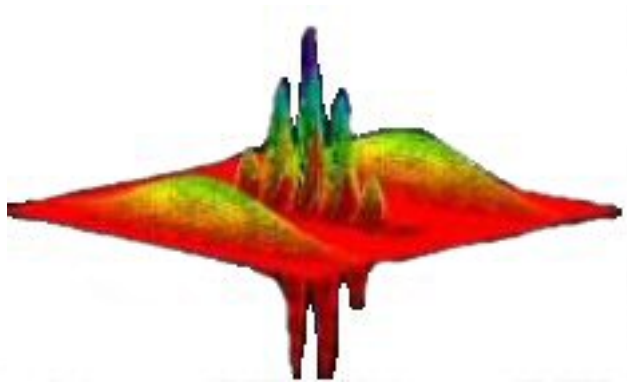
Crittografia Quantistica



Maurizio Pinzi

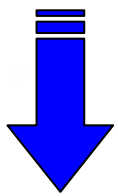
Sommario

- Introduzione
- Fisica quantistica
- Canale quantistico
- Protocollo
- Attacchi
- Oblivious Transfer
- Conclusioni

Fantascienza?!?

Idea di Calcolatore Quantistico

Potenza di calcolo teoricamente infinita



Cambiamento strategia nella crittografia attuale

Introduzione

Punti deboli crittografia classica:

- Un intercettatore “Eva” può sempre trascrivere il cifrato (eavesdropping)

Le leggi della fisica quantistica applicate alla Crittografia garantiscono:

- Perfetta sicurezza
- Certezza di non intercettazione

Idea

Principio di indeterminazione di Heisenberg:

“non è possibile conoscere simultaneamente la posizione e la velocità di una particella con precisione arbitraria ”

In parole povere …

Lo studio di un sistema quantistico in genere lo perturba

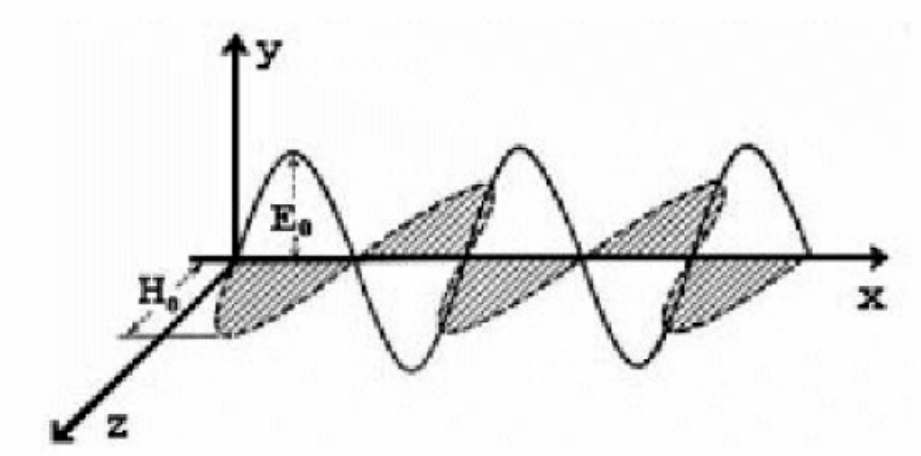
Funzionamento

Crittografia Quantistica

- Distribuzione delle chiavi (QKD)
- Canale Quantistico
- Utilizzo di fotoni
- Canale ordinario
- Messaggio crittato con One-Time-Pad

Fotone

- **Quantità discreta di energia: Fotone**
- **La polarizzazione del fotone rappresenta l'informazione associata ad esso**

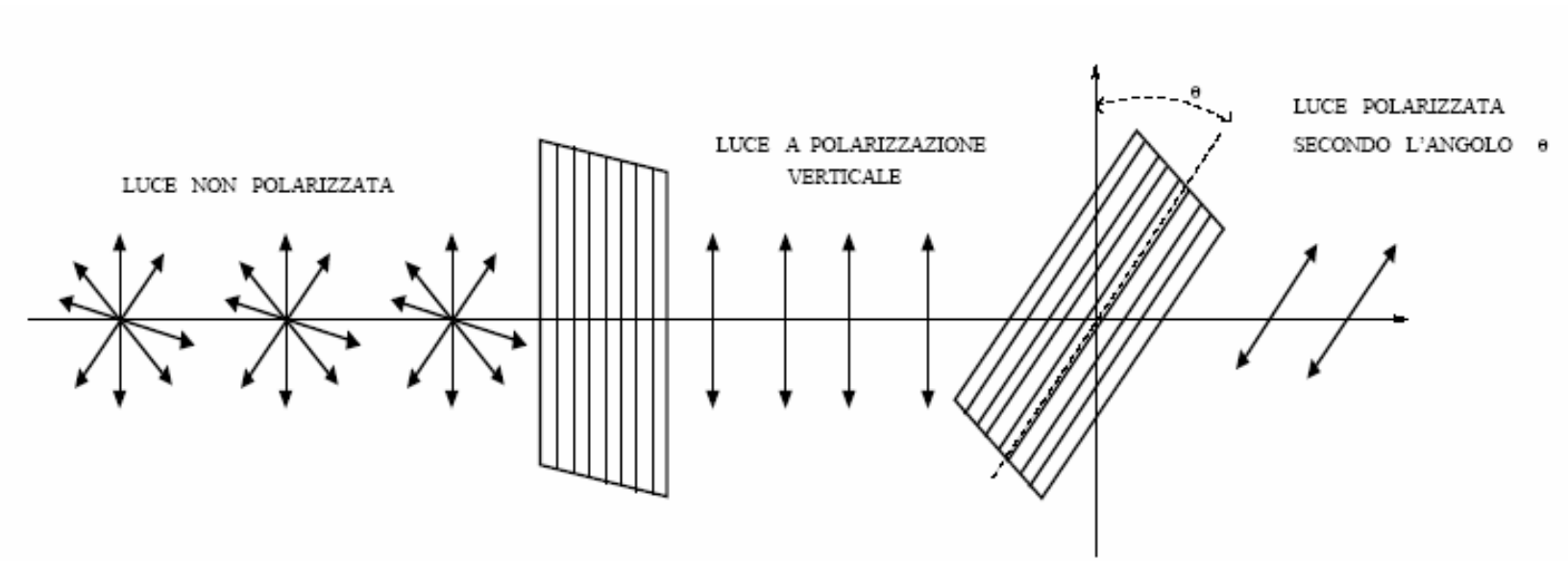


Canale Quantistico

- **Dispositivo ottico capace di produrre fotoni polarizzati**
- **Cavo su cui viaggiano i fotoni (es. Fibra Ottica)**
- **Un dispositivo ottico che permetta all'utente destinatario di misurare la polarizzazione**

Filtro

Normalmente i fotoni non sono polarizzati si utilizza quindi un θ-filter per polarizzare i fotoni secondo un angolo θ



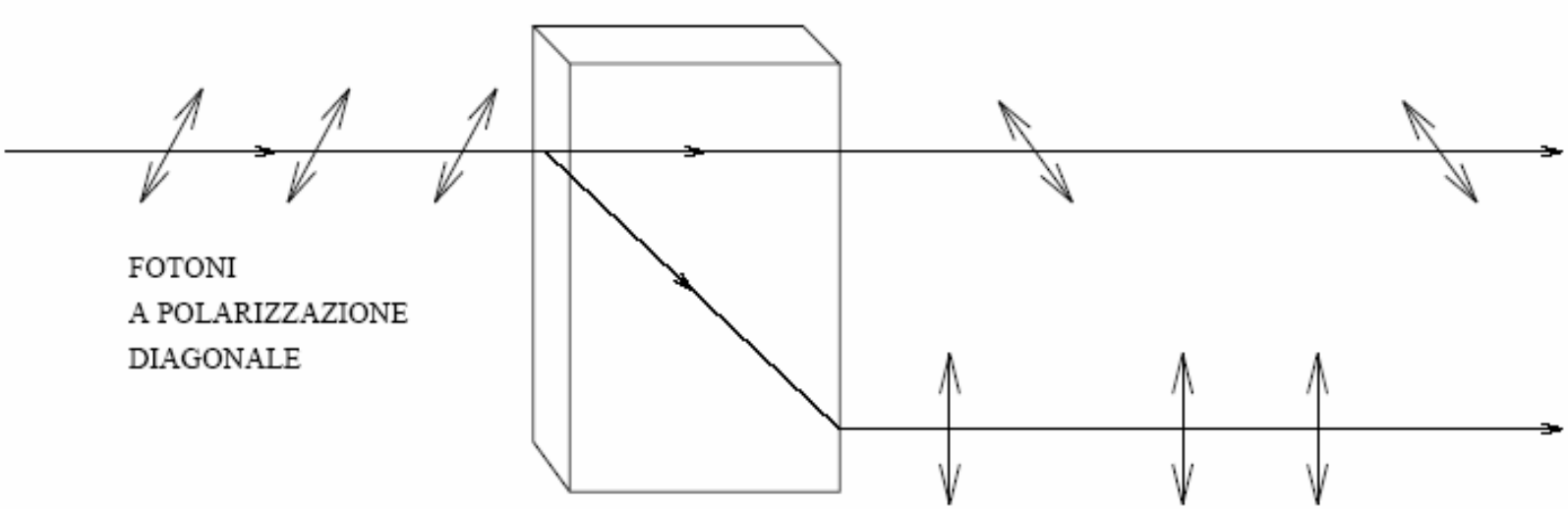
Detector(1)

Un fotone quando incontra un detector si può comportare in 3 modi a seconda della sua polarizzazione rispetto all'asse ottico del detector:

- Se il fotone è polarizzato come l'asse ottico del cristallo il fotone viene traslato.
- Se il fotone è polarizzato perpendicolarmente rispetto l'asse ottico del cristallo lo attraversa in linea retta.
- Se il fotone è polarizzato secondo qualche direzione intermedia si comporterà in modo casuale e perderà la sua polarizzazione originaria.

Detector(2)

Esempio con cristallo con asse ottico verticale:



Protocollo(1)

Canale quantistico

Scambio di una chiave tra due interlocutori

Canale ordinario

Confronto per capire se la trasmissione è stata disturbata da un origliatore

R	D	Bit
$\leftrightarrow$	$\nearrow$	0
$\updownarrow$	$\searrow$	1

Protocollo(2)

1° Passo

Alice sceglie una stringa casuale di bit ed una sequenza casuale di basi di polarizzazione (rettilinea, o diagonale) e manda a Bob una sequenza di fotoni, ognuno rappresentante un bit della stringa, nella base scelta.

2° Passo

Bob sceglie casualmente per ogni fotone mandatogli da Alice se misurare la polarizzazione rettilinea o diagonale. Così Bob ottiene dati significativi solo dal 50% dei fotoni che ha misurato supponendo che non vi siano state alterazioni dovute ad origliamento.

Protocollo(3)

3° Passo

Bob annuncia pubblicamente le basi con cui ha analizzato i fotoni.

4° Passo

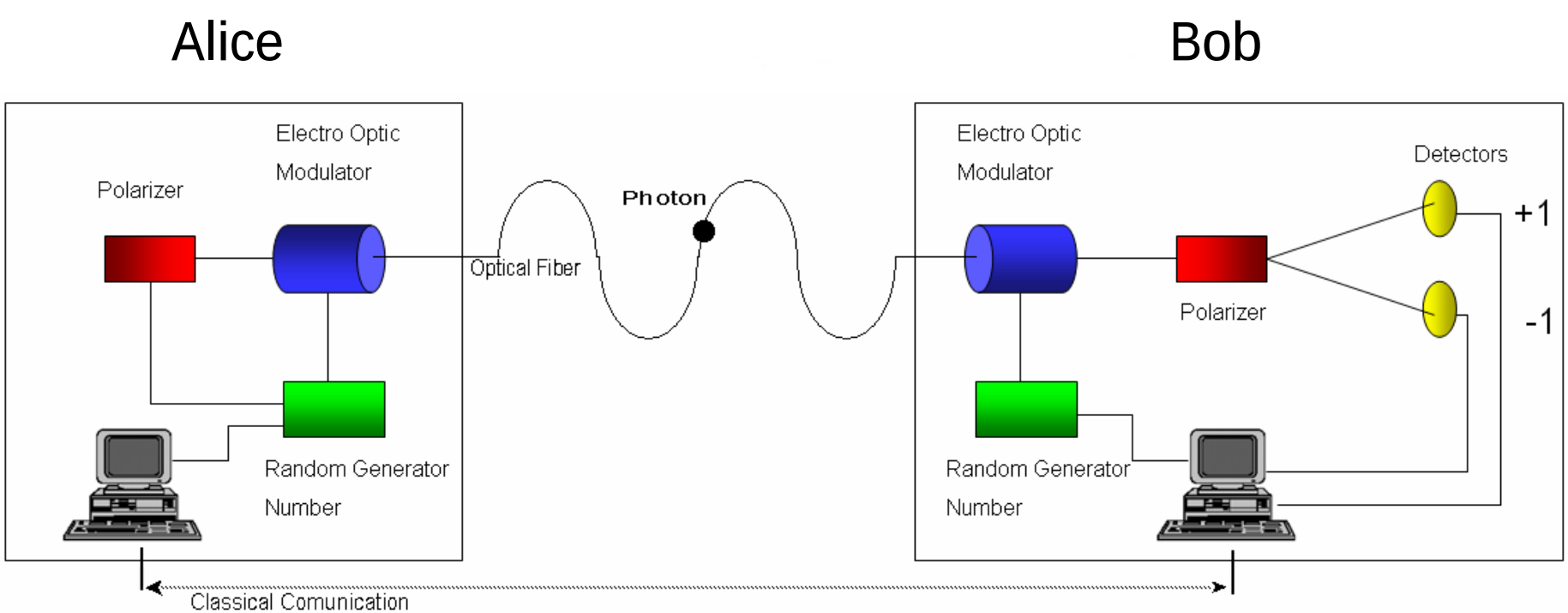
Alice comunica a Bob pubblicamente, se per ciascun fotone che egli ha ricevuto ha eseguito il tipo giusto di misurazione.

Protocollo(4)

5° Passo

Alice e Bob, per verificare se le loro risultanti stringhe di bit sono identiche confrontano pubblicamente un sottoinsieme casuale dei bit correttamente ricevuti da Bob, cioè con la base esatta. Se tutti i fotoni (o quasi) concordano, Alice e Bob possono concludere che la trasmissione quantistica. è stata libera da significativi origliamenti, per cui i rimanenti bit segreti possono costituire la chiave. Se invece vi è stato un notevole origliamento, la trasmissione è scartata e si riprova con un nuovo gruppo di fotoni.

Trasmissione



Riconciliazione

La probabilità che le 2 stringhe concordino completamente non può essere pari a 1 anche in assenza di origliamento si potrebbe quindi:

- Utilizzare un codice a correzione d'errore che introduca sufficiente ridondanza
- Confronto di parità su blocchi di dimensione fissa
- Confronto di parità su blocchi di dimensione casuale

Utilizzo funzione Hash

Attacchi

- Intercettare/Rimandare
- Divisione di Raggio

Intercettare/Rimandare

- Eva intercetta i fotoni inviati da Alice
- Eva indovina il 50% delle basi
- Eva fabbrica e manda i fotoni con la stessa polarizzazione e stessa intensità

È dimostrato che il 25% dei fotoni rimandati a Bob produrrà errori

Divisione di Raggio

- Eva con uno specchio parzialmente argentato devia una frazione f dell'intensità dell'impulso
- A Bob arriva un raggio di intensità 1-f
- Eva potrebbe memorizzare gli impulsi e misurarli solo dopo che Bob ha annunciato le sue basi pubblicamente

Non applicabile in pratica

Informazioni acquisite $\mu/2$

Oblivius Transfer(1)

Alice parte con due messaggi di due bit di sua scelta. Lo scopo del protocollo è, per Alice, trasmettere i messaggi a Bob in maniera tale che egli possa scegliere di ricevere uno di loro ma non possa ottenere informazioni significative su entrambi, mentre Alice rimane completamente ignorante di quale dei due bit Bob abbia ricevuto.
Siano, ora b0 e b1 i bit di Alice e sia, c la scelta di Bob (cioè Bob vuole ottenere bc).

1° Passo

Bob ed Alice si mettono d'accordo su dei parametri iniziali

2° Passo

Alice manda a Bob una sequenza, casuale di *2N/a* impulsi

Oblivius Transfer(2)

3° Passo

Quindi Bob riceverà con successo approssimativamente 2N impulsi, Bob non dice le basi che ha usato per misurarli né i risultati delle sue misure

4° Passo

Alice rivela a Bob le basi che ha usato per mandare ognuno degli impulsi da lui ricevuti

5° Passo

Bob partiziona, i suoi impulsi in due insiemi di N impulsi ciascuno: un *buon* insieme consistente di impulsi ricevuti nella corretta base, ed un cattivo insieme consistente di impulsi ricevuti nella base errata. Egli dice ad Alice gli indirizzi dei due insiemi ma non le dice qual'è il buono o il cattivo insieme.

Oblivius Transfer(3)

6° Passo

Alice computa un sottoinsieme casuale di parità per ogni insieme e rivela a Bob gli indirizzi definenti tali sottoinsiemi ma non le risultanti parità. A questo punto, Bob conosce una di queste parità esattamente (quella relativa al suo buon insieme), mentre non conosce niente (o quasi niente) circa l'altra parità. D'altra parte, Alice conosce entrambe le parità, ma non sa quale di queste Bob conosce. Siano x0 e x1 questi bit di parità e sia c* la conoscenza di Bob ossia xc

7° Passo

Bob dice ad Alice se c = c* o meno (notiamo che questa è la prima volta c entra in gioco nel protocollo).

8° Passo

Se c = c*, Alice manda a Bob $x0 \oplus b0$ e $x1 \oplus b1$ nell'ordine prescritto (solo ora entrano in gioco b0 e b1), altrimenti gli manda $x0 \oplus b1$ e $x1 \oplus b0$. Da queste informazioni. Bob è in grado di apprendere il suo bc

Realtà

Crittografia quantistica utilizzata per effettuare una transazione elettronica di denaro tra il municipio di Vienna ed una banca austriaca utilizzando fotoni “entangled”

- Un fotone di ogni coppia correlata è stato poi inviato dalla banca al municipio attraverso una fibra ottica. Giunti a destinazione, è stato osservato il loro stato di polarizzazione. In questo modo entrambe le estremità del collegamento avevano a disposizione lo stesso dato

I fotoni "entangled" (correlati quantisticamente) obbediscono agli strani principi della meccanica quantistica: disturbando lo stato di uno, si disturba automaticamente anche l'altro, non importa a che distanza si trovino.