Crittografia Quantistica

QKD: Quantum Key Distribution

Metro Olografix Crypto Meeting 2006
Pescara, 25 marzo 2006

Ing. Francesco Amendola - Security Consultant
www.transtecservices.com

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

Crittografia Quantistica - Definizione

"It may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve"

E.A. Poe - The Gold Bug

- **Crittografia**

κρυπτός *(nascosto)* + γραφή *(scrittura)*

- **Quantistica**

meccanica quantistica, teoria fisica moderna, basata su ipotesi di grandezze discrete *(quanti)*

Crittografia Quantistica - Definizione

- Traduzione non appropriata di *Quantum Key Distribution (QKD)*
- **QKD**

  tecnica di distribuzione sicura di chiavi crittografiche simmetriche su un canale non sicuro, utilizzando i principi della meccanica quantistica

- **Non è un algoritmo crittografico**

  si utilizza congiuntamente ad un algoritmo di cifratura della informazioni, es. *One-time-pad (OTP)*

- **OTP *(Vernam-Mauborgne 1917-18)***

  unico algoritmo matematicamente indecifrabile *(Shannon 1949)*

- **One-time-pad indecifrabile se**
  - *Lunghezza chiave = lunghezza testo*
  - *Chiave random mono-uso*
  - *Scambio sicuro della chiave*

Crittografia Quantistica

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Limiti crittografia tradizionale**
  - continua competizione tra i *code makers*, che inventano algoritmi di cifratura *(crittografia)* ed i *code breakers*, che cercano di violarli *(crittoanalisi)*
  - le intercettazioni sul canale non sono rilevabili
  - le decifratura di un messaggio richiede "solo" tempo *(Shor 1994)*

- **Distribuzione chiavi crittografiche**
  - chiave simmetrica lunga quanto il messaggio
  - chiave casuale valida una sola volta
  - ci si accorge di un eventuale intruso che origlia sul canale

- **OTP non compatibile con crittografia tradizionale**
  - occorrono chiavi realmente casuali
  - elaboratori elettronici generano chiavi pseudo-random
  - dalle correlazioni tra le chiavi è possibile identificare il messaggio in chiaro corretto

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Sicurezza assoluta nello scambio della chiave**

  chiave crittografica simmetrica scambiata in maniera sicura su un canale non sicuro

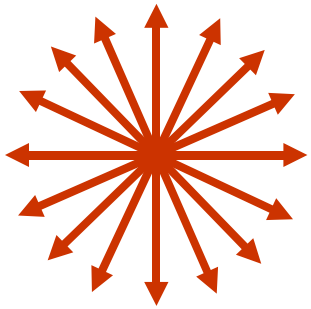
- **Sicurezza assoluta delle informazioni**

  se si utilizza la *QKD* in congiunzione ad un algoritmo *OTP* si ha la certezza matematica di non poter essere intercettati in maniera intelligibile

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Radiazione luminosa naturale**
  - Polarizzazione: direzione lungo la quale oscilla la componente elettrica dell'onda elettro-magnetica
  - Polarizzazione lineare o circolare



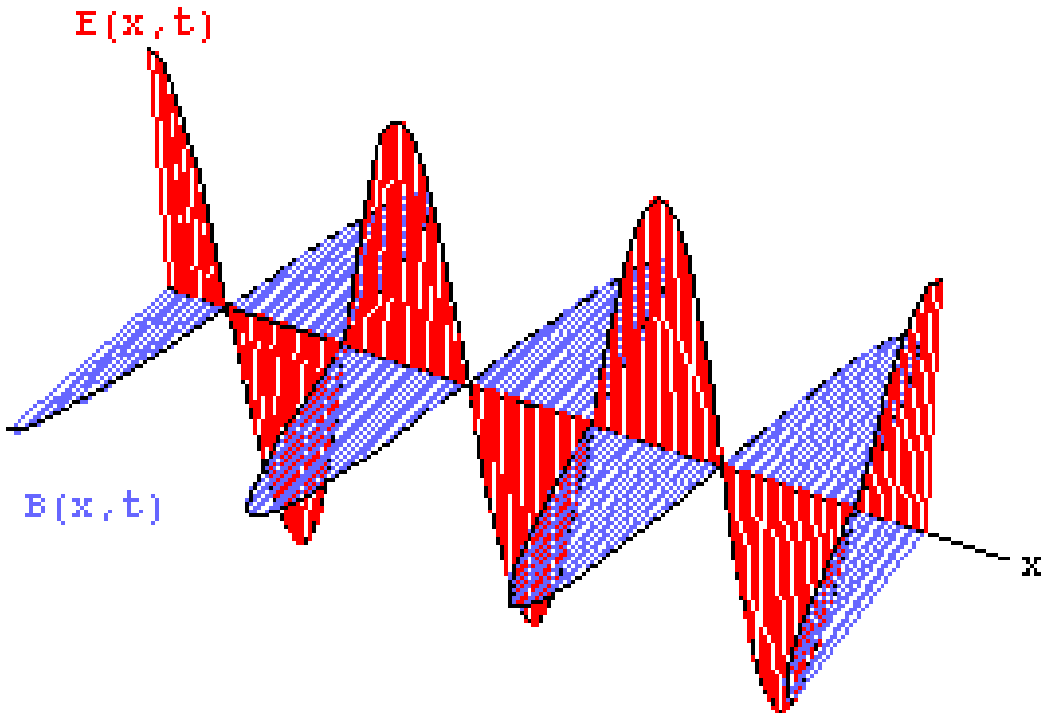
Luce non polarizzata

Luce polarizzata verticalmente

Luce polarizzata orizzontalmente

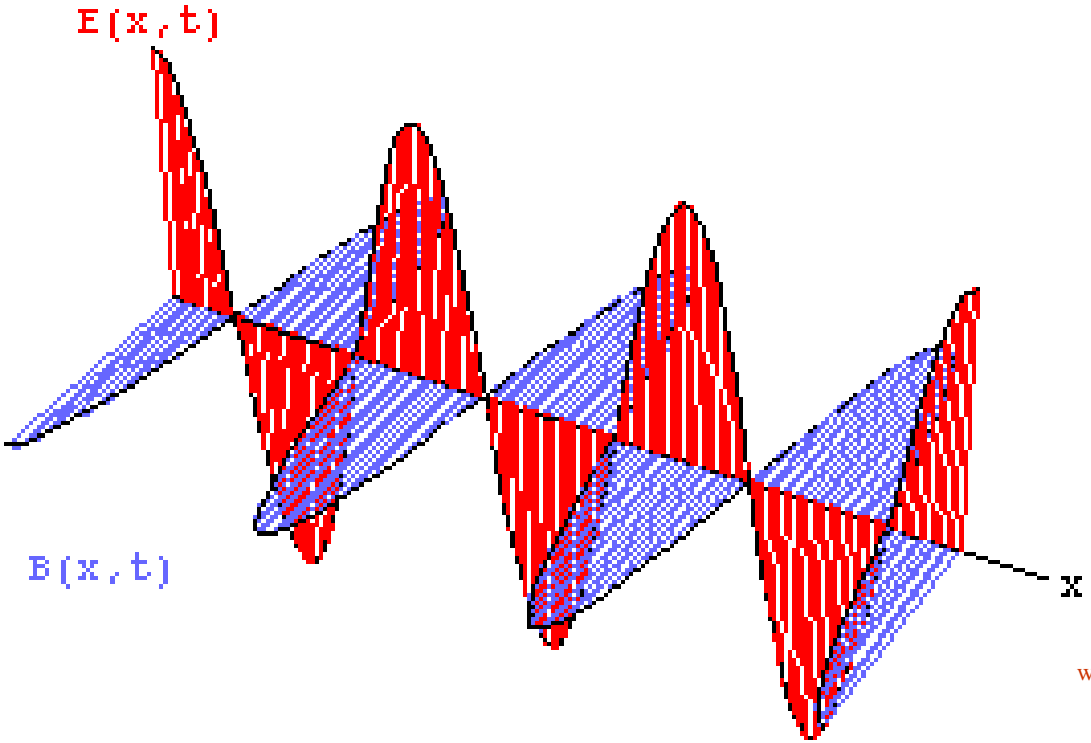
Luce polarizzata obliquamente

- **Radiazione luminosa naturale**
  - Polarizzazione lineare



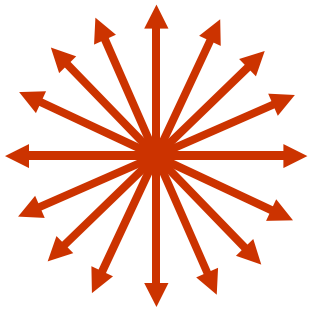
www.physics.cornell.edu

- **Radiazione luminosa naturale**
  - Polarizzazione circolare

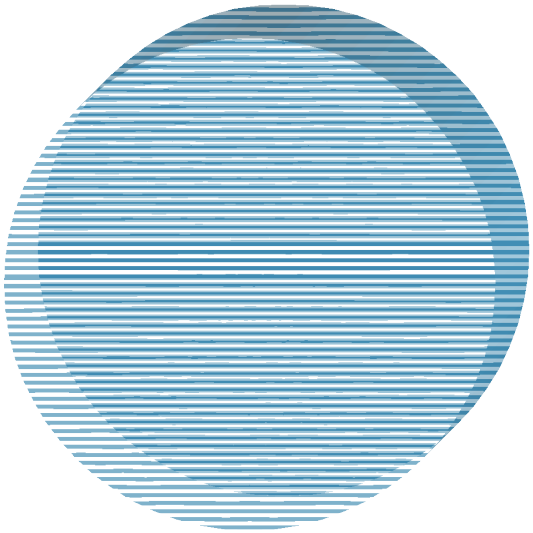


www.physics.cornell.edu

- **Radiazione luminosa naturale**
  - Filtro polarizzatore orizzontale



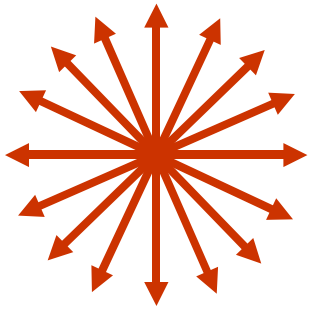
Luce non polarizzata



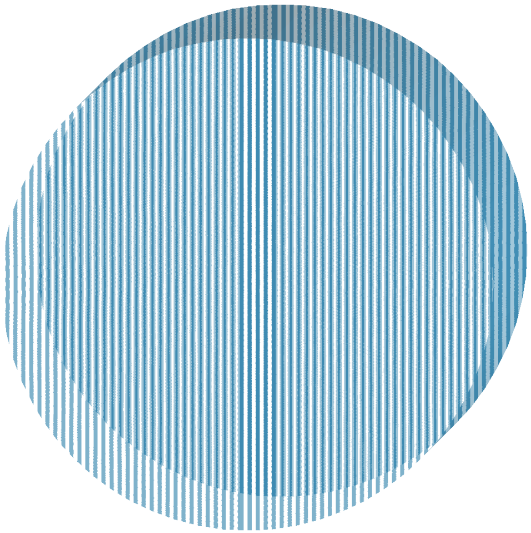
Lente polarizzata orizzontalmente

Luce polarizzata orizzontalmente

- **Radiazione luminosa naturale**
  - Filtro polarizzatore verticale



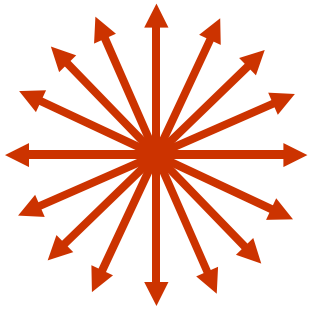
Luce non polarizzata



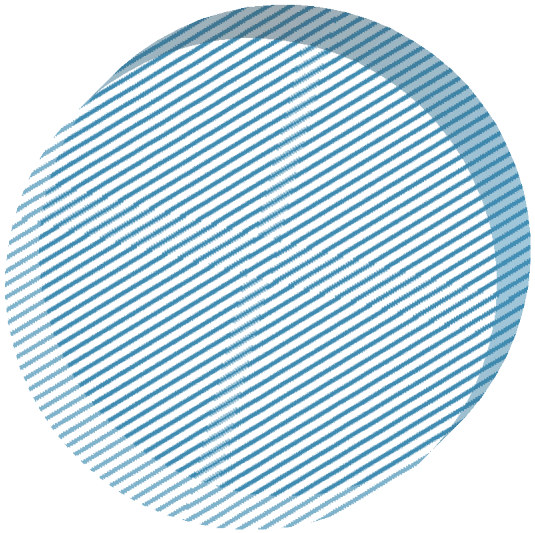
Lente polarizzata verticalmente

Luce polarizzata verticalmente

- **Radiazione luminosa naturale**
  - Filtro polarizzatore obliquo



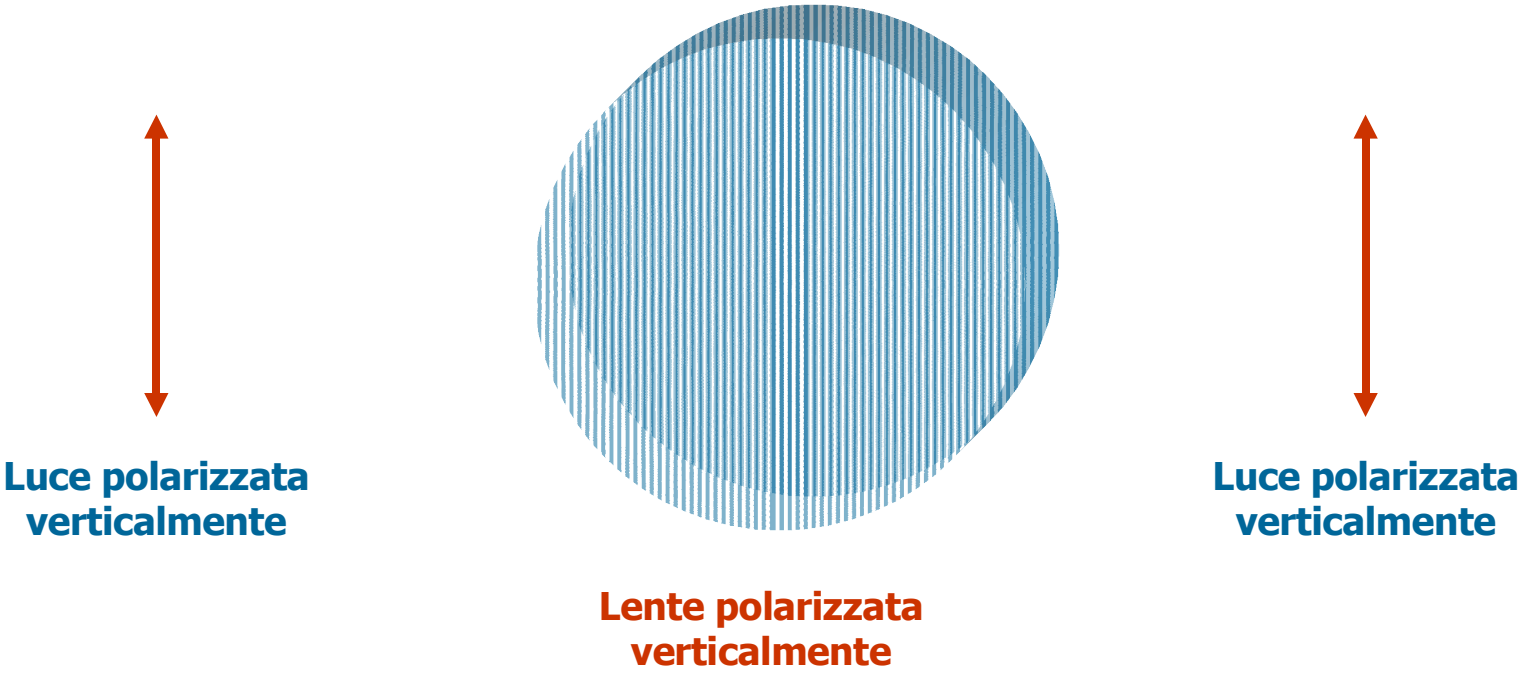
Luce non polarizzata



Lente polarizzata obliquamente

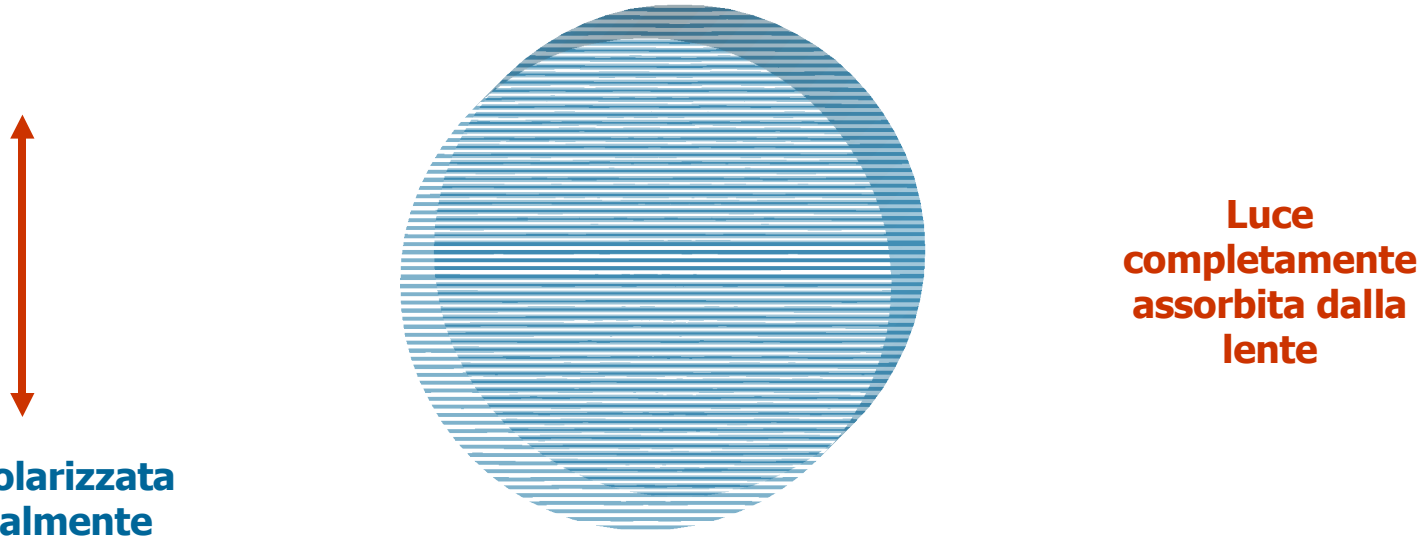
Luce polarizzata obliquamente

- **Radiazione luminosa naturale**
  - Filtro polarizzatore verticale



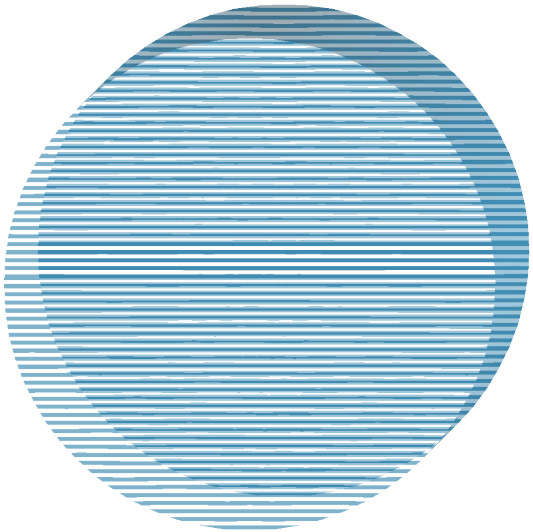
- **Quanto di luce *(fotone)***
  - Filtro polarizzatore verticale

- **Radiazione luminosa naturale**
  - Filtro polarizzatore orizzontale



- **Quanto di luce *(fotone)***
  - Filtro polarizzatore orizzontale

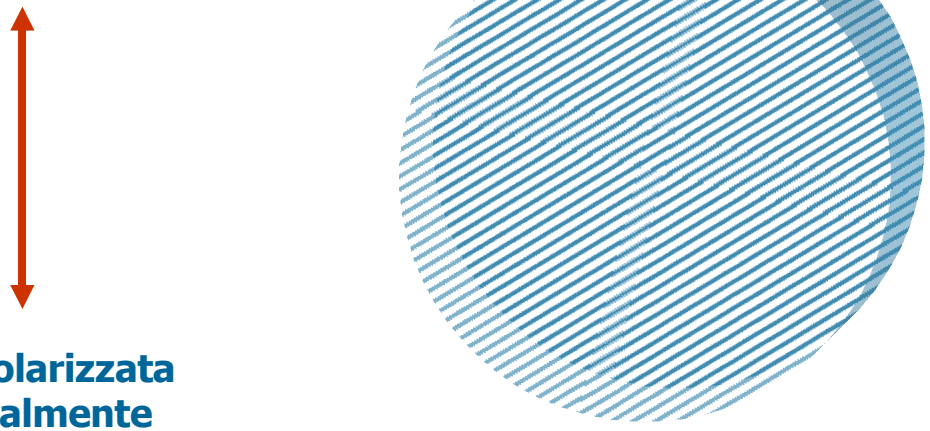
Particella polarizzata verticalmente



Lente polarizzata orizzontalmente

Particella completamente assorbita dalla lente

- **Radiazione luminosa naturale**
  - Filtro polarizzatore obliquo

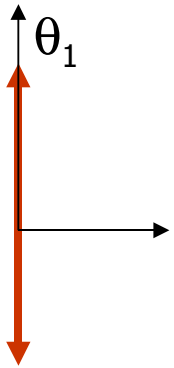


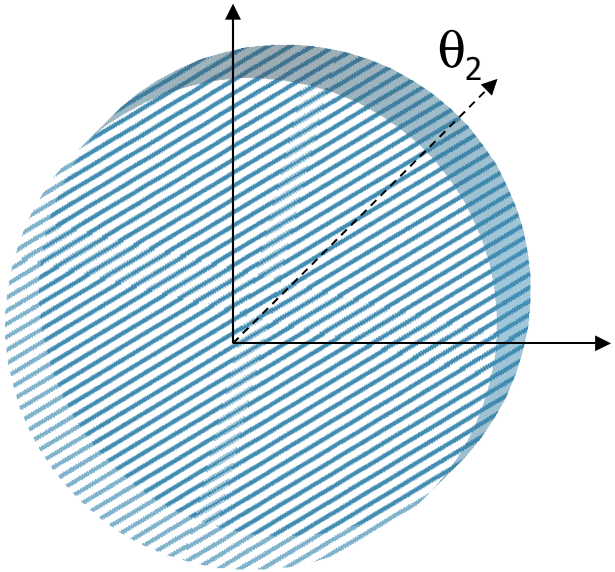
Luce polarizzata verticalmente

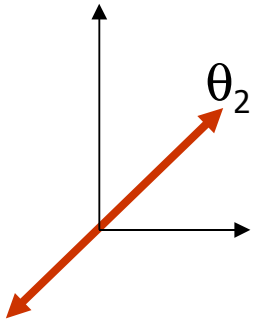
Lente polarizzata obliquamente

Cosa accade alla luce?

- **Radiazione luminosa naturale**
  - Filtro polarizzatore obliquo con luce polarizzata verticalmente







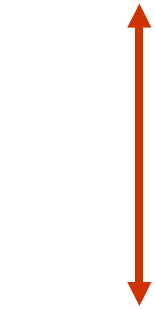
Angolo θ_1

Angolo θ_2

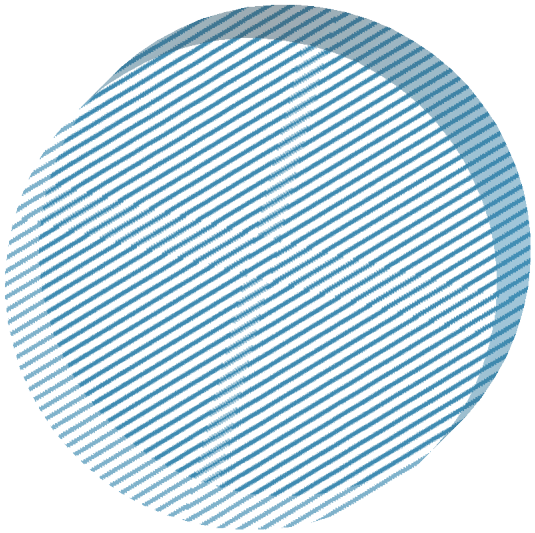
$I=I_0\cos^2(\theta_2 - \theta_1)$

Legge di Malus

- **Quanto di luce *(fotone)***
  - Filtro polarizzatore obliquo



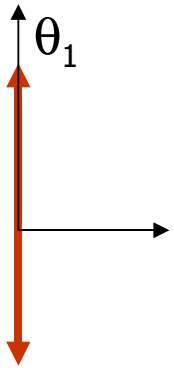
Particella polarizzata verticalmente

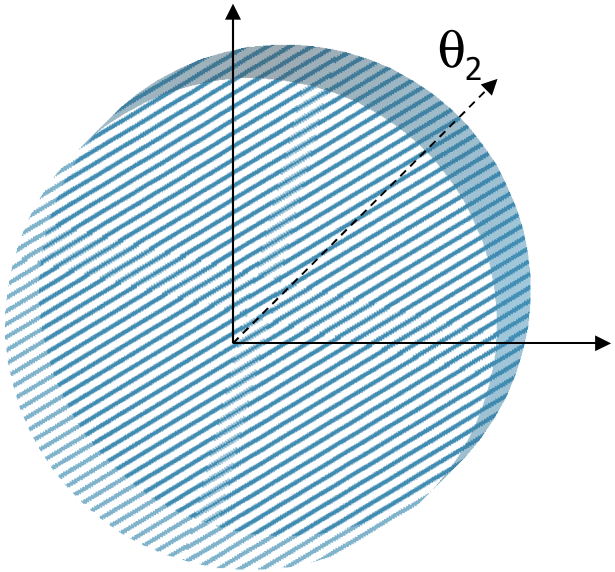


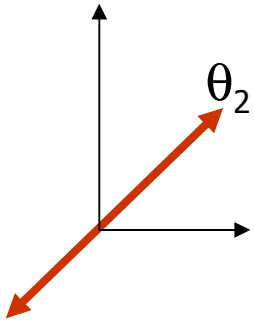
Lente polarizzata obliquamente

Cosa accade al fotone?

- **Quanto di luce *(fotone)***
  - Filtro polarizzatore obliquo con luce polarizzata verticalmente







Angolo θ_1

Angolo θ_2

$Pr(\theta_1,\theta_2) \partial \cos^2(\theta_2 - \theta_1)$

- **Quanto di luce *(fotone)***

$Pr \partial \cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕				
Fotone orizzontale $\theta_1 = 90°$ ↔				
Fotone obliquo + $\theta_1 = 45°$ ⤢				
Fotone obliquo - $\theta_1 = -45°$ ⤡				

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕	100%			
Fotone orizzontale $\theta_1 = 90°$ ↔				
Fotone obliquo + $\theta_1 = 45°$ ⤢				
Fotone obliquo - $\theta_1 = -45°$ ⤡				

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕	100%	0%		
Fotone orizzontale $\theta_1 = 90°$ ↔				
Fotone obliquo + $\theta_1 = 45°$ ⤢				
Fotone obliquo - $\theta_1 = -45°$ ⤡				

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕	100%	0%	50%	
Fotone orizzontale $\theta_1 = 90°$ ↔				
Fotone obliquo + $\theta_1 = 45°$ ↗↙				
Fotone obliquo - $\theta_1 = -45°$ ↖↘				

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕	100%	0%	50%	50%
Fotone orizzontale $\theta_1 = 90°$ ↔				
Fotone obliquo + $\theta_1 = 45°$ ⤢				
Fotone obliquo - $\theta_1 = -45°$ ⤡				

- **Quanto di luce *(fotone)***

Pr ∂ $\cos^2(\theta_2 - \theta_1)$	Pol. verticale 0°	Pol. orizzontale 90°	Pol. obliqua 45°	Pol. obliqua -45°
Fotone verticale $\theta_1 = 0°$ ↕	100%	0%	50%	50%
Fotone orizzontale $\theta_1 = 90°$ ↔	0%	100%	50%	50%
Fotone obliquo + $\theta_1 = 45°$ ⤢	50%	50%	100%	0%
Fotone obliquo - $\theta_1 = -45°$ ⤡	50%	50%	0%	100%

- **Quanto di luce *(fotone)***

Base / Valore	0	1
+		
x		

- **Quanto di luce *(fotone)***

Base / Valore	0	1
+		
x		

- **Quanto di luce *(fotone)***

Base / Valore	0	1
+		
x		

- **Quanto di luce *(fotone)***

Base / Valore	0	1
+		
x		

- **Quanto di luce *(fotone)***

Base / Valore	0	1
+		
x		

- **Principi di Meccanica Quantistica**
  - Non è possibile conoscere lo stato di polarizzazione di un fotone se non misurandolo
  - Non è possibile misurare contemporaneamente la polarizzazione con la base + e con quella x
  - Non è possibile duplicare lo stato di polarizzazione di un fotone non ancora misurato

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Protocollo BB84**
  - Charles Bennett e Gilles Brassard (1984)
  - Consente lo scambio sicuro di una chiave crittografica su un canale non sicuro, senza alcuna informazione preventivamente concordata
  - Consente di rilevare eventuali intercettazioni
  - Necessita di un canale quantistico e di uno classico

- **Protocollo BB84**
  - Mittente determina una sequenza casuale dei quattro possibili stati di polarizzazione di un fotone (0°, 90°, 45°, -45°)
  - Invia ciascun fotone sul canale quantistico, annotando la base utilizzata ed il valore di polarizzazione previsto nella sequenza
  - Ad ogni fotone inviato corrisponde una base tra + e X, nota solo al mittente

- **Protocollo BB84**
  - Destinatario misura ogni fotone ricevuto con una base scelta casualmente tra + e X, nota solo al destinatario
  - Annota, nell'ordine, le basi scelte e gli esiti delle singole misure
  - Non c'è correlazione tra la base scelta dal mittente e quella del destinatario per ogni singolo fotone

- **Protocollo BB84**
  - Probabilità del 50% che il destinatario scelga una base diversa dal mittente
  - Dopo numerosi scambi, attraverso il canale classico il mittente comunica al destinatario, nell'ordine, tutte le basi scelte
  - Non vengono comunicati i risultati delle misure, ovvero gli stati di polarizzazione dei fotoni inviati
  - Destinatario può verificare se ha scelto le basi in sintonia

- **Protocollo BB84**
  - Destinatario sa per certo che se la base scelta è la stessa di quella utilizzata dal mittente, l'esito della misura è il medesimo per entrambi
  - Passa al setaccio le basi utilizzate e scarta tutti i risultati delle misure effettuate con basi differenti da quelle scelte dal mittente, dando comunicazione a quest'ultimo circa le basi non concordi
  - I risultati della basi coincidenti formano la *sifted key*

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+
Polarizzazione del fotone inviato	1	0	1	1	0	0	1	0

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+
Polarizzazione del fotone inviato	1	0	1	1	0	0	1	0
Base scelta dal destinatario	+	+	x	+	x	x	x	+

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+
Polarizzazione del fotone inviato	1	0	1	1	0	0	1	0
Base scelta dal destinatario	+	+	x	+	x	x	x	+
Polarizzazione del fotone misurata	1	1	1	1	0	0	1	0

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+
Polarizzazione del fotone inviato	1	0	1	1	0	0	1	0
Base scelta dal destinatario	+	+	x	+	x	x	x	+
Polarizzazione del fotone misurata	1	1	1	1	0	0	1	0

- **Protocollo BB84**

Sequenza casuale	↔	↗	↔	↔	↗	↕	↘	↕
Base scelta dal mittente	+	x	+	+	x	+	x	+
Polarizzazione del fotone inviato	1	0	1	1	0	0	1	0
Base scelta dal destinatario	+	+	x	+	x	x	x	+
Polarizzazione del fotone misurata	1	1	1	1	0	0	1	0
Sifted Key	1	-	-	1	0	-	1	0

- **Protocollo BB84**
  - Dalla chiave setacciata viene estratta una sequenza casuale di bit, che viene confrontata tra mittente e destinatario tramite il canale pubblico non quantistico
  - Se vi è anche solo una discrepanza di un bit significa che, in assenza di rumore sul canale quantistico, la chiave è stato intercettata
  - Se la sottosequenza della *sifted key* coincide tra mittente e destinatario, la restante parte della chiave può essere utilizzata come chiave simmetrica sicura

- **Protocollo BB84**
  - In presenza di rumore sul canale quantistico si stima il BER (Bit Error Rate)
  - Se il BER è inferiore alla soglia massima attesa è possibile "riconciliare" la chiave, ovvero rimuovere gli errori
  - Gli errori sono considerati al pari di intercettazioni sul canale quantistico
  - Attraverso un processo di *Privacy Amplification* si perviene alla chiave finale

- **Protocollo BB84**
  - In generale, a prescindere dal rumore presente sul canale quantistico, è possibile stimare la percentuale di corrispondenza tra le informazioni inviate e quelle ricevute
  - La probabilità che mittente e destinatario scelgano la stessa base, su due disponibili, è ½ → 50%
  - La probabilità che, scegliendo basi diverse (50%), i risultati coincidano è ancora il 50%

- **Protocollo BB84**
  - Quindi la probabilità che gli esiti delle due misure coincidano è il 50% (stessa base) + 25% (base diversa, ma stesso esito), in totale il 75%
  - Se questa probabilità non viene rispettata su tutta la sequenza significa che vi è stata un'alterazione di estranei dell'informazione trasmessa sul canale quantistico

- **Protocollo Ekert91**
  - Artur Ekert (1991)
  - Parte dal paradosso EPR (*Einstein, Podolsky, Rosen 1935*), che sembrava violare i fondamenti della meccanica quantistica
  - Utilizza coppie di fotoni *entangled*, dove l'esito della misura sul primo fotone è identico a quello sul secondo, indipendentemente dalla distanza a cui si trovano i due apparati di misura

- **Protocollo Ekert91**
  - Si invia un fotone della coppia *entangled* al mittente e l'altro al destinatario
  - Ognuno misura la polarizzazione con una base scelta casualmente tra quelle concordate, mutuamente escludentesi
  - Si procede in maniera analoga al BB84, confrontando le basi scelte, poi verificando una sottosequenza degli esiti delle misure effettuate con la medesima base

- **Protocollo Ekert91**
  - È possibile utilizzare gli esiti scartati per rilevare la presenza di intrusi sul canale quantistico
  - Si ricorre alla teoria delle variabili nascoste *(LHV)* ed alla disuguaglianza di Bell *(1963)* per stimare la probabilità che la chiave trasmessa sia stata intercettata
  - Se la disuguaglianza di Bell è soddisfatta, allora la chiave quantistica è stata interecettata

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Vantaggi**
  - Sistema intrinsecamente sicuro
  - Si basa su principi della matematica e della fisica
  - La sicurezza non dipende da fattori esterni, variabili nel tempo
  - Si possono generare codici realmente casuali
  - Permette di rilevare le intrusioni sul canale

- **Svantaggi**
  - **Costo elevato (~ 100.000 euro)**
  - **Limiti sul canale quantistico**
    - **Fibra ottica**
    - **Distanza massima ~ 100 km**
  - **Limiti delle applicazioni tecnologiche, non ancora consolidate**

Crittografia Quantistica - QKD

- Definizione
- Motivazione
- Utilizzo
- Principi di funzionamento
- Protocolli di trasmissione
- Pro & Contro
- Conclusioni

- **Esempio**

- **Riferimenti bibliografici**
  - **Un' occhiata alle carte di Dio** di *G.C. Ghirardi*

    Casa editrice **Net**, edizione 2003, costo 12 euro
  - **Aspetti di Crittografia Moderna: da DES alla Crittografia Quantistica** di *Andrea Pasquinucci*

    http://www.clusit.it/download/Q01_web.pdf
  - **A Quick Glance at Quantum Cryptography** di *S.J. Lomonaco, Jr.*

    http://www.cs.umbc.edu/~lomonaco/lecturenotes/9811056.pdf

Grazie!

info@transtecservices.com
www.transtecservices.com

info@ingamendola.com
www.ingamendola.com