alpha \langle \psi | \hat{F}\phi \rangle + \alpha^* \langle \phi | \hat{F}\psi \rangle + |\alpha|^2 \langle \phi | \hat{F}\phi \rangle$$

questo deve essere un numero reale indipendentemente dal valore di α , che è arbitrario. Questo è sempre vero se e solo se il secondo ed il terzo termine sono l'uno il complesso coniugato dell'altro, ovvero

$$\langle \psi | \hat{F} \phi \rangle = \langle \phi | \hat{F} \psi \rangle^*$$

per qualsiasi coppia di funzioni ψ e ϕ . Un operatore che soddisfi quest'ultima uguaglianza è detto **hermitiano** o autoaggiunto.

Notazione Bra e Ket

Dato un operatore \hat{F} e due funzioni scelte arbitrariamente ψ e ϕ , il prodotto scalare $\langle \phi | \hat{F} \psi \rangle$ è detto **elemento di matrice**¹⁶ dell'operatore \hat{F} ; esso può essere interpretato come un elemento della matrice che si ottiene variando indipendentemente le funzioni ψ e ϕ all'interno di un dato insieme.

Un elemento di matrice di \hat{F} verrà indicato, in modo più simmetrico, come $\langle \phi | \hat{F} | \psi \rangle$.

Allo scopo di rendere più formale questa notazione, che definisce implicitamente l'operazione di integrazione tra funzioni si associa ad ogni funzione ψ il simbolo $|\psi\rangle$, chiamato **ket**: un vettore elemento di un astratto spazio vettoriale. Ad ogni ket facciamo poi corrispondere un vettore $\langle \psi |$, detto **bra**, appartenente ad uno spazio vettoriale duale al precedente.

Il bra è una rappresentazione della complessa coniugata di una funzione, pronta per essere usata in un integrale di sovrapposizione o elemento di matrice.

Il prodotto bra-ket $\langle \phi | \psi \rangle$, prodotto scalare di due vettori, corrisponde all'integrale di sovrapposizione visto in precedenza. Vale anche che $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$.

Il prodotto, a termini invertiti, di un ket per un bra $|\phi\rangle\langle \psi |$ non è un numero, ma un **operatore**: moltiplicandolo a destra per un altro ket $|\chi\rangle$ si ottiene di nuovo il ket $|\phi\rangle$ moltiplicato per il numero $\langle \psi | \chi \rangle$; moltiplicandolo invece a sinistra per un bra $\langle \chi |$ fornisce come risultato il bra $\langle \psi |$ moltiplicato per $\langle \chi | \phi \rangle$.

Proprietà

Vengono adesso introdotte alcune proprietà degli operatori (lineari), espresse nel formalismo bra-ket.

Il prodotto di un operatore \hat{F} per un ket $|\psi\rangle$ è uguale al ket associato alla funzione ottenuta dall'operazione di \hat{F} sulla funzione ψ , ovvero $\hat{F}|\psi\rangle \equiv |\hat{F}\psi\rangle$.

Un operatore \hat{F} può agire su un bra, fornendo ancora un bra: $\langle \phi | = \langle \psi | \hat{F}$, si noti come il secondo termine in questo caso non sia in generale il bra corrispondente al ket $\hat{F}|\psi\rangle$: questa operazione deriva direttamente dalla proprietà associativa della moltiplicazione.

¹⁶ F. Tarantelli, "Appunti di Chimica Teorica", <http://www.thch.unipg.it/~franc/ct/index.html>, 2007

Bibliografia

C. E. Shannon, "Communication Theory of Secrecy Systems", *Bell System Technical Journal*, vol. 28, 1949

A. Kerckhoffs, "La cryptographie militaire", *Journal des sciences militaires*, vol. IX, pp. 5–38, Gennaio 1883, pp. 161–191, Febbraio 1883.

A. Einstein, B. Podolsky, N. Rosen, "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* **47**, 777-780, 1935.

Wiesner, "Conjugate Coding", *Sigact News* 15, 1983

C.H. Bennet, G. Brassard, "Quantum cryptography: public key distribution and coin tossing", *International Conference on Computers, Systems & Signal Processing*, 1984

C.H. Bennet, F. Bessette, G. Brassard, L. Salvail, J. Smolin "Experimental Quantum cryptography", *Journal of Cryptology*, vol. 5, 1992

C.H. Bennet, G. Brassard, M. Robert "Privacy amplification by public discussion", *Siam Journal*, vol.17, 1988

A. Ekert, "Quantum Cryptography based on Bell's Theorem", *Physical Review Letters* Vol. 67, N. 6, 5 Agosto 1991

M. Rabin "How to exchange secrets with oblivious transfer" *Technical report TR-81, Aiken Computation Lab, Harvard University*, 1981

C.H. Bennet, G. Brassard, C. Crépeau M.H. Skubiszewska "Practical quantum oblivious transfer", 2 Aprile 1992

W. Diffie, M. Hellman, "New Directions in Cryptography", *IEEE Transactions on Information Theory*, Novembre 1976

P. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer”, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Novembre 1994

F. Tarantelli, “Appunti di Chimica Teorica”, <http://www.thch.unipg.it/~franc/ct/index.html>, 2007

G.C. Ghirardi, “Un’occhiata alle carte di Dio”, 2003

D. Bouwmeester, A. Ekert, A. Zeilinger “The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation”, 2005

D. Deutsch "Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer". *Proc. Roy. Soc. Lond. A400*: 97–117, 1985

D. Deutsch “The fabric of reality”, 1997

S. Singh “The code book”, 1999

W. Stallings “Crittografia e sicurezza delle reti”, 2003

B. Schneier, N. Ferguson “Crittografia Pratica”, 2005