Università degli Studi di Cagliari

Facoltà di Scienze

Corsi di Laurea in Fisica

Tesi di Laurea Triennale

Crittografia Quantistica

Relatore: Michele Saba

Candidata: Samuela Furcas

Anno Accademico 2014/2015

Indice

I Introduzione **3**

II La crittografia **5**

1 La Crittografia tradizionale a chiave privata **7**

1.1 Principi di funzionamento 7

2 Cenni di ottica quantistica **9**

2.1 Luce coerente 9

2.2 Ottica quantistica 10

2.3 Statistica dei fotoni: la distribuzione di Poisson 11

2.3.1 Statistica iper-Poissoniana 14

2.3.2 Statistica Poissoniana 15

2.3.3 Statistica sub-Poissoniana 15

2.4 Degradazione statistica dei fotoni 17

2.5 La funzione di correlazione al secondo ordine 18

2.6 Classificazione della luce secondo la funzione di correlazione $g^{(2)}(0)$ 19

2.6.1 Bunched light 20

2.6.2 Coherent light 20

2.6.3 Antibunched light 20

3 La Crittografia quantistica **23**

3.1 Princìpi base 23

3.2 Il teorema quantistico di non clonazione 24

3.2.1 Dimostrazione del teorema quantistico di non clonazione 24

3.3 Comunicazione basata sulla misurazione degli stati di polarizzazione dei fotoni 25

3.3.1 Il protocollo BB84 27

3.3.2 Schema protocollo BB84 29

3.4 Errori nella comunicazione 30

3.4.1 Cancellazione random di fotoni 30
3.4.2 Birifrangenza 30
3.4.3 Rivelazione di conteggi al buio 31
3.5 L'importanza della sorgente di singolo fotone 31
3.5.1 Sorgenti di singoli fotoni 32

4 Dimostrazioni pratiche della crittografia quantistica 33
4.1 Dimostrazione nello spazio libero 33
4.1.1 Schema dell'esperimento 33
4.1.2 Principali fonti di errore riscontrate 34
4.2 Dimostrazione in fibra ottica 34
4.2.1 Vantaggi e svantaggi rispetto allo spazio libero . . . 34
4.2.2 Codifica della fase ottica 35
4.3 Applicazioni industriali 36
4.3.1 Impieghi odierni della crittografia quantistica 36
4.3.2 Ricerca e sfide tecnologiche 38

III Conclusioni 40

Parte I

Introduzione

Uno dei settori in costante crescita mondiale è quello delle telecomunicazioni, in particolare della comunicazione internet, che dalla sua nascita sta avendo uno sviluppo sempre maggiore. Internet è entrato a far parte sempre più della vita quotidiana ma svolge ruoli fondamentali anche per scopi governativi e militari.

Al giorno d'oggi si stima che un terzo della popolazione mondiale abbia un accesso a internet, in forte crescita è il traffico internet nei *cloud web storage* (che presto surclasseranno i dispositivi di massa tradizionali), attualmente di circa *2 zettabyte all'anno,* e che è previsto diventi di *8 zettabyte* all'anno entro il 2019[1], così come l'*internet delle cose* (Internet of Everything) che connette persone, processi e cose, che si prevede avrà un impatto sempre maggiore nella crescita del traffico dati.

Tuttavia, la crescita e la richiesta sempre maggiore dei servizi di telecomunicazione sono accompagnati dal problema della *sicurezza dei dati,* sia nel loro stoccaggio che nel trasferimento. Attualmente lo schema di codifica per la sicurezza in internet più utilizzato è quello *RSA*, che ha il suo punto di forza sulla difficoltà di fattorizzare grandi numeri interi, ma tale problema di fattorizzazione, vista la sempre maggiore crescita anche nell'efficienza e nelle capacità di calcolo dei computer, potrebbe in futuro essere risolto in tempi relativamente brevi da rendere la codifica RSA obsoleta.

La *crittografia quantistica* sfrutta le proprietà della meccanica quantistica per introdurre il vantaggio di scoprire se una certa trasmissione di dati stia avvenendo in maniera sicura, un'assoluta novità rispetto alla crittografia tradizionale.

Nel corso della tesi si analizzeranno i fondamenti fisici di tale metodo di codifica, il suo schema di funzionamento, e le implementazioni pratiche che si hanno al giorno d'oggi. Il primo capitolo è dedicato alla crittografia tradizionale, che garantisce la sicurezza nella maggior parte dei sistemi in-

[1] fonte http://www.cisco.com

formatici, nel secondo si espongono tutti i concetti di ottica necessari alla comprensione dell'elaborato, nonché alla base della crittografia quantistica; nel terzo capitolo si giunge al tema centrale oggetto della tesi, mentre nel quarto, e ultimo, si tratta delle applicazioni attuali di questo tipo di codifica e delle sfide tecnologiche in tale campo.

Parte II

La crittografia

Capitolo 1

1 La Crittografia tradizionale a chiave privata

Il termine *crittografia* ha la sua etimologia nel greco antico, da $\kappa\rho\upsilon\pi\tau o\varsigma$, *nascosto*, e $\gamma\rho\alpha\varphi\iota\alpha$, *scrittura*, e può essere definita come l'arte di codificare un messaggio in maniera tale che, nonostante esso sia visibile da chiunque, risulti comprensibile solo da chi è autorizzato. Lo scopo è dunque quello di trasmettere in sicurezza dei dati segreti o confidenziali.

1.1 Principi di funzionamento

Mittente e ricevente condividono un codice comune chiamato *chiave,* che è costituita da una sequenza di cifre binarie lunga quanto il messaggio stesso.

Il testo del messaggio da cifrare, tramite un certo algoritmo precendentemente concordato, è tradotto in una stringa binaria, e cui è aggiunta la chiave tramite l'operatore logico XOR *(exclusive or)*; quest'ultima stringa che si ottiene costituisce il testo cifrato. In linea di principio quindi solo il ricevente, che si suppone sia l'unico a in possesso della chiave, è in grado di decodificare il messaggio.

Il punto di debolezza della crittografia a chiave privata sta però nel fatto che non c'è modo di sapere con certezza se una terza parte, oltre il mittente e il ricevente, sia riuscita ad ottenere una copia del messaggio, ovvero che sia avvenuta una *intercettezione*. Oltretutto l'intercettatore potrebbe avere a disposizione team di criptoanalisti o un computer potente in grado di decodificare il messaggio.

Un metodo che potrebbe ridurre questa debolezza è quello di usare uno schema di codificazione detto ONE-TIME-PAD, che consiste nel fatto che si utilizzi una nuova chiave, creata in maniera random, per ogni nuovo messaggio che il mittente e il ricevente si scambiano. Questo metodo è considerato sicuro ma poco pratico, in quanto mittente e ricevente devono, di volta in volta, condivere la chiave in maniera sicura. Una maniera sicura per lo

scambio della chiave potrebbe essere un incontro privato tra i due comunicanti, che utilizzano poi la chiave sino al successivo incontro, ma espone il messaggio cifrato ai rischi di un eventuale intercettazione.

Un'altra maniera sicura di trasmettere la chiave sarebbe l'utilizzo di una *chiave pubblica di cifratura*. La chiave pubblica di cifratura è composta da altre due chiavi: una *pubblica* e una *privata.* Uno dei due utilizzatori genera la chiave privata, che viene utilizzata per creare la chiave pubblica. La chiave pubblica viene trasmessa apertamente tramite un canale pubblico (per esempio una linea telefonica) e viene utilizzata per decodificare il messaggio. Il messaggio nonstante sia codificato tramite una chiave pubblica può essere codificato agevolmente solo da chi è in possesso della chiave privata.

Un noto esempio di codifica con chiave pubblica è costituito dalla codifica RSA, utilizzata per la sicurezza dei dati trasmessi tramite internet. In questo caso la chiave pubblica è costiuita dal prodotto di due grandi numeri primi che comprendono la chiave privata. La decodificazione non può avvenire quindi se non sono noti questi due grandi numeri primi, e loro scoperta da parte di in un intercettatore è un'operazione di discreta difficoltà, in quanto non si conosce (ancora) alcun algortimo per la fattorizzazione di grandi interi in numeri primi.

Si è visto quindi come la crittografia classica per essere sicura necessiti di una chiave privata che debba essere trasmessa tra i due utilizzatori in maniera perfettamente sicura. La tramissione sicura però non sempre è possibile o comunque non pratica (basti pensare a due interlocutori molto distanti che non possono incontrarsi), e l'uso invece di una chiave pubblica diminuisce la sicurezza della codificazione. Da ciò nasce l'esigenza di sviluppare la crittografia quantistica, che permette di rilevare l'attività di un eventuale intercettatore.

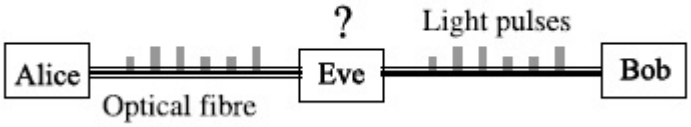

Figura 1.1: Schema di una telecomunicazione classica. Due interlocutori, Alice e Bob, si scambiano degli impulsi luminosi, ma non c'è modo di rilevare la presenza o meno di un intercettatore Eve.

Capitolo 2

2 Cenni di ottica quantistica

2.1 Luce coerente

Le fonti luminose reali emettono luce con una frequenza ω ben definità, bensi con una frequenza angolare appartenente ad un intervallo $\Delta\omega$. Una delle conseguenza più immediate di questo fatto è che non osserviamo fenomeni di interferenza prodotti dalla luce che usiamo quotidianamente, in quanto avviene che le frange luminose per una data frequenza dell'intervallo vengano compensate dalla frange scure di un'altra frequenza dell'intevallo. La proprietà che descrive la stabilità della luce è detta *coerenza.*

La coerenza della luce può essere *temporale* o *spaziale.*

La coerenza temporale della luce quantifica l'intervallo temporale in cui la frequenza luminosa resta stabile; questo tempo è denotato dal *tempo di coerenza* τ_c. Il tempo di coerenza è definito come

$$\tau_c \approx \frac{1}{\Delta\omega}.$$

Da questa definizione appare evidente che per una luce non coerente, come la radiazione termica, la cui frequenza di oscillazione varia in un intervallo $\Delta\omega$ ampio, il tempo di coerenza è piccolo, mentre per un fascio perfettamente monocromatico, avente $\Delta\omega = 0$, il tempo di coerenza è infinito.

2.2 Ottica quantistica

In fisica classica la luce è considerata essere un'onda elettromagnetica, mentre la novità sostanziale dell'ottica quantistica è quella di considerare un fascio di luce come costituito da un *flusso di fotoni*, ovvero quanti, *particelle*, di luce. Il flusso di fotoni può essere studiato dal punto di vista statistico.

Si consideri un'esperienza di rivelazione di fotoni, dove un fascio di luce colpisce il rivelatore. Il rivelatore, che può essere costituito da un tubo fotomoltiplicatore o da un fotodiodo, è collegato a un contatore elettronico, che registra un conteggio ogni volta che il rivelatore invia un impulso elettrico; il rivelatore a sua volta emette un impulso elettrico come conseguenza della rivelazione di un fotone. In sostenza il contatore ha un funzionamento del tutto analogo al contatore di Geiger per il conteggio dei decadimenti radioattivi, di conseguenza ci si aspetta che il numero medio dei conteggi non sia costante nel tempo. In particolare il numero medio di conteggi dipende dall'intesità del fascio, ma avrà delle fluttuazioni di misura in misura.

Si voglia quindi misurare il numero dei fotoni che colpiscono il rivelatore nell'intervallo di tempo T. Il flusso dei fotoni Φ è relativo a un fascio di luce monocromatico, con impulso e intensità I. Il flusso è definito come il numero medio di fotoni che attraversano una sezione A per unità di tempo, quindi si può esprimere come

$$\Phi = \frac{I \cdot A}{\hbar\omega} = \frac{P}{\hbar\omega}$$

dove P è la potenza e $\hbar$ è la costante di Plack ridotta, $\hbar = \hbar/2\pi = 1,054571726 \times 10^{-34} J \cdot s$.

La rivelazione da parte dello strumento dipende anche dalla sua *efficienza quantica* η, definita come il rapporto tra il numero dei conteggi registrati e il numero dei fotoni incidenti. Il numero di conteggi nel tempo T è dato quindi da

$$N(T) = \eta\Phi T$$

e il tasso di conteggi nel tempo invece da

$$R = \frac{N}{T} = \eta\Phi$$

Occorre considerare inoltre che il rivelatore necessita di un certo tempo di risposta, che per il fotomoltiplicatori è dell'ordine del μs, per cui il tasso R dei conteggi ha un limite pratico dipendente dallo strumento.

Nonostante Φ sia ben definito tuttavia il numero di fotoni per piccoli intervalli di tempo sarà sempre soggetto a delle fluttuazioni, in sostanza si può parlare solo di numero medio di fotoni. Questa è un diretta conseguenza della natura quantizzata della luce.

Le fluttuazioni statistiche sono dovute al fatto che non si conosce esattamente la posizione dei fotoni all'interno del fascio e sono tanto maggiori quanto più è piccolo l'intervallo temporale che si considera.

2.3 Statistica dei fotoni: la distribuzione di Poisson

La statistica dei fotoni descrive le fluttuazioni nei conteggi. Si consideri il tipo di luce più stabile che si possa immaginare, ovvero un fascio perfettamente coerente, con frequenza angolare ωcostante , ampiezza E_0 costante, vettore d'onda $k = \omega/c$ e fase φ. L'equazione del campo elettrico di una simile onda luminosa è dato da

$$E(x,t) = E_0 sen(kx - \omega t + \varphi).$$

Un fascio simile può essere emesso da un laser ideale. L'intensità è proporzionale al quadrato di E_0,e quindi è costante nel tempo, così come è costante nel tempo il flusso Φ. Si supponga di dividere il fascio di luce in segmenti. Il numero medio $\overline{n}$ di fotoni in un segmento di lunghezza L è dato da

$$\overline{n} = \frac{\Phi L}{c}$$

dove c è la velocità della luce nel vuoto.

Si consideri il caso in cui $\overline{n}$ sia un numero intero e il segmento L venga diviso in ulteriori N segmenti di uguale lunghezza. N si assume essere abbastanza grande, in maniera tale che la probabilità $p = \overline{n}/N$ di trovare

un singolo fotone nel segmento sia molto piccola, mentre la probabilità di trovare più di un fotone sia trascurabile.

La probabilità *P(n)* di trovare n fotoni in un fascio di lunghezza L diviso in N segmenti è quella data considerando la probabilità di trovare n segmenti contenenti un fotone, e i restanti *(N-n)* non contenenti alcun fotone, in ogni possibile ordine.

Tale probabilità si calcola tramite la *distribuzione binomiale:*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

dove $\left(\begin{array}{c} n \\ k \end{array} \right)$ è il *coefficiente binomiale*: $\left(\begin{array}{c} n \\ k \end{array} \right) = \dfrac{n!}{k!(n-k)!}$.

Nel caso considerato la distribuzione si può scrivere come:

$$P(n) = \frac{N!}{n!(N-n)!} \cdot \left(\frac{\overline{n}}{N}\right)^n \cdot \left(1 - \frac{\overline{n}}{N}\right)^{N-n}.$$

La distribuzione cercata si ottiene facendo il limite $N \to \infty$.

Per risolvere più facilmente il limite si può scrivere la probabilità come:

$$P(n) = \frac{1}{n!} \cdot \left(\frac{N!}{(N-n)!N^n}\right) \cdot \overline{n}^n \cdot \left(1 - \frac{\overline{n}}{N}\right)^{N-n}.$$

Per risolvere il limite del fattore $\dfrac{N!}{(N-n)!N^n}$ posso ricordare la formula di Stirling

$\lim_{N\to\infty}(\ln N!) = N \cdot (\ln N) - N$, da cui:

$$\lim_{N\to\infty} \left[\ln \left(\frac{N!}{(N-n)!N^n} \right) \right] = 0$$

e, per le proprietà dei logaritmi

$$\lim_{N\to\infty} \left(\frac{N!}{(N-n)!N^n} \right) = 1.$$

Il fattore $\left(1 - \frac{\overline{n}}{N}\right)^{N-n}$si può riscrivere più comodamente attraverso lo sviluppo binomiale:

$$\left(1-\frac{\overline{n}}{N}\right)^{N-n}=\frac{(N-n)!}{(N-n)!}\cdot 1^{N-n}\cdot\left(-\frac{\overline{n}}{N}\right)^{0}+\frac{(N-n)!}{(N-n-1)!}\cdot 1^{N-n-1}\cdot\left(-\frac{\overline{n}}{N}\right)^{1}+...$$

ovvero:

$$\left(1-\frac{\overline{n}}{N}\right)^{N-n}=1-(N-n)\cdot\frac{\overline{n}}{N}+\frac{1}{2!}\cdot(N-n)\cdot(N-n-1)\cdot\left(\frac{\overline{n}}{N}\right)^{2}+...$$

Il limite per $N\to\infty$ di questo sviluppo è

$$1-\overline{n}+\frac{1}{2!}\cdot\overline{n}^{2}-...$$

che non è altro che lo sviluppo in serie di $e^{-\overline{n}}$.

A questo punto il limite per $N\to\infty$di *P(n)* è:

$$P(n)=\frac{1}{n!}\cdot\overline{n}\cdot e^{-n}$$

che non è altro che la *distribuzione di Poisson.*

La distribuzione di Poisson è unicamente caratterizzata dal valore medio $\overline{n}$, valore per il quale la funzione presenta il suo picco. Al crescere di $\overline{n}$ la aumenta anche la grandezza del picco.

Per tale distribuzione si trova che la varianza sia uguale al valore medio $\overline{n}$:

$$(\Delta n)^2=\overline{n}$$

e di conseguenza la deviazione standard risulta essere:

$$\Delta n=\sqrt{\overline{n}}.$$

Questo dimostra che le fluttuazioni attorno al valor medio diventanto sempre più importanti con il crescere del valor medio stesso, ma dimostra altresì che il rapporto $\Delta n/\overline{n}$ diventa sempre più piccolo al crescere di $\overline{n}$: ovvero al crescere di $\overline{n}$ la fluttuazioni sono relativamente meno importanti.

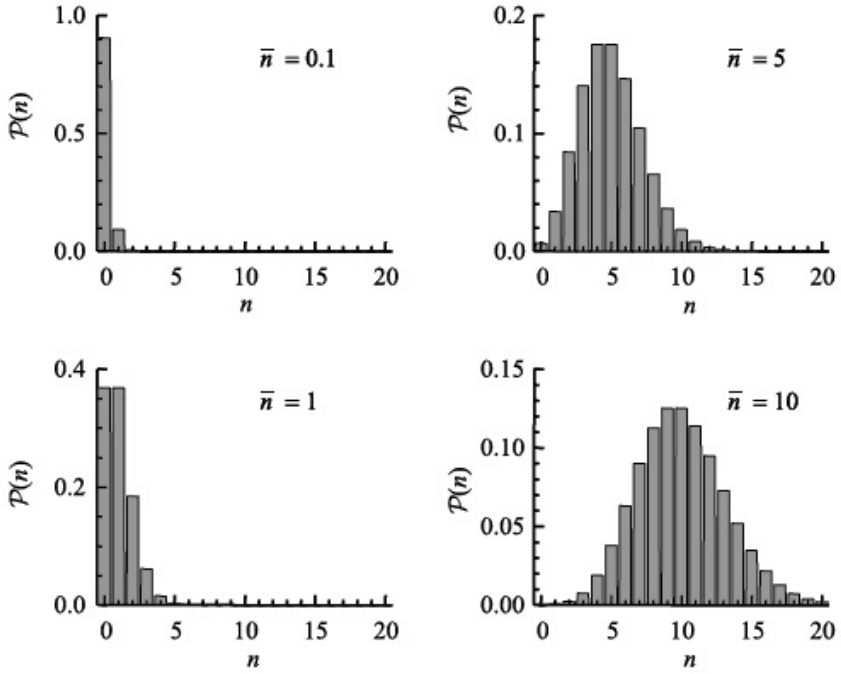

Figura 2.1: Istogrammi della distribuzione di Poisson per diversi $\overline{n}$

Posso quindi classificare tutti i fenomeni luminosi in tre categorie in base alle fluttuazioni dei conteggi.

2.3.1 Statistica iper-Poissoniana

È il caso in cui si verifica la condizione $\Delta n > \sqrt{\overline{n}}$.

Cade in questa categoria tutta la luce classica, parzialmente coerente e che abbia intentisà variabile nel tempo. Esempi di luce seguente la statistica iper-Poissoniana sono la *luce termica* e la *luce caotica*.

La *luce termica*, o radiazione di corpo nero, è descritta dalla legge di Planck, che indica la densità di energia di una radiazione di frequenza angolare compresa tra ω e $\omega+d\omega$, emessa in una cavità a temperatura T:

$$u(\omega, T)d\omega = \frac{\hbar\omega^3}{\pi^2 c^3} \frac{1}{\exp(\hbar\omega/kT) - 1} d\omega.$$

La radiazione di corpo nero può essere interpretata come uno spettro continuo di modi oscillanti, e la legge di Plank implica che l'energia della

radiazione sia quantizzata. Si può quindi considerare ogni singolo modo di oscillazione come un oscillatore armonico di frequenza angolare ω con energia quantizzata $E_n = (n + \frac{1}{2})\hbar\omega$, energia che in ottica quantistica è interpretata come n fotoni oscillanti alla frequenza angolare ω.

La *luce caotica*, o luce parzialmente coerente, è il tipo di luce che può essere prodotto da un insieme di atomi eccitati casualmente da una scarica elettrica, come avviene in una lampada a scarica. Una luce di questo tipo è detta caotica in quanto la sua intensità ha delle fluttuazioni, il cui ordine di grandezza è determinato dal tempo di coerenza. Queste fluttuazioni di intensità corrispondono a fluttuazioni nel numero di fotoni

2.3.2 Statistica Poissoniana

È il caso in cui si verifica la condizione $\Delta n = \sqrt{\overline{n}}$.

Segue questa statistica un fascio di luce perfettamente coerente e con intensità costante nel tempo, ovvero la forma più stabile di luce classica.

2.3.3 Statistica sub-Poissoniana

È il caso in cui si verifica la condizione $\Delta n < \sqrt{\overline{n}}$.

Questo tipo di luce non ha un corrispettivo nella fisica classica, e costituisce un fascio di stabilità maggiore rispetto alla luce poissoniana, perfettamente coerente. Un fascio di luce simile è costituito da un fascio di fotoni intervallati da un tempo Δt costante. Il numero dei conteggi di fotoni in un tempo T per un fascio simile sarebbe dato da:

$$N = Int\left(\eta \cdot \frac{T}{\Delta t}\right)$$

Sarebbe quindi un valore sempre intero, dipendente dall'*efficienza quantica* η, e sarebbe *uguale per ogni misura.*

Di conseguenza la deviazione standard sarebbe $\Delta n = 0$. Un fascio di fotoni con queste caratteristiche è detto *photon number state.*

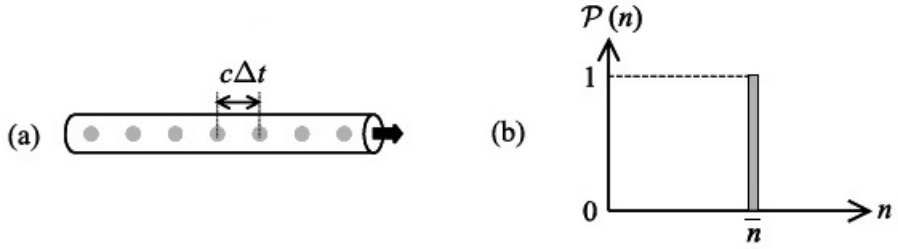

Figura 2.2: a) Schema fotoni equispaziati temporalmente in un fascio sub-Poissoniano; b) Istogramma distribuzione sub-Poissoniana

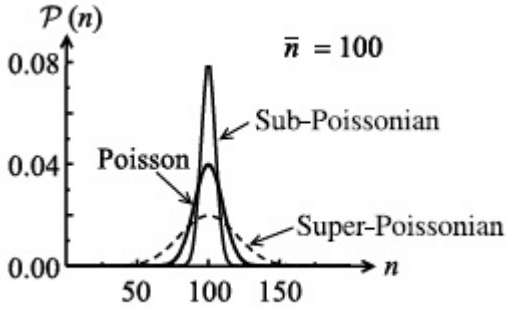

Figura 2.3: Confronto tra la statistica di probabilità di una distribuzione sub-Poissoniana, Poissoniana e iper-Poissoniana, per $\overline{n} = 100$.

2.4 Degradazione statistica dei fotoni

L'effetto di un mezzo di trasmissione T che causa la perdita di fotoni di un fascio di luce può avere la stessa interpretazione di un fascio diviso con rapporto $T : (1 - T)$. Un fascio di luce che passa attraverso un mezzo simile quindi si riduce a una frazione T del fascio originario, e va a colpire il rilevatore, che registra i conteggi.

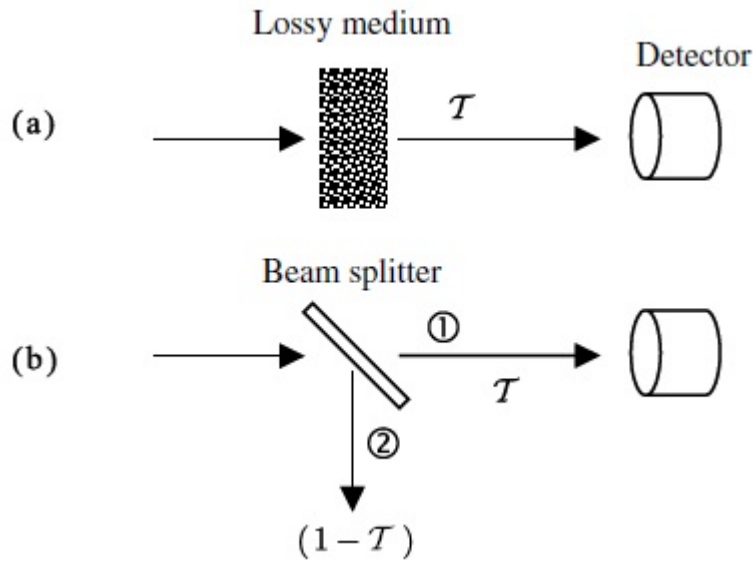

Figura 2.4: a) L'effetto che subisce un fascio di luce passante per un mezzo che ne riduce l'intensità a un fattore T è il medisimo che si osserva in un separatore di fascio descritto nell'immagine b)

Il processo di divisione del raggio avviene casualmente a livello dei singoli fotoni, ovvero il filtro seleziona casualmente i fotoni del fascio con probabilità T. La distribuzione che si ottiene da un campionamento casuale di un dato set di dati aumenta il grado di casualità della distribuzione di partenza, ovvero la presenza di filtri che operano come un campionamente casuale degrada la regolarità del flusso di fotoni.

Il modello secondo cui ogni perdita di fotoni del fascio possa essere interpretato come un fascio separato è funzionale per interpretare i diversi fattori che riducono l'efficienza degli esperimenti di fotoconteggio, come lo scatte-

ring o l'assorbimento di fotoni nelle componenti ottiche stesse o la bassa efficienza quantica.

Questi argomenti mostrano che la luce a statistica sub-Poissoniana sia facilmente suscettibile a casualizzazione della sua statistica, quindi per la produzione e rivelazione di luce con tale statistica occorre evitare accuratamente le perdite ottiche e usare rivelatori con alta efficienza quantica.

2.5 La funzione di correlazione al secondo ordine

La funzione di correlazione al secondo ordine $g^{(2)}(\tau)$ della luce è definita come

$$g^{(2)}(\tau) = \frac{\langle E^*(t)E^*(t+\tau)E(t)E(t+\tau)\rangle}{\langle E^*(t)E(t)\rangle \langle E(t+\tau)E^*(t+\tau)\rangle} = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle \langle I(t+\tau)\rangle}$$

dove E è il campo elettrico, I l'intensità e il simbolo $\langle \ldots \rangle$ indica che si è fatta la media su un grande intervallo temporale.

Se si considera una sorgente di intensità media costante nel tempo, ovvero $\langle I(t)\rangle = \langle I(t+\tau)\rangle$, allora la funzione di correlazione $g^{(2)}(\tau)$ dà informazioni sulla coerenza temporale della sorgente.

Se $\tau = 0$ la funzione di correlazione al secondo ordine diventa:

$$g^{(2)}(0) = \frac{\langle I(t)^2\rangle}{\langle I(t)\rangle^{\,2}}.$$

La scala temporale del tempo di fluttuazione si è visto dipendere dal tempo tempo di coerenza della sorgente; di conseguenza se considero un intervallo temporale $\tau \gg \tau_c$ le fluttuazione dell'intensità al tempo t e $t+\tau$ saranno completamente scorrelate tra di loro.

Si dimostra in questo caso che $\langle I(t)I(t+\tau)\rangle = \langle I(t)\rangle^{\,2}$, per cui la funzione di correlazione diventa

$$g^{(2)}(\tau) = \frac{\langle I(t)\rangle^{\,2}}{\langle I(t)\rangle^{\,2}} = 1.$$

Considerando una sorgente perfettamente monocromatica e coerente, avente quindi intensità I_0 costante, la funzione di correlazione diventa:

$$g^2(\tau) = \frac{\langle I(t)I(t+\tau)\rangle}{\langle I(t)\rangle \langle I(t+\tau)\rangle} = \frac{I_0^2}{I_0^2} = 1.$$

ovviamente per qualsiasi τ.

Si consideri infine il caso di una sorgente di intensità variabile nel tempo; in questo caso si può innanzitutto osservare che $\langle I(t)^2\rangle > \langle I(t)\rangle^2$. Segue quindi che

$$g^2(0) > 1.$$

2.6 Classificazione della luce secondo la funzione di correlazione $g^{(2)}(0)$

In base al valore che assume $g^{(2)}(0)$ posso dividere la luce in tre categorie:

- *bunched light*: $g^{(2)}(0) > 1$;
- *coherent light*: $g^{(2)}(0) = 1$;
- *antibunched light*: $g^{(2)}(0) < 1$.

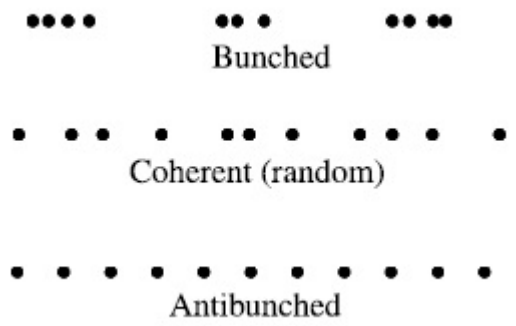

Figura 2.5: Rappresentazione grafica di *bunched light,* luce coerente, e *antibunched light*

2.6.1 Bunched light

È il tipo di luce per il quale $g^{(2)}(0) > 1$, e consiste in un flusso di fotoni nel quale i fotoni sono raggruppati a grappoli. Ciò implica che se rilaviamo un fotone ad un certo istante t, allora c'è un'alta probabilità di rilevare altri fotoni negli istanti molto vicini a t piuttosto che in quelli più distanti.

Un esempio di bunched light è la *luce caotica*, che può essere prodotta dalla scarica di una lampada. Una sorgente di luce di intensità variabile nel tempo rappresenta un esempio di *bunched light,* in quanto il numero di fotoni del fascio è proporzionale all'intensità della luce. Da ciò segue che nell'intervallo di tempo in cui l'intensità è maggiore saranno presenti più fotoni rispetto all'intervallo di tempo in cui l'intensità è minore.

2.6.2 Coherent light

È il tipo di luce per il quale $g^{(2)}(\tau) = 1$ per qualsiasi τ, e si è visto come i fotoni di tale fascio seguano la statistica Poissoniana e che i fotoni del flusso siano intervallati da tempi casuali.

Dal momento che i fotoni nel flusso sono distribuiti casualmente, saranno casuali anche le fluttuazioni dell'intensità. Si può scrivere quindi:

$$g^2(0) = \frac{\langle I(t)I(t)\rangle}{\langle I(t)\rangle \langle I(t)\rangle} \Longrightarrow \frac{\langle I(t)^2\rangle}{\langle I(t)\rangle^2} = 1.$$

Si può interpretare il risultato di $g^{(2)}(\tau) = 1$ come una manifestazione della casualità della statistica dei fotoni che la compongono.

2.6.3 Antibunched light

È il tipo di luce per il quale $g^{(2)}(0) < 1$, e consiste in un flusso nel quale i fotoni fluiscono ad intervalli regolari gli uni dagli altri.

La dimostrazione di questo risultato si può ricavare considerando l'esperimento di Hanbury Brown–Twiss. In tale esperimento un fascio di fotoni colpisce un divisore di fascio con tasso del 50%, e viene quindi diviso in due fasci di medesima intensità; i fotoni del primo fascio sono poi rilevati dalla porta D1, quelli del secondo dalla porta D2. Il rivelatore D1 è collegato al-

l'interrutore *start* di un contatore timer, che si avvia quando D1 rivela un fotone, mentre il rivelatore D2 è collegato all'interrutore *stop*, che ferma il timer quando il fotone colpisce D2.

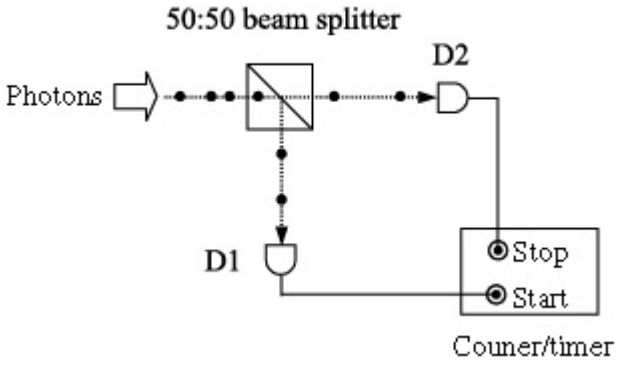

Figura 2.6: Apparato dell'esperimento HBT.

Il contatore timer quindi registra il tempo che passa tra gli impulsi rilevati da D1 e D2, e conteggia il numero degli impulsi in ogni ingresso durante tale intervallo.

Dal momento che il numero dei conteggi registrati è proporzionale all'intesità, la formula di correlazione $g^{(2)}(\tau)$ si può scrivere come:

$$g^2(\tau) = \frac{\langle n_1(t) n_2(t+\tau) \rangle}{\langle n_1(t) \rangle \langle n_2(t+\tau) \rangle}$$

dove $n_1(t)$ è il numero di conteggi registrati dal rivelatore D1 al tempo t, e $n_2(t+\tau)$ è il numero di conteggi registrati dal rivelatore D2 al tempo $t+\tau$. Questo mostra che il fattore di correlazione $g^{(2)}(\tau)$ è proporzionale, rilavato il primo fotone a $t=0$, alla probabilità di rilevare un secondo fotone a $t=\tau$. L'esperimento quindi restituisce una misura diretta di $g^{(2)}(\tau)$ della luce interpretata come composta da fotoni.

Se si suppone che la luce in esame sia costituita da un fascio di fotoni distanziati regolarmente gli uni dagli altri, questi colpiranno il divisore di fascio uno alla volta, e andranno verso D1 o D2 con uguale probabilità. Nell'istante in cui quindi viene attivato l'interrutore *start* c'è probabilità

nulla di ottenere un impulso in D2 che attiverebbe l'interrutore *stop*; questo si traduce in 0 eventi per $\tau = 0$.

Il fotone successivo che giunge al divisore di fascio ha nuovamente il 50% di probabilità di colpire ciasciuno dei due rivelatori, e se colpirà D2 fermerà il timer. In generale l'interrutore stop quindi potrebbe venire attivato dal fotone successivo, o dal secondo fotone successivo, ma mai a $\tau = 0$. Non ci si aspetta quindi alcun evento per $\tau = 0$, ma per $\tau > 0$. La media dei conteggi registrati durante l'intervallo in cui il timer è attivo è 0, ovvero $g^{(2)}(0) = 0$.

Questo è un risultato che contraddice i risultati ottenuti considerando la luce classica:

$g^{(2)}(0) \geq 1$ e $g^{(2)}(0) \geq g^{(2)}(\tau)$.

La *antinbunched light* quindi è l'unico tipo di luce dove possiamo trovare dei fotoni "isolati", e può essere prodotta quindi da una *sorgente di singolo fotone.* Un fascio di singoli fotoni è la risorsa necessaria per poter realizzare la crittografia quantistica, che verrà introdotta nel capitolo 3.

Capitolo 3

3 La Crittografia quantistica

La crittografia quantistica si è sviluppata con l'obiettivo di fornire un metodo sicuro per la trasmissione della chiave privata e sopratutto rilevare l'attività di un eventuale intercettatore.

3.1 Princìpi base

Esistono due schemi differenti su cui si può basare la crittografia quantistica: il primo si basa sulle proprietà di sovrapposizione di stati delle particelle, il secondo sulla loro misurazione quantistica. Quest'ultimo schema è quello più diffusamente utilizzato.

Supponiamo che due utilizzatori, Alice e Bob (che d'ora in poi verranno chiamati semplicemente A e B), vogliano scambiarsi delle informazioni riservate trasmettendo impulsi luminosi lungo un cavo di fibra ottica, e che l'intercettatore Eve (che d'ora in poi verrà chiamato semplicemente E) voglia ascoltare il messaggio. E dovrà avere un apparato di rivelazione che potrebbe essere costituito da un *beam splitter* e un *amplificatore ottico*, attravero i quali E riesce ad ottenere una copia del messaggio.

Se A e B stanno utilizzando la crittografia quantistica si accorgeranno quindi della presenza di E, che quindi ha ascoltato il messaggio. A e B quindi possono scartare le informazioni che sono state intercettate e riinviare una nuova chiave, sino a quando non saranno certi che la trasmissione sia avvenuta in sicurezza. Questo tipo di comunicazione può avvenire attraverso un canale pubblico.

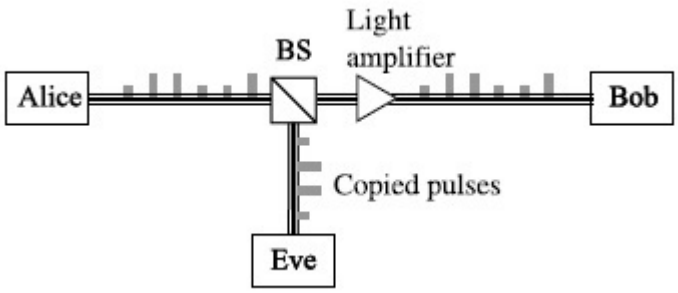

Figura 3.1: schema di comunicazione tra A e B con l'attività di un intercettatore E.

3.2 Il teorema quantistico di non clonazione

Tutto ciò può avvenire semplicemente perché non esiste una legge fisica che ci impedisca di misurare dei dati e di farne una copia esatta, ma la meccanica quantistica ci dice che non è possibile fare una misura quantistica su una particella senza che il suo stato venga alterato. Questo equivale a dire che non è possibile copiare esattamente, *clonare*, uno stato quantistico non noto a priori. Nel contesto della crittografia questo comporta il fatto che non si possibile, inviduato un certo fotone, estrerne le informazioni quantistiche e successivamennte trasmettere un altro fotone che sia una copia esatta del precedente. Questo è il motivo per cui in una codificazione quantistica l'intercettatore rivela necessariamente la sua presenza.

3.2.1 Dimostrazione del teorema quantistico di non clonazione

Siano $|\varphi\rangle$e $|\psi\rangle$due stati appartenenti a un certo spazio H che definiamo *sorgente,* e $\left|s\right\rangle$ uno stato *obiettivo* appartenente a uno spazio *H'*, dove si vogliono copiare gli stati sorgente. Tutti gli stati sono normalizzati.

Si definisce un operatore unitario U che agisce sugli stati sorgente, con la proprietà:

$$U\left(|\varphi\rangle|s\rangle\right) = |\varphi\rangle|\varphi\rangle$$

e

$$U\left(|\psi\rangle|s\rangle\right) = |\psi\rangle|\psi\rangle.$$

Si consideri il prodotto scalare tra le due relazioni, ricordando che la proprietà dell'operatore unitario è quella di conservare il prodotto scalare:

$$\left(\langle s|\langle\varphi|U^{\dagger}\right)\left(U|\psi\rangle|s\rangle\right) = \langle s|s\rangle\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle.$$

Ma se l'azione di U è quella clonare entrambi gli stati, si ha:

$$\left(\langle s|\langle\varphi|U^{\dagger}\right)\left(U|\psi\rangle|s\rangle\right) = \left(\langle\varphi|\langle\varphi|\right)\left(|\psi\rangle|\psi\rangle\right) = \left(\langle\varphi|\psi\rangle\right)^2$$

Uguagliando le due relazioni si ottiene

$$\langle\varphi|\psi\rangle = \left(\langle\varphi|\psi\rangle\right)^2.$$

Questa uguaglianza è vera solo se i due prodotti scalari sono uguali a *1* o *0*, ovvero se due stati sorgente sono identici o ortogonali tra di loro. Questo si interpreta col fatto che sia possibile clonare solo degli stati ortogonali tra di loro, mentre in tutti gli altri casi la clonazione non è possibile.

3.3 Comunicazione basata sulla misurazione degli stati di polarizzazione dei fotoni

Uno dei metodi più utilizzati nella codifica quantistica è la misurazione dello stato di polarizzazione di un singolo fotone.

L'apparato utilizzato nella comunicazione è costituito da un *divisore di fascio polarizzante (polarizing beam splitter),* che trasmette la luce polarizzata verticalmente e ruota di 90° la luce polarizzata orizzontalmente, e da due rivelatori di singoli fotoni, D_1 e D_2.

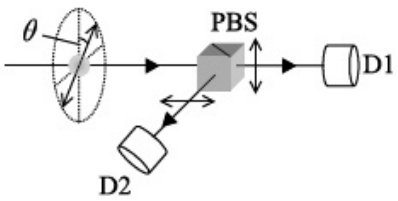

Figura 3.2: Apparato di misurazione dello stato di polarizzazione del singolo fotone

Si consideri che inizialmente il fotone sia polarizzato linearmente con un angolo ϑ rispetto alla verticale. Se $\vartheta = 0°$ il fotone codificato verrà rilevato attravero la porta D_1, mentre se $\vartheta = 90°$ il fotone verrà rilevato attraverso la porta D_2.

In tutti gli altri casi, dove il vettore di polarizzazione ha una angolo ϑ qualsiasi, questo dovrà essere scomposto nelle sue componenti orizzontale e verticale.

Gli stati quantici di polarizzazione verticale e orizzontale possono essere rappresentati rispettivamente con la notazione

$\left|\updownarrow\right\rangle$e $\left|\leftrightarrow\right\rangle$. Lo stato quantico più generale di un fotone polarizzato con un angolo ϑ può essere scritto quindi come sovrapposizione dei due stati di polarizzazione ortogonali:

$$\left|\vartheta\right\rangle = \cos\vartheta\left|\updownarrow\right\rangle + \sin\vartheta\left|\leftrightarrow\right\rangle.$$

La probabilità che il fotone passi per la porta D_1 è data da $\left|\left\langle\updownarrow\left|\vartheta\right\rangle\right|^2 = \cos^2\vartheta$.

La probabilità che il fotone passi per la porta D_2 è data da $\left|\left\langle\leftrightarrow\left|\vartheta\right\rangle\right|^2 = \sin^2\vartheta$.

Se quindi A invia un fotone codificato con una certa polarizzazione, a seconda di ϑ, B lo potrà rilevare in D_1 o D_2. L'intercettatore E è in possesso di una copia dell'apparato di A e dell'apparato rivelatore di B. Nel tentivivo di procurarsi una copia del messaggio e non essere scoperto, misura ϑ e successivamente cerca di inviare un altro fotone con lo stesso angolo di polarizzazione. Tuttavia E può sapere con precisione il valore di ϑsolo nei

casi speciali in cui l'angolo di polarizzazione è verticale o orizzontale, mentre in tutti gli altri casi E non può far altro che inviare un fotone con un angolo $\vartheta' \neq \vartheta$. Ciò comporta il fatto che B faccia le sue misure sui fotoni di angolo ϑ', con conseguente introduzione di errori nella comunicazione.

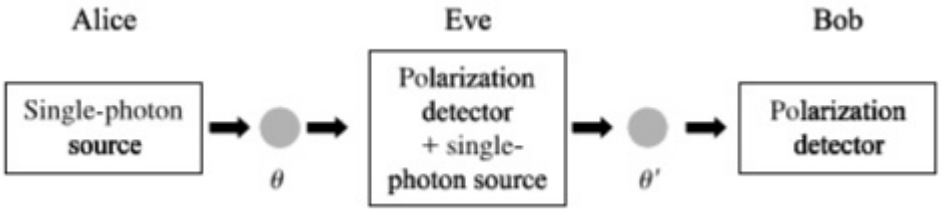

Figura 3.3: Schema della comunicazione tra A e B con la presenza di E. E prova a misurare l'angolo di polarizzazione del fotone inviato da A a B ed invia un fotone identico a quello misurato a B. E rivela però la sua presenza in quanto nel 50% dei casi invierà un fotone con un angolo di polarizzazione $\vartheta' \neq \vartheta$.

La conclusione è quella che non è possibile estrarre informazioni da un sistema quantistico senza alterarne il suo stato, per cui qualsiasi attività di intercettazione verrà sempre rilevata.

3.3.1 Il protocollo BB84

Il protocollo di Bennet e Brassard, proposto nel 1984 e noto brevemente con il nome BB84, è uno degli schemi più utilizzati per la crittografia quantistica.

Nel protocollo BB84 esistono due basi ortogonali rispetto cui poi posso essere polarizzati e rilevati i fotoni.

- base $\oplus$: le cifre binarie 1 e 0 corrispondono rispettivamente a fotoni polarizzati con angoli $\vartheta = 0°$ e $\vartheta = 90°$, che sono rappresentati dalla notazione $|\updownarrow\rangle$ e $|\leftrightarrow\rangle$;
- base $\otimes$: le cifre binarie 1 e 0 corrispondono rispettivamente a fotoni polarizzati con angoli $\vartheta = 45°$ e $\vartheta = 135°$, che sono rappresentati dalla notazione $|\nearrow\rangle$ e $|\nwarrow\rangle$.

Apparato sperimentale di Alice: è costituito da una sorgente di fotoni polarizzati verticalmente e una *Pockels cell*[2] (PC1). Tramite la PC1 A può modificare l'angolo del vettore polarizzazione dei fotoni, producendo angoli di $\vartheta = 0$, 45°, 90° o 135°, utilizzando quindi a scelta sia la base $\oplus$ che $\otimes$.

Apparto sperimentale di Bob: è costituito dal divisore di fascio polarizzante, dalla Pockels cell PC2 e dai i rivelatori di singoli fotoni D_1 e D_2. Per ogni fotone in arrivo B può scerglierne la base di rilevamento, ruotandone, tramite la PC2, l'angolo del vettore di polarizzazione di 0 o -45°, ovvero sceglie se rilevare nella base $\oplus$ o $\otimes$.

La scelta della base di rilevamento è del tutto casuale: B infatti non conosce quale sia stata la scelta di A che alla stessa maniera invia fotoni codificati secondo una base scelta casualmente. B registrerà quindi un risultato corretto solo nei casi in cui avrà scelto la stessa base scelta da A, e , dal momento che sia A che B scelgono di volta in volta la base in maniera del tutto casuale, B rileverà il risultato corretto nel 50% dei casi.

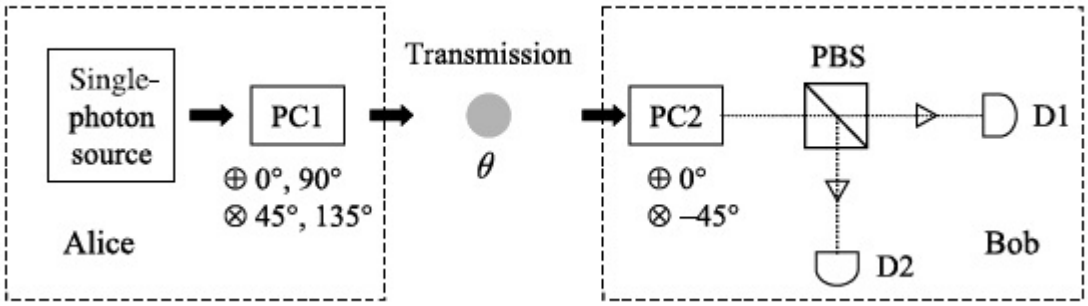

Figura 3.4: Schema della codifica dei dati secondo il protocollo BB84

[2]La Pockels cell è un dispositivo ottico in grado di ruotare il vettore di polarizzazione della luce che vi passa attraverso in maniera proporzionale al voltaggio che vi viene applicato.

3.3.2 Schema protocollo BB84

Lo schema di funzionamento del protocollo BB84 può essere sintetizzato in dei semplici passaggi:

- A codifica la sue sequenza di bit passando casualmente dalla base $\oplus$ alla base $\otimes$, poi trasmette i fotoni codificati a B con intervalli di tempo regolari e prestabiliti;
- B riceve i fotoni e registra i risultati passando casulamente dalla base di rilevamento $\oplus$ alla base $\otimes$;
- Tramite un canale pubblico B comunica ad A per ogni istante quale sia stata la sua scelta della base di riferimento;
- A confronta le sue scelte della base di riferimento con quelle effettuate da B ed individua l'insieme degli intervalli temporali in cui hanno fatto la stessa scelta. B può quindi scartare tutti i bit rilevati durante gli istanti in cui aveva scelto la base errata;
- Tramite un canale pubblico B comunica ad A una parte dei suoi bit rilevati correttamente;
- A confronta i bit ricevuti da B con i propri, e presenta l'analisi degli errori: se la media degli errori è inferiore al 25%, A deduce che non vi è stata alcuna intercettazione e che la comunicazione è avvenuta in maniera sicura.

Se fosse stato presente l'intercettatore E, anche lui durante la rilevazione avrebbe dovuto scegliere casulamente di volta in volta la base $\oplus$ o $\otimes$, con il 50% di probabilità di scegliere la base corretta. Per metà del tempo quindi E rileva effetivamente il risultato corretto ed invia a B i fotoni con la polarizzazione corretta, ma nel nell'altra metà del tempo E avrà inviato fotoni codificati casualmente.

Nel caso in cui, dall'analisi degli errori, emerga che B abbia registrato dei risultati errati anche negli intervalli temporali in cui ha scelto la base corretta, e che quindi il tasso degli errori sia maggiore del 25%, sicuramente

la comunicazione non si è svolta correttamente. I motivi sostanzialmente possono essere due: o i rivelatori e la trasmissione sono imperfetti e si sono verificati troppi errori e perdite, o è avvenuta un'intercettazione. In ogni caso le cifre trasmesse verranno comunque scartate.

3.4 Errori nella comunicazione

Si è appreso quindi che il modo in cui E manifesta la sua presenza è l'introduzione di errori nella comunicazione, anche se verranno riscontrati degli errori anche se non c'è la presenza alcun intercettatore. Gli errori non introdotti dalla presenza di E posso essere dovuti a diversi fattori come la cancellazione di fotoni, la birifrangeza del mezzo in cui i fotoni viaggiano e la rivelazioni di *conteggi al buio*.

3.4.1 Cancellazione random di fotoni

La cancellazione casuale di fotoni lungo il tragitto tra A e B comporta il fatto che all'invio di un fotone da parte di A non corrisponda alcuna ricezione da parte di B. L'eliminazione random può avvenire per diverse cause: l'assorbimento di fotoni lungo il tragitto, la collimazione insufficiente della luce (cosicché alcuni fotoni manchino il rivelatore) e l'inefficienza dei rivelatori.

Dal momento che questo tipo di errore è del tutto casuale, e colpisce qualsiasi esperimento di crittografia quantistica, si può costatare che non influisca sulla sicurezza del sistema.

3.4.2 Birifrangenza

Se il mezzo attraverso cui viaggiano i fotoni è birifrangente l'angolo di polarizzazione di essi varia con la propagazione. Di conseguenza B può registrare un risultato errato anche nel caso in cui abbia scelto la corretta base di rivelazione e non ci sia alcun intercettatore.

Questo tipo di errore è il pià grave, in quanto fisicamente produce lo stesso effetto di un intercettatore.

3.4.3 Rivelazione di conteggi al buio

L'errore dovuto alla rivelazione di conteggi al buio avviene quando B registra un conteggio che non corrisponde ad alcun fotone inviato da A In questo caso quindi B registra come conteggio quello che in realtà è il rumore termico nel fotocatodo. Anche questo tipo di errore necessita un'adeguata calibrazinoe degli apparati sperimentali.

Il risultato combinato di tutti questi errori porta a una riduzione della lunghezza della chiave privata condivisa tra A e B, in quanto occorre eliminare una porzione delle cifre selezionate, concordemente con gli algoritmi di correzione. In ogni caso la sicurezza del sistema non viene alterata, purché il tasso degli errori sia inferiore al 25%, seppur l'efficienza invece venga ridotta.

La correzione degli errori avviene tramite lo scambio tra A e B di una serie di cifre. Il numero delle cifre necessario per effettuare la correzione è tanto maggiore quanto lo è la probabilità ε che N cifre siano errate, ed è dato da

$$N_{CORREZIONE} = N \cdot [-\varepsilon \cdot log_2\varepsilon - (1-\varepsilon) \cdot log_2 \cdot (1-\varepsilon)]$$

A e B devono quindi cercare di rendere ε il più piccolo possibile, ed in ogni caso significativamente più piccolo dell'errore che introduce l'intercettatore.

3.5 L'importanza della sorgente di singolo fotone

Durante la trattazione del metodo della crittografia quantistica si è supposto che A inviasse un fotone per volta, ciò implica che la sua sorgente luce sia in grado di produrre un singolo fotone per volta. Il fatto che la sorgente di A sia una sorgente di singoli fotoni è una condizione necessaria per il corretto funzionamento della comunicazione.

Si supponga il caso in cui A invii degli impulsi contenenti ognuno 2 fotoni, con stesso vettore di polarizzazione, e che lungo il loro tragitto ci sia un intercettatore. Nel caso in cui E stia rilevando con la base errata nel 50% dei casi registrerà un fotone tramite D_1 e l'altro tramite D_2: questa sarebbe per E la prova di star usando la base errata. E potrebbe quindi

scartare questi bit nascondendo la sua attività a B. L'analisi degli errori rileverebbe la mancata rivelazione di questi due fotoni, ma la attribuirebbe a una cancellazione random. In sostanza quindi l'invio di impulsi con più di un fotone ridurrebbe i fotoni errati inviati da E , e il sistema non sarebbe più in grado di rilevarne la presenza.

3.5.1 Sorgenti di singoli fotoni

La procedura standar per la produzione di una sorgente di singolo fotone è quella di attenuare fortemente un laser. L'attenuazione può essere ottenuta con l'impiego di appositi filtri, sino a quano $\overline{n}$ sia piccolo. Tuttavia una sorgente simile produce dei fotoni che seguono la statistica di Poisson, secondo cui molti intervalli temporali non conterranno alcun fotone, una piccola parte un solo fotone e una parte molto più piccola più di un fotone. Le comuni implementazioni moderne di sorgenti di singolo fotone hanno un $\overline{n}$ =0,1.

La realizzazione di vere sorgenti di singolo fotone si basa sulle tecniche per la produzione di *antibunched light*. Una vera sorgente di singolo fotone deve essere dunque in grado di emettere esattamente un solo fotone in risposta ad un impulso, che può essere elettrico o ottico. La sorgente può essere costituita da un atomo. Una volta eccitato l'atomo questo emette una cascata di fotoni e ritorna allo stato fondamentale. Dal momento che i fotoni emessi hanno differenti lunghezze d'onda, è possibile tramite un filtro selezionare i fotoni di un particolare colore.

In modo più semplice di fare una sorgente di singolo fotone è usare come innesco della produzione del fotone un laser apposito.

Capitolo 4

4 Dimostrazioni pratiche della crittografia quantistica

La comunicazione codificata tramite la crittografia quantistica può avvenire principalmente attraverso due mezzi: tramite lo spazio libero e in fibra ottica.

4.1 Dimostrazione nello spazio libero

4.1.1 Schema dell'esperimento

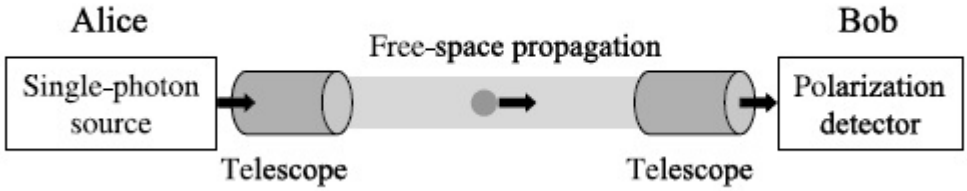

Figura 4.1: Schema comunicazione nello spazio libero

A invia dei fotoni verso B che viaggiano attraverso l'aria. A spara i suoi fotoni attraverso un telescopio, che ha la funzione di espandere, collimare e direzionare il fascio verso il rivelatore di B. Anche l'apparato ricevente di B ha un telescopio, che permette di raccogliere in maniera efficiente i fotoni. I due telescopi hanno la funzione di minimizzare gli effetti di espansione del flusso, che avviene sopratutto quando A e B sono separati da una grande distanza; in caso contrario l'espansione del flusso causerebbe una grande perdita di fotoni, che mancherebbero il rivelatore di B.

I sistemi usanti la crittografia quantistica hanno dimostrato la validità della distribuzione di chiave quantistica nello spazio libero su distanze di 10 km sia in orario diurno che notturno, mentre su una distanza di 23 km in

orario notturno. I fotoni utilizzati per tali dimostrazioni hanno lunghezza d'onda dell'intervallo 600-900 nm.

L'obiettivo a lungo termine è quello di utilizzare tale codifica per la comunicazione con i satelli nelle orbite terrestri più basse.

4.1.2 Principali fonti di errore riscontrate

- turbolenze nell'aria: causano deviazioni casuali dei fotoni. Tali effetti possono essere minimizzati inviando un impulso luminoso classico prima di ogni fotone codificato.

- luce parassita: la luce di oggetti luminosi, come il sole o delle lampade, può produrre dei conteggi errati nel rivelatori; tale effetto può essere ridotto tramite l'uso di opportuni filtri posti davanti al rivelatore oppure attivando il rivelatore solo nell'intervallo di tempo in cui è previsto l'arrivo del fotone codificato.

Occorre considerare infine che parte di questi errori può essere ricondotta a turbolenze atmosferiche che si verificano entro i primi km da terra, e che quindi non influirebbero significativamente sullo sviluppo della comunicazione con i satelliti.

4.2 Dimostrazione in fibra ottica

4.2.1 Vantaggi e svantaggi rispetto allo spazio libero

Il più importante vantaggio dell'utilizzo della fibra ottica per la codifica quantistica sta nel fatto che utilizzerebbe un mezzo della telecomunicazione standard, oltre al fatto che il fascio non è soggetto ad espansione.

Tuttavia sono presenti anche degli svantaggi rispetto ai sistemi che lavorano nello spazio libero:

- decadimento dell'intensità del segnale, dovuto alle perdite che introduce la fibra; tali perdite dipendono fortemente dalla lunghezza d'onda dell'impulso. Tipicamente i sistemi a fibra ottica lavorano con impulsi facenti parte di tre bande di lunghezza: a 850 nm, 1300 nm e 1500 nm.

I fotoni a 850 nm possono essere rilevati da un fotodiodo a valanga SPAD, rivelatore in silicio. I fotoni a 1300 nm e 1500 nm necessitano invece di rivelatori di un materiale avente gap energetico minore, come il germanio.

- birifrangenza delle fibre ottiche, che inevitabilemente rende inapplicabile la codificazione basata sullo stato di polarizzazione del fotoni. La crittografia quantistica implementata su fibra ottica quindi si basa sulla *codificazione della fase ottica*.

4.2.2 Codifica della fase ottica

La codifica della fase ottica è il tipo di codifica più idoneo per la tramissione di dei dati criptati tramite fibra ottica.

La codifica avviene tramite un interferometro di Mach-Zehnder, che cambia la fase ottica sia in A che in B Quando la fase relativa tra A e B $|\varphi_A - \varphi_B|$ è $\varphi = 0$ o $\varphi = \pi$, il fotone esce da una porta definita dalla seconda fibra accopiatrice. Questo caso è equivalente, nella codifica basata sugli stati di polarizzazione, a un fotone con angolo di polarizzazione 0°.

Se invece la fase relativa è $\varphi = \pi/2$ o $\varphi = 3\pi/2$, il fotone può uscire da entrambe le porte, con una probabilità del 50% per ognuna. Quest'ultimo caso è equivalente invece a un fotone con angolo di polarizzazione di 45°. Si nota che quindi la codifica della fase ottica è del tutto equivalente a quella dello stato di polarizzazione, e può essere quindi implementata nel protocollo BB84.

A's Bit value	ϕ_A	ϕ_B	$\lvert\phi_A - \phi_B\rvert$	B's bit value
0	0	0	0	0
0	0	$\pi/2$	$\pi/2$	0 or 1
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	0 or 1
0	$\pi/2$	0	$\pi/2$	0 or 1
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	0 or 1
1	$3\pi/2$	$\pi/2$	π	1

Figura 4.2: Tabella codifica basata sulla fase ottica

4.3 Applicazioni industriali

4.3.1 Impieghi odierni della crittografia quantistica

La crittografia quantistica ha già avuto diverse implementazioni e sono già disponibili prodotti che offrono soluzioni basate su questa tecnologia. Reti che funzionano con codifica quantistica si sono sviluppate recentemente in USA, Austria, Svizzera, Giappone e Cina.

Un'importante e massiccia struttura dove è implemenetata tale tecnologia si trova a Tokyo. È costituita da un'architettura basata su *nodi trusted*, che possono essere saparati da distanze comprsa tra 1 e 90 km. La rete è composta da tre sezioni principali: una sezione QKD, dove viene prodotta la chiave, una sezione dove essa viene gestita e una sezione dove essa viene utlizzata dagli utenti per le loro comunicazioni.

Altre recenti applicazioni della crittografia quantistica sono avvenute in Svizzera, durante le elezioni nazionali per la protezione dei conteggi dei voti, e durante la coppa del mondo FIFA in Sud Africa nel 2010.

Altre potenziali applicazioni ci possono essere nell'ambito dei backup esterni, nelle reti aziendali private, nella protezione di infrastrutture, nella protezione degli accessi delle reti ad alta sicurezza.

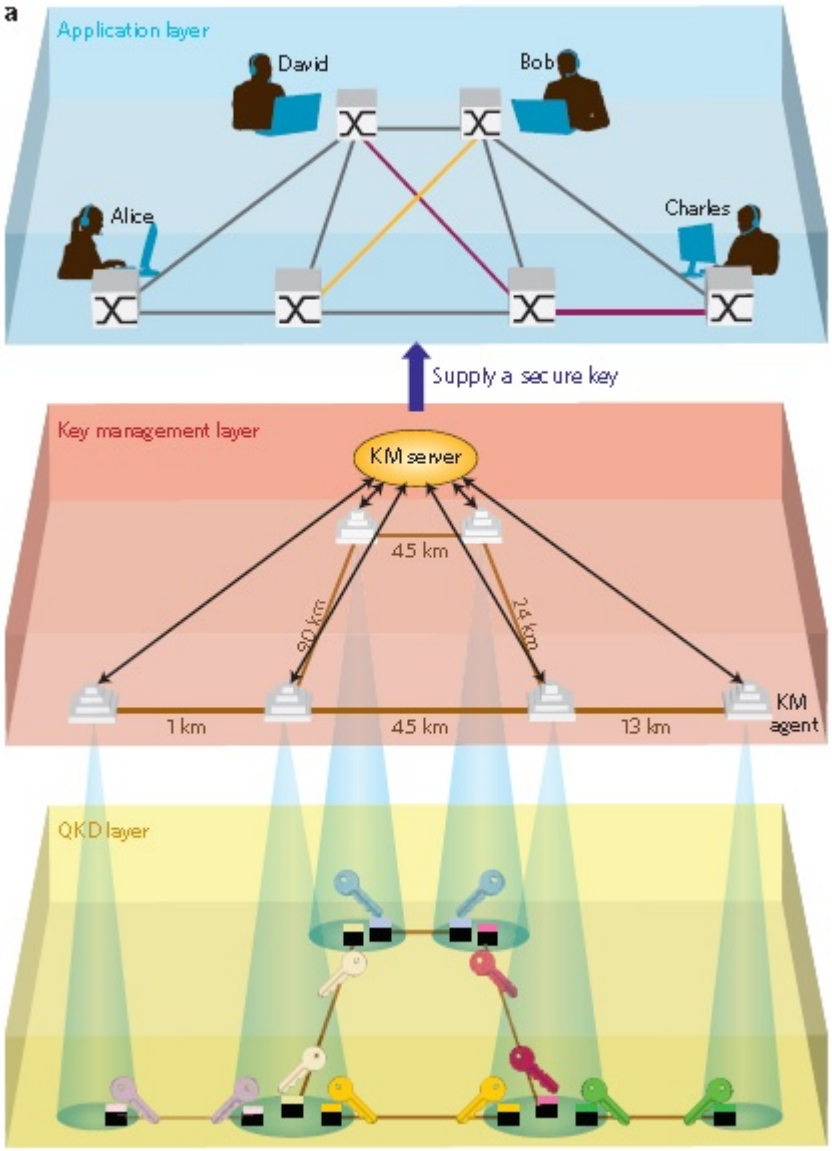

Figura 4.3: Schema della struttura della rete a sicurezza quantistica di Tokyo. Sono evidenziate le tre sezioni.

4.3.2 Ricerca e sfide tecnologiche

Attualmente la ricerca è volta alla progettazione e costruzione di sistemi di codifica quantistica ad alta velocità e sulla possibilità di far viaggiare forti segnali classici e deboli segnali quantici nella stessa fibra ottica.

Di recente sono stati condotti dei test su un dispositivo che combina due segnali quantici in un medesimo canale di comunicazione, utilizzando la divisione e moltiplicazione delle lunghezza d'onda. Come risultato sono state ottenute delle chiavi quantistiche molto stabili da parte di entrambi i segnali, su trenta giorni senza alcuna manutenzione. Questo risultato è molto promettente per l'obiettivo di far viaggiare la comunicazione quantistica sui cavi di fibra ottica utilizzati già per la comunicazione tradizionale.

Altro parametro importante da migliorare è la distanza che tale comunicazione può coprire, che per i momento è limitata a circa 350 km, a causa delle perdite di segnale che porta la fibra. Una soluzione a tale inconveniente potrebbe essere l'utilizzo di nodi trust, che potrebbero permettere una comunicazione sicura sino a distanze di oltre 10000 km. Altra soluzione potrebbe essere invece l'impiego di satelliti, che potrebbe permettere di trasportare la chiave quantistica in ogni punto del globo. Per tale implementazione è necessario innanzitutto affinare le tecniche di puntamento di precisione.

Un esperimento di questo tipo è stato eseguito nel corso del 2015 da un team italiano[3][4]. Tale esperimento ha dimostrato che lo stato di polarizzazione di un fotone si preserva efficacemente anche tramite la trasmissione su impulsi laser su satelliti in orbita ad una quota di 1000 km, che li riflettono sulla terra.

Una serie di impulsi laser, ciascuno dei quali con quattro possibili stati di polarizzazione, sono stati inviati dall'osservatorio di Matera verso cinque satelliti in orbita, equipaggiati con dei dispositivi per la riflessione del segnale. I segnali riflessi poi venivano rilevati da appositi sturmenti in laboratorio.

Solo quattro di questi satelliti erano effettivamente in grado di conservare lo stato di polarizzazione dei fotoni, tuttavia l'esperimento ha avuto successo

[3] http://journals.aps.org/prl/abstract/10.1103/PhysRevLett.115.040502

[4] http://www.lescienze.it/news/2015/07/22/news/messaggi_quantistici_comunicazioni_via_satellite-2699628/

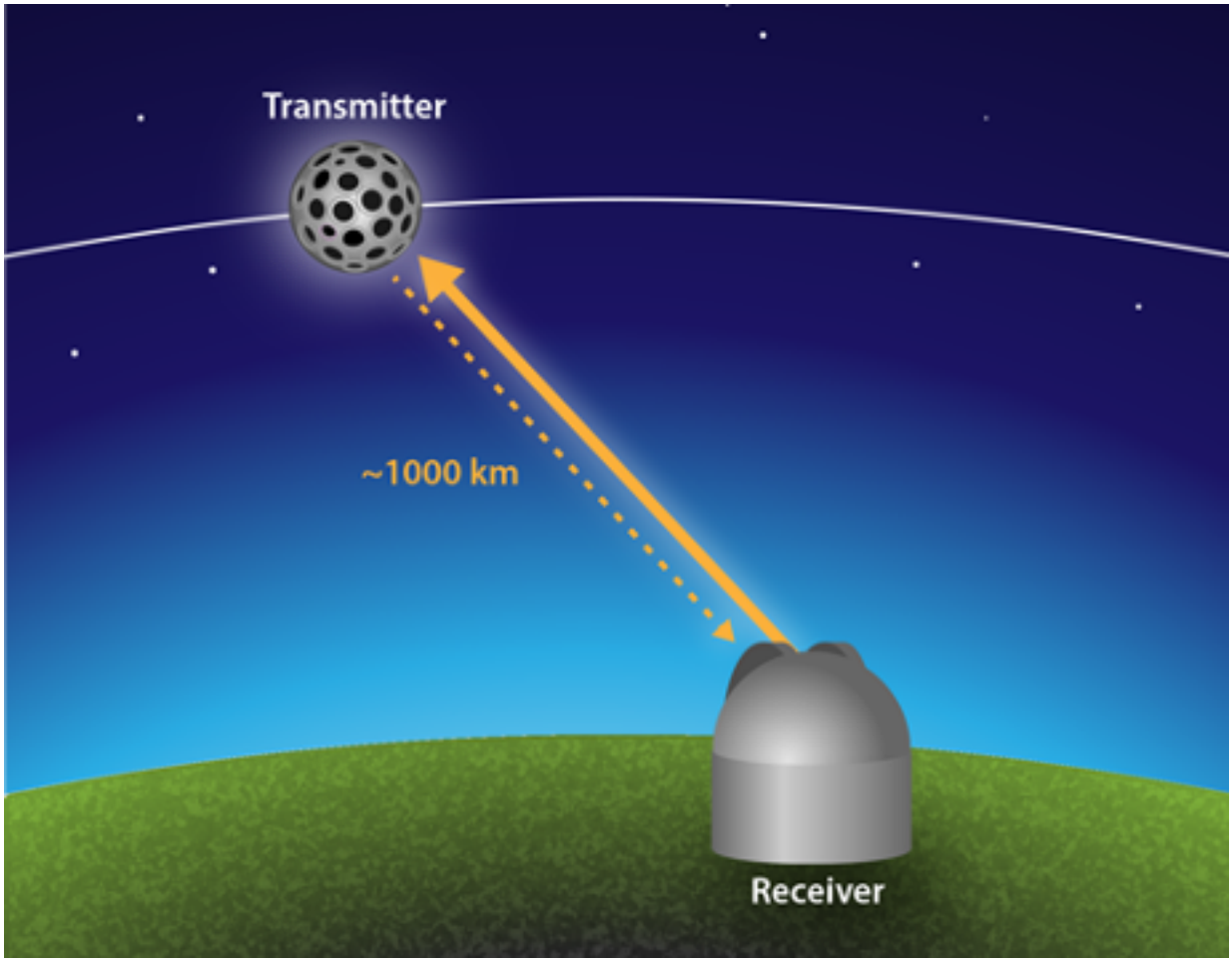

Figura 4.4: Schema dell'esperimento di comunicazione quantistica con satelliti effettuato presso l'osservatorio di Matera.

e attualmente rappresenta il caso di massima distanza a cui sia avvenuta una comunicazione quantistica.

Parte III

Conclusioni

Durante questa tesi si è cercato, oltre che di illustrare i principi fisici e il funzionamento della crittografia quantistica, anche di evidenziarne la sua importanza, sopratutto in vista della esponenziale crescita tecnologica e della richiesta di servizi di telecomunicazion e trasmissione dati in generale.

Gli esperimenti che si stanno svolgendo su questo campo sono atti al suo sviluppo sia tramite i cavi per le telecomunicazioni già esistenti che nella comunicazione satellitare, ed in entrambi i casi i risultati sono promettenti. Attualmente le implementazioni pienamente operative delle crittografia quantistica sono poche, ma le ricerche in atto hanno già evidenziato come questo nuovo tipo di codifica, non solo sia realmente realizzabile, ma sopratutto garantisca la reale sicurezza della trasmissione dei dati e del loro stoccaggio a lungo termine; infatti una codifica a chiave privata sicura al giorno d'oggi potrebbe non esserlo più in un futuro prossimo, quando si potrebbe disporre di un computer in grado di risolvere la codifica in tempi relativamente brevi.

I sistemi di sicurezza a distribuzione di chiave quantistica potranno quindi garantire la sicurezza delle informazioni di governi, organizzazioni militari, imprese commerciali, banche.

La crittografia quantistica si proprone come una branchia dell'*informatica quantistica*, che è basata sull'utilizzo dei *quanti* per l'elaborazione e memorizzazione dei dati. Le macchine che utilizzano questo tipo di informatica sono i *computer quantistici*, e sono caratterizzati da una potenza e precisione di calcolo teoricamente infiniti.

Riferimenti delle figure

1. Figura 1.1: Fig. 12.1 a) pag 247, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

2. Figura 2.1: Fig. 5.3 pag. 81, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

3. Figura 2.2: Fig. 5.6 pag. 88, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

4. Figura 2.3: Fig. 5.4 pag. 82, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

5. Figura 2.4: Fig. 5.7 pag. 88, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

6. Figura 2.5: Fig. 6.6 pag 115, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

7. Figura 2.6: Fig. 6.5 pag 114, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

8. Figura 3.1: Fig. 12.1 b) pag 247, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

9. Figura 3.2: Fig. 12.2 pag 247, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

10. Figura 3.3: Fig. 12.5 pag 254, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

11. Figura 3.4: Fig. 12.4 pag 250, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

12. Figura 4.1: Fig. 12.6 pag 257, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

13. Figura 4.2: Table 12.3 pag 260, M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

14. Figura 4.3: Figure 3 pag 598, Hoi-Kwong Lo, Marcos Curty, Kiyoshi Tamaki, *Secure Quantum Key Distribution.* Nature Photonics, 31 Luglio 2014

15. Figura 4.4: http://www.lescienze.it/images/2015/07/21/193233433-07e86daa-6808-4f97-ac3f-e9e75d7b796c.png

Bibliografia

[**1**] M. Fox, *Quantum Optics: an introduction.* Oxford University Press, 2006.

[**2**] David J. Griffiths, *Introduzione alla meccanica quantistica.* Casa Editrice Ambrosiana, 2005.

[**3**] Hoi-Kwong Lo, Marcos Curty, Kiyoshi Tamaki, *Secure quantum key distribution.* pagg 595-604, Nature Photonics, 31 Luglio 2014