UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Fisica e Astronomia "Galileo Galilei"

Dipartimento di Ingegneria dell'Informazione "DEI"

Corso di Laurea Triennale in Fisica

Tesi di Laurea

Confronto tra Protocolli di Distribuzione Quantistica di Chiave

Relatore

Prof. GIUSEPPE VALLONE

Laureando

GIUSEPPE MENEGHINI

Anno Accademico 2017/2018

Indice

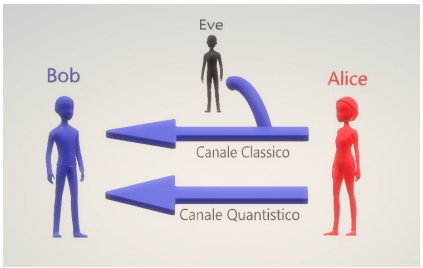
Introduzione

La crittografia è il campo di applicazioni che fornisce privacy, autenticazione e confidenzialità agli utenti. Un importante sottosettore è quello della comunicazione sicura, che si prefigge il compito di permettere la comunicazione confidenziale tra utenti, in modo tale che non sia accessibile a terzi non autorizzati. Nella crittografia classica un protocollo molto importante è il one-time-pad di Vernam, del quale Shannon prova l'ottimalità, (ovvero non può esistere una chiave più breve). Questo protocollo prevede che la chiave di crittografia sia *usa e getta*, necessita che i due utenti abbiano un modo sicuro di condividere la chiave ed essa è tanto lunga quanto il messaggio da trasmettere e crittografare. Per ovviare a questo problema al giorno d'oggi si utilizzano altre tecniche di crittografia che, seppur non ottimali e la cui sicurezza non può essere provata a priori, possono essere bypassate ma con una considerevole potenza computazionale. Questo vuol dire che all'interno dei vari protocolli ci sono dei parametri che indicano la potenza computazionale richiesta per intercettare la chiave, e questi vengono impostati in modo tale da risultare oltre le potenze di calcolo possedute ad oggi, affinchè risulti il più complicata possibile la decrittazione. In questo scenario si inserisce la nascita della crittografia quantistica, che, tramite i principi della fisica quantistica, si prefigge di risolvere il problema della distribuzione delle chiavi (Key distribution).

L'obiettivo di questa tesi è quello di confrontare direttamente due tipi di implementazioni del protocollo BB84: *P&M decoy state* e *entangled base*.

Capitolo n. 1

Quantum Key Distribution (QKD)



La QKD prevede che i due utenti autorizzati interessati a scambiarsi la chiave di decrittazione (nella letteretura chiamati convenzionalmente Alice e Bob, che in seguito, per brevità, verranno chiamati A e B) comunichino attraverso due canali, uno classico e uno quantistico. Una caratteristica che deve possedere solo canale classico è l'autenticazione dei due utenti, questo permette di garantire che un utente esterno possa intercettare le informazioni ma non possa manometterle. Il punto nell'usare i due canali è che, mentre nel canale classico un eventuale intercettatore (convenzionalmente Eva) può operare in tutti i modi possibili per carpire i dati, nel canale quantistico può agire liberamente, ma i suoi eventuali attacchi sono comunque soggetti ai principi fondamentali della meccanica quantistica.

1.1 La sicurezza della QKD

La sicurezza che si prefigge di raggiungere la QKD trova le sue fondamenta in tre "principi" della meccanica quantistica. Il primo principio è il *teorema di non-clonazione*, che afferma che uno stato quantistico sconosciuto non può essere duplicato mantenendo l'originale intatto. Un secondo aspetto importante è che, in fisica quantistica una misura di uno stato modifica lo stato del sistema misurato. Un terzo principio importante è che la correlazione quantistica ottenuta da misurazioni separate su membri di coppie entangled viola le *disuguaglianze di Bell* e non può essere create prima, da un accordo prestabilito. Il fatto che la sicurezza possa basarsi su principi generali fisici, suggerisce la possibilità

che essa sia *incondizionata*, ovvero la possibilità di riuscire a garantire sicurezza senza dover imporre alcuna restrizione sul potere dell'intercettatore. É da evidenziare infatti che *incondizionata* non va erroneamente associato ad *assoluta*. Con sicurezza assoluta infatti si intende che l'intercettatore non può in alcun modo intercettare o interrompere la comunicazione tra gli utenti. In realtà anche con i protocolli di natura quantistica nulla può prevenire che l'intercettatore agisca fisicamente sul canale di comunicazione per ostacolare la comunicazione. L'aggettivo incondizionata invece si riferisce al fatto che per studiare l'efficienza di tutti i protocolli non si pone mai un limite alle capacità tecnologiche, e quindi di calcolo, dell'intercettatore. Questo, come accennato nell'introduzione, è una delle differenze principali della QKD rispetto ai protocolli classici, che prevedono invece una sicurezza relativa alla potenza di calcolo dell'intercettatore.

1.2 La luce come mezzo per la trasmissione di informazione nel canale quantistico

In generale i processi che riguardano il campo dell'informazione quantistica possono essere implementati con qualsiasi sistema, come ad esempio ioni, atomi, luce e spin. Tuttavia per quanto riguarda il campo della QKD, e per la sua futura commercializzazione, la luce è l'unica scelta pratica. La praticità della luce risiede nella sua proprietà di non interagire facilmente con la materia, e questo significa che stati quantistici di luce possono essere trasmessi a grandi distanze senza perdere coerenza, perchè piccole perturbazioni sono già previste nella definizione del modo ottico. D'altro canto, il problema principale che comporta l'utilizzo della luce è lo scattering, ovvero le perdite: molto spesso i fotoni non arrivano a destinazione. Il modo in cui le perdite influenzano la QKD dipende dalla scelta del canale di trasmissione (di cui si parlerà nel paragrafo 1.4). Per prima cosa le perdite impongono dei limiti sul rate di produzione della chiave e sulla distanza raggiungibile. In secongo luogo le perdite possono rivelare informazioni all'intercettatore. Tuttavia la facilità d'implementazione rende questa scelta la più diffusa.

1.3 Sorgenti

1.3.1 Laser

Le sorgenti di luce più pratiche e versatili disponibili al giorno d'oggi sono i Laser, e per questa ragione sono le più utilizzate nei protocolli di QKD. Per lo scopo della tesi si ritiene necessario evidenziare che un fascio laser è descritto da uno

stato coerente di un campo elettromagnetico,

$$\left|\sqrt{\mu}e^{i\theta}\right\rangle \equiv |\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \,. \tag{1.1}$$

L'esponenziale rappresenta la fase del fascio, se tale riferimento è disponibile, altrimenti il fascio si deve descrivere da una sovrapposizione di stati,

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi} |\alpha\rangle \langle\alpha| \, dx = \sum_n P(n|\mu) |n\rangle \langle n| \,, \tag{1.2}$$

con

$$P(n|\mu) = e^{-\mu} \frac{\mu^n}{n!}. \tag{1.3}$$

Dal momento che due decomposizioni della stessa matrice di densità non possono essere distinte, si può affermare che in assenza di un riferimento per la fase, il laser produce una distribuzione poissoniana di numero di stati. La necessità di un riferimento per la fase è fondamentale per i protocolli che prevedono l'utilizzo di variabili continue e "distributed-phase-reference". D'altro canto per i protocolli che prevedono l'utilizzo di schemi a variabili discrete, tale necessità non è di alcuna importanza, ma quello che risulta rilevante è la rappresentazione dello stato come distribuzione poissoniana.

1.3.2 Sorgenti di fotoni *entangled*

Coppie di fotoni *entangled*, adatte ai protocolli che prevedono il loro utilizzo, sono per la maggior parte generate dal processo denominato *Spontaneous Parametric Down-Conversion* (SPDC). In questo processo alcuni fotoni da una pompa laser vengono convertiti in coppie di fotoni con energie minori a causa di interazioni non lineari in un cristallo ottico (come ad esempio $KNbO_3$, $LiIO_3$, $LiNbO_3$ etc). Vengono conservati sia il momento che l'energia totale. Nell'approssimazione di due modi uscenti, lo stato dei due fotoni entangled può essere descritto come segue:

$$|\psi\rangle_{\mathrm{PDC}} = \sqrt{1-\lambda^2} \sum_{n=0}^{\infty} \lambda^n |n_{\mathrm{A}}, n_{\mathrm{B}}\rangle \,, \tag{1.4}$$

dove $\lambda = \tanh \xi$, con ξ proporzionale all'ampiezza della pompa laser, e $|n_{\mathrm{A}}, n_{\mathrm{B}}\rangle$ denotano gli stati con n fotoni nei due modi differenti.

1.4 Tipologie di canale quantistico

Come si è detto per i protocolli QKD è previsto l'utilizzo di due canali, uno classico e uno quantistico. Per quanto riguarda quello quantistico, avendo l'intercettatore

piena possibilità d'azione su di esso, per caratterizzare le perdite e stabilirne la sicurezza si possono fare solo stime a posteriori. Tuttavia, conoscenze sul possibile comportamento a priori sono importanti per la progettazione del setup sperimentale. Per la luce sono usati due principali canali quantistici: la fibra ottica e lo spazio libero. Quello che caraterizza la bontà di un canale è la percentuale di perdite, dato che tutta l'informazione persa potrebbe essere raccolta, nello scenario peggiore, da un intercettatore. In particolare, siccome il segnale quantistico non può essere amplificato, il rate di produzione della chiave diminuisce con la distanza come la trasmissione del canale t. Un altro fattore che contribuisce a ridurre la distanza raggiungibile è che a un certo punto il rate di rivelazione raggiunge il livello dei dark counts dei detectors. É da evideniare che un altro possibile problema del canale potrebbe essere dovuto all'interazione dei fotoni con la materia che potrebbe comportare un effetto di decoerenza. Questo problema dipende però strettamente dai gradi di libertà che vengono usati nella scelta del mezzo di trasmissione.

Fibra ottica

Nelle fibre ottiche le perdite sono dovute a processi di scattering casuale dei fotoni, e dipendono esponenzialmente dalla lunghezza,

$$t = 10^{\frac{-\alpha l}{10}}. \tag{1.5}$$

Il valore di α dipende fortemente dalle lunghezze d'onda utilizzate, e risulta minimo nelle due *telecom windows*, ovvero attorno ai 1330 nm ($\alpha = 0.34 dB/km$) e 1550 nm ($\alpha = 0.2 dB/km$).

I canali di decoerenza e la loro importanza varia con la codifica dell'informazione. Nelle fibre ottiche sono due i principali effetti che modificano lo stato della luce. Il primo è la dispersione cromatica, in quanto frequenze diverse viaggiano a velocità differenti, che portano a una diffusione temporale incoerente del segnale luminoso. Questo potrebbe costituire un problema se si sovrapponessero impulsi successivi. Tuttavia, la dispersione cromatica è una quantità fissata per una data fibra, che può essere compensata. Il secondo, invece, consiste nella dispersione dei modi di polarizzazione. Si tratta di un effetto di birifrangenza, che produce due modi di polarizzazione uno veloce e uno lento, ortogonali, così che ogni segnale luminoso tende a splittarsi in due componenti. Questo induce una depolarizzazione del segnale. Inoltre la direzione della birifrangenza può variare nel tempo, in quanto dipende dall'apparato. Per questo motivo non può essere compensato staticamente. Nei protocolli che prevedono l'utilizzo della polarizzazione come stato quantistico per la codifica questo potrebbe diventare un problema, anche se questo dipende strettamente dalla fibra e dalla sorgente utilizzata, recenti implementazioni infatti dimostrano che è possibile stabilizzare tale effetto.

1.5 Variabili per stimare la sicurezza di un protocollo: *Secret Key Rate*

Innanzitutto bisogna definire le grandezze fondamentali in gioco. Viene chiamato con R il rate di produzione della chiave grezza, questa quantità rappresenta la lunghezza delle chiavi producibili nell'intervallo di tempo unitario. Un'altra quantità importante è rappresentata dalla *secret fraction*, indicata con la lettera r, questa quantità può essere pensata come $r = \lim_{N\to\infty} \frac{l}{n}$, dove N rappresenta il numero di bit usati per codificare la chiave, quindi il numero di segnali scambiati e misurati, n la lunghezza della chiave grezza, ovvero i bit restanti dopo la procedura di sifting, e l la lunghezza della chiave finale sicura. Il caso in cui $N \to \infty$ è chiamato caso asintotico di chiavi infinite. Date le definizioni di R e r si può definire la quantità K che rappresenta rate della chiave segreta finale: $K = Rr$.

Raw Key Rate (R)

Il Raw Key Rate dipende da due fattori: il primo è la frequenza di ripetizione, ovvero il numero di segnali che riesce a inviare la sorgente nell'intervallo di tempo, il secondo è costituito dalla probabilità che Bob legga il segnale. In formule $R = \nu_{\mathrm{s}} P_{\mathrm{Bob}}$. Per capire il primo termine dobbiamo analizzare i suoi limiti. Il primo limite è intrinseco alla scelta della sorgente ed è la frequenza massima di emissione, ovvero $\nu_{\mathrm{s}} \leq \nu_{\max}$, con $\nu_{\mathrm{s}}^{\max}$ frequenza massima raggiungibile dalla sorgente. Tuttavia sono individuabili altri due limiti. Uno derivante dal tempo morto derivante dal detector, infatti è inutile spedire più luce di quanta ne possa essere rivelata (porterebbe ad un sicuro vantaggio per l'intercettatore). Quindi, indicando con τ_{d} l'intervallo di tempo minimo necessario a Bob per rilevare un solo fotone e con $\mu t t_{\mathrm{B}} \eta$ la probabilità che Bob riveli, otteniamo una stima per questa seconda limitazione ovvero: $\frac{1}{\tau_{\mathrm{d}} \mu t t_{\mathrm{B}} \eta}$. La terza limitazione è dovuta alla procedura operativa: non si possono spedire segnali contemporaneamente, ma bisogna aspettare che Bob effettui la misura su un fotone per poterne inviare un altro. Chiamiamo quindi questo tempo $\mathrm{T_{dc}}$, dove dc sta per *duty cycle*. Possiamo infine dire che l'equazione corretta per la stima di ν_{s} è:

$$\nu_{\mathrm{s}} = \min\left(\nu_{\mathrm{s}}^{\max}, \frac{1}{\tau_{\mathrm{d}} \mu t t_{\mathrm{B}} \eta}, \frac{1}{T_{\mathrm{dc}}}\right) \tag{1.6}$$

Il secondo termine invece, ovvero la probabilità legata al fatto che Bob accetti o meno, verrà trattato in seguito (nel capitolo 2 del presente lavoro), perché è specifico del protocollo utilizzato.

Secret Fraction (r)

La secret fraction è una quantità che dipende dalla parte finale del protocollo scelto, chiamata *post-processing*. In generale però quello che si può dire è che i limiti di sicurezza sulla secret fraction dipendono da come avviene il controllo sulla Raw key. In particolare r è legata, come provato da Shannon, al numero di simboli perfettamente correlati estraibili da una lista di simboli parzialmente correlati, e il tutto è legato alla mutua informazione ovvero: $I(A:B) = H(A) + H(B) - H(AB)$, dove H è l'entropia di Shannon. Nel contesto dei protocolli pensando in termini di "mittente" M e "destinatario" D, la formula può essere riorganizzata come $I(A:B) = H(M) - H(M|D)$: chi invia il segnale deve rivelare una quantità di informazione almeno grande quanto l'incertezza che l'altro utente ha nell'ottenerla. Si vedranno in seguito, nel capitolo 2, le considerazioni su r derivanti dal particolare protocollo scelto.

1.6 Differenze tra protocolli teorici e sperimentali

Dal 1984, dopo i lavori di Bennett e Brassard, l'interesse e la fattibilità della QKD crebbero notevolmente. Vennero proposti numerosi protocolli sperimentali che miglioravano il BB84 in termini di distanza raggiungibile. Grandi passi furono fatti anche dai teorici che proposero nuovi tipi di protocollo, come il *six-state protocol*, ma, di gran lunga più importante fu il fatto che si iniziò a lavorare su prove di sicurezza rigorose che avrebbero sostituito le argomentazioni intuitive, fondate sulle stime sperimentali. A questo proposito sono molto importanti i lavori di Mayers, Lo e Chau, Short e Preskill. Negli anni 2000, molti passi in avanti sono stati fatti sia sul versante sperimentale, sia su quello teorico. Tuttavia, inevitabilmente, si è aperto un gap tra i due: le prove di sicurezza venivano derivate solo per schemi molto idealizzati, d'altro canto i setup sperimentali venivano resi più pratici senza curarsi troppo della questione sicurezza. Il punto di questo gap viene colto dopo la scoperta del possibile attacco *photon-number-splitting*: il problema era da ricercarsi nella sorgente. Nei protocolli teorici studiati veniva sempre supposto l'utilizzo di una sorgente di fotoni singoli, mentre nel panorama sperimentale si utilizzavano i fasci laser attenuati, con media di fotoni emessa minore di uno. I fasci laser, infatti, avendo fotoni distribuiti secondo una poissoniana, a volte presentavano due o più fotoni e questo causava un grosso distacco dal caso teorico. Questa problematica oggi è stata in parte superata con l'introduzione del metodo *decoy states* e con la realizzazione di nuovi tipi di protocollo quali il *continuous variable protocol* e il *distributed-phase-reference protocol*. Il divario es-

sendo stato colmato, apre le porte per la commerciabilità di sistemi di crittografia basati su protocolli QKD.

Capitolo n. 2

Protocollo BB84

I tipi di protocolli di QKD sono, a livello teorico, infiniti, ma le varie possibilità si sono ad oggi suddivise in tre grandi famiglie: codifica a *variabile discreta*, codifica a *variabile continua* e codifica a *riferimento di fase distribuita*. La differenza principale è sullo schema di rilevazione del segnale e su come esso viene codificato. I primi protocolli ad essere stati realizzati e per i quali è stata dimostrata la sicurezza, appartengono alla prima famiglia, e ad oggi i protocolli a variabile discreta sono ancora i più utilizzati. Il primo e il più famoso di questi protocolli è il BB84, che prende il nome dai suoi ideatori Bennet e Brassard, pubblicato nel 1984. Il protocollo, come tutti gli altri, prevede l'utilizzo di due canali di comunicazione, uno classico autenticato, e l'altro quantistico. Tale protocollo verrà innanzitutto presentato nella forma P&M (*prepare-and-measure*), e in particolare si tratterà con l'implementazione del decoy state, successivamente si presenterà nella versione entangled base.

NB: Le formule che verranno ricavate nei capitoli successivi tengono conto dello scenario peggiore possibile, ovvero che tutta la luce non raccolta dai detectors sia utilizzabile dall'intercettatore. Così facendo si pone un limite inferiore alla formulazione in modo tale che le prove di sicurezza per tutti gli altri scenari, una volta trattato il peggiore, siano ancora valide.

2.1 Prepare and Measure (P&M)

Supponiamo che sia Alice ad avere la sorgente di fotoni. Le proprietà spettrali dei fotoni sono definite così che l'unico grado di libertà sia la polarizzazione. Alice e

Bob allineano i polarizzatori e concordano sull'utilizzo di due tipi di base, ovvero orizzontale-verticale (+), o la base complementare di polarizzazione lineare, cioè +45/-45 (X). Questi stati di polarizzazione in bit equivalgono a:

$$\begin{array}{ll} |H\rangle, \text{ codes for } 0_+ & |{+}45\rangle, \text{ codes for } 0_\mathrm{X} \\ |V\rangle, \text{ codes for } 1_+ & |{-}45\rangle, \text{ codes for } 1_\mathrm{X}. \end{array}$$

Una volta accordatisi sulla tipologia di codifica, il protocollo prosegue con Alice che prepara i fotoni in uno dei quattro stati descritti sopra, e uno alla volta li invia a Bob attraverso il canale quantistico. Bob ha la possibilità di misurare in una delle basi + o X ogni fotone. Alla fine di questo step i due operatori possiederanno N coppie (bit,base) in base al numero di fotoni inviati. Ultimato l'invio dei fotoni si apre la seconda parte del protocollo: la fase di *post-processing* (per i protocolli analizzati verrà utilizzata la *one-way classical post-processing*, indicante che le informazioni nel canale classico vengono inviate da un unico operatore). In particolare prima si esegue lo step definito *sifting*, che consiste nella comparazione delle basi di ognuna delle coppie, e vengono scartate le coppie per le quali i due operatori hanno basi diverse. Al termine di questo processo, se il numero di fotoni N è molto elevato, il numero di coppie restanti tenderà a N/2. La lista delle coppie restanti viene chiamata *raw key* (chiave grezza). Per completare il protocollo i due operatori rivelano un campione casuale della chiave grezza e stimano la percentuale di errore (ovvero di perdite) del canale quantistico, e questo, nel limite peggiore, rappresenta tutta l'informazione che potrebbe avere a disposizione un eventuale intercettatore. In assenza di errori, la chiave di Alice e Bob è identica e la chiave grezza rappresenta già quella finale. Nel caso in cui l'errore stimato sia superiore a quello previsto teoricamente dai mezzi materiali tramite i quali si comunica, Alice e Bob devono scartare la chiave e provvedere a ripetere il protocollo dall'inizio. Gli ultimi passaggi avvengono entrambi nel canale classico, per questo motivo l'ultima parte del protocollo prende il nome di *classical postprocessing*. Dall'analisi della procedura si può già ricavare, nel caso specifico del BB84 P&M, quale sarà la formula generale per il raw key rate, che nell'introduzione era stato presentato nella formula generale $R = \nu_\mathrm{s} P_\mathrm{Bob}$. La probabilità che Bob accetti dipende unicamente dal fatto che abbia usato o meno la stessa base di Alice, e questo avviene con probabilità p_sift. Quindi scrivendo per comodità $\tilde{\nu}_\mathrm{S} = \nu_\mathrm{S} p_\mathrm{sift}$ risulta:

$$R_\mathrm{n} = \tilde{\nu}_\mathrm{S} p_\mathrm{A}(n) f_\mathrm{n} \tag{2.1}$$

dove f_n è la probabilità che Eva inoltri qualche segnale a Bob per una pulsazione di n-fotoni.

2.1.1 BB84 P&M Protocollo ideale: singolo fotone

Il protocollo ideale prevede una sorgente ideale che emetta singoli fotoni, in questo modo si ha la possibilità di avere la conoscenza, fotone per fotone, della quantità di informazione esatta persa. Quindi tutti i protocolli teorici partono dallo scenario di sorgente a fotone singolo. Per riuscire a prevedere i risutati sperimentali serve una formula che leghi il Key Rate ai parametri ottenibili dall'esperimento, ovvero Q, errore percentuale dovuto alle perdite di segnale, e R, raw key rate. Per fare questo si parte dalla definizione generale di K, $K = rR$, e si vanno a definire in modo dettagliato i due termini. Il termine r, come accennato precedentemente, riguarda l'informazione che può essere utilizzata da quella che viene effettivamente scambiata. È stato provato che pur scegliendo come seconda parte del protocollo la *one-way classical post-processing* si ottiene:

$$r = I(A : B) - \min(I_{\mathrm{EA}}, I_{\mathrm{EB}}) \tag{2.2}$$

Questa formula indica che la miglior chiave selezionabile, è quella su cui l'intercettatore ha meno informazione possibile. Nel caso del protocollo in esame $H(A) = H(B) = 1$ in quanto Alice e Bob scambiano singoli fotoni, e $H(A|B) = H(B|A) = H(Q)$, con Q Qber, ovvero la percentuale di perdite rispetto ai fotoni inviati. Quindi la formula per il Key rate ottenibile diventa, a partire dall'eq. 2.1:

$$K = R[1 - leak_{\mathrm{EC}}(Q) - I_{\mathrm{E}}] \tag{2.3}$$

dove $leak_{\mathrm{EC}}(Q) \geq h(Q)$ e $I_{\mathrm{E}} = min(I_{\mathrm{AE}}, I_{\mathrm{BE}})$. Per proseguire nella trattazione si introducono delle notazioni comode in seguito. Si definisce come R il rate totale di rilevazione e come $\mathrm{R_n}$ il rate di rilevazione per gli eventi in cui Alice invia n fotoni ($\sum_n R_{\mathrm{n}} = R$). Il rapporto $\frac{R_{\mathrm{n}}}{R}$ viene chiamato Y_{n} ($\sum_n Y_{\mathrm{n}} = 1$). I conteggi sbagliati rispetto agli $\mathrm{R_n}$ verranno chiamati $R_{\mathrm{n}}^{\mathrm{w}}$, in modo tale da poter definire il tasso di errore sul segnale di n fotoni come $\varepsilon_{\mathrm{n}} = \frac{R_{\mathrm{n}}^{\mathrm{w}}}{R_{\mathrm{n}}}$. Infine per indicare la percentuale di errore totale utilizziamo $Q = \sum_n Y_{\mathrm{n}}\varepsilon_{\mathrm{n}}$, che viene anche chiamato Qber. Tornando all'eq. 2.2, si può ora vedere come calcolare i vari termini. Per quanto riguarda $\mathrm{I_E}$ possiamo definirlo come $I_{\mathrm{E}} = \max_{Eva} \sum_n Y_{\mathrm{n}} I_{\mathrm{E,n}}$, dove il massimo è da prendersi su tutti i possibili attacchi disponibili all'intercettatore, compatibili con i parametri da misurare. In particolare nel caso che si sta presentando, ossia quello di fotone singolo, $I_{\mathrm{AE}} = I_{\mathrm{BE}}$; inoltre l'intercettatore può guadagnare informazione solo alle spese di introdurre un errore ε_1 (dato che per eventi in cui Alice non invia fotoni ma Bob ha una rilevazione $\mathrm{I_{E,0}}$=0), quindi si ottiene che $I_{\mathrm{E},1} = h(\varepsilon_1)$, dove h è l'entropia binaria. Si arriva infine a ottenere

$$\begin{aligned} I_{\mathrm{E}} &= \max_{Eva}[Y_1 h(\varepsilon_1) + (1 - Y_0 - Y_1)] \\ &= 1 - \min_{Eva}\{Y_0 + Y_1[1 - h(\varepsilon_1)]\}, \end{aligned} \tag{2.4}$$

il cui significato è che l'informazione a disposizione dell'intercettatore è quella totale scambiata a cui va a sottrarsi il minimo del segnale perso da A e B, ovvero il rumore di fondo più l'informazione persa nell'invio del singolo fotone, a cui va però a sottrarsi l'errore introdotto per effettuare tale misurazione. Ovviamente il minimo valore è quello per cui Eva non ottiene alcun rumore di fondo, per cui $Y_0 = 0$. Infine si pone $\varepsilon_{\geq 2} = 0$, così $\varepsilon_1 = \frac{Q}{Y_1}$. Tuttavia essendo il caso di fotone singolo, Eva quando ruba l'informazione ottiene esattamente il fotone intercettato quindi $Y_1 = 1$. Questo permette di scrivere la formula per il Key rate raggiungibile, partendo dall'eq. 2.2 sostituendo i termini otteniamo infatti:

$$K = R[1 - h(Q) - leak_{\mathrm{EC}}(Q)] \tag{2.5}$$

Per stimare analiticamente questa formula a priori bisogna assumere che l'errore introdotto nella misurazione dell'intercettatore sia il minore possibile, quindi $leak_{\mathrm{EC}} = h(Q)$. Per quanto riguarda R, come visto all'inizio del paragrafo, in questa implementazione assume la forma $R_{\mathrm{n}} = \tilde{\nu_{\mathrm{S}}} p_{\mathrm{A}}(n) f_{\mathrm{n}}$, e considerando che il protocollo viene analizzato con implementazione in fibra e con classical post-processing si ottiene $R = \tilde{\nu}_{\mathrm{s}} t t_{\mathrm{B}} \eta$. Sostituendo questa ultima correzione alla formula 2.4 otteniamo la formula finale:

$$K = \tilde{\nu}_{\mathrm{s}} t t_{\mathrm{B}} \eta [1 - 2h(Q)] \tag{2.6}$$

dove $Q = \frac{\frac{(1-V)}{2} P + \frac{P_{\mathrm{d}}}{2}}{R}$, in cui P rappresenta la probabilità di rivelare un fotone e P_{d} la probabilità di dark-count. La curva rappresentata nel grafico successivo mostra come varia il rate di produzione della chiave in funzione della distanza. La forma tipica della curva nella parte finale dipende dalle caratteristiche del canale quantistico. Oltre una distanza dipendente dalle specifiche dell'apparato sperimentale infatti, l'informazione desumibile dai fotoni si confonde totalmente con il rumore di fondo.

NB: Il risultato ottenuto per fotone singolo rappresenta il limite ideale a cui tendono tutte le implementazioni sperimentali P&M. Per questo motivo anche nella trattazione che segue esso verrà preso sempre come riferimento per il confronto.

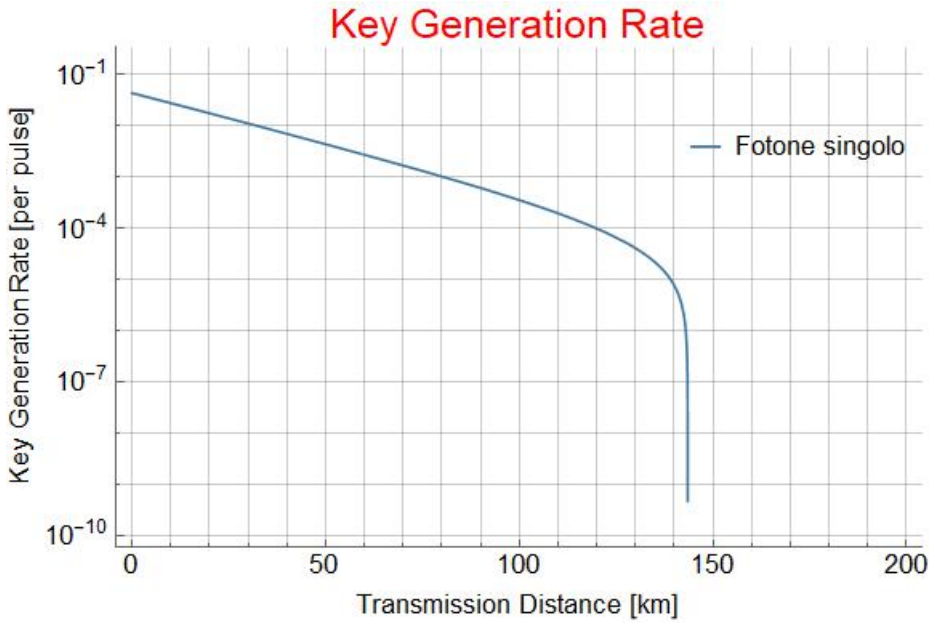


Figura 2.1: *Key generation rate* per segnale ideale composto da un singolo fotone

2.1.2 BB84 P&M Decoy-State

L'idea su cui si fonda l'implementazione del BB84 P&M con decoy state è un'idea semplice, che non aggiunge molto alla procedura operativa, ma sul fronte sicurezza rappresenta un notevole balzo avanti rispetto alle implementazioni che non utilizzano tale metodo. In questa versione del protocollo, infatti, quello che provvede a fare Alice è cambiare la natura del segnale quantistico in modo casuale durante la procedura, e solo alla fine del trasferimento di informazione rivela quale stato ha inviato in ogni singolo scambio. Così facendo l'intercettatore non può adeguare il suo attacco allo stato inviato da Alice, d'altro canto invece, Alice e Bob possono utilizzare questo parametro addizionale per stimare meglio a posteriori l'errore nella trasmissione. Si è detto che la peculiarità del protocollo consiste nel modificare la natura del segnale quantistico, ma come viene modificato tale segnale? Ebbene la modifica di cui si parla è la modifica di uno dei parametri del fascio laser, ξ. Il parametro più facile da modificare è l'intensità del fascio, in poche parole il parametro μ della distribuzione di fotoni nella poissoniana, che rappresenta il valore medio del numero di fotoni emessi, così da avere $\xi = \mu$. Quello che avviene dunque nello scambio di informazione è che per la maggior parte della procedura Alice invia un fascio laser con $\mu = 1$, e in modo casuale varia di tanto in tanto il parametro μ. Alla fine dello scambio Alice e Bob condividono i vari ξ utilizzati. A questo punto, a differenza del protocollo originale, in cui i due utenti stimano R e Q totali sulla totalità dei dati raccolti, qui vengono calcolati R^{ξ} e Q^{ξ} per ogni

valore di ξ cambiato durante lo scambio. Se si indica con χ l'insieme di valori tra cui si sceglie ξ, Alice e Bob misurano quindi $2|\chi|$ parametri, ovvero χ-volte R^ξ e Q^ξ. Il set χ è noto pubblicamente come parte del protocollo, ma se $|\chi| > 1$, Eva non può adattare la sua strategia ai singoli valori di ξ per ogni pulsazione, perchè non li conosce. Nelle formule per la stima del raw key rate e per il Qber, rispettivamente $R^\xi = \sum_{n\geq 0} R^\xi_{\mathrm{n}}$ e $Q^\xi = \sum_{n\geq 0} \frac{R^\xi_{\mathrm{n}}}{R^\xi}\varepsilon_{\mathrm{n}}$, con $R^\xi_{\mathrm{n}} = \tilde{\nu}_{\mathrm{S}} p_{\mathrm{A}}(n|\xi) f_{\mathrm{n}}$, f_{n} e ε_{n} sono indipendenti da ξ, quindi le formule rappresentano in realtà un sistema lineare di $2|\chi|$ equazioni. Per semplicità, nella presentazione dei risultati, si suppone che tutti i termini f_{n} e ε_{n} siano stati ricavati esattamente. Si deduce così che la quantità rappresentante l'informazione di Eva è

$$I^\xi_{\mathrm{E}} = 1 - Y^\xi_0 - Y^\xi_1[1 - h(\varepsilon_1)] \tag{2.7}$$

con rispettivamente $Y^\xi_{0,1} = \frac{R^\xi_{0,1}}{R^\xi}$. Si ottiene così la formula per il secret key rate:

$$K^\xi = R^\xi\{Y^\xi_0 + Y^\xi_1[1 - h(\varepsilon_1)] - h(Q^\xi)\} \tag{2.8}$$

dove $R = \nu_{\mathrm{S}}(P + P_{\mathrm{d}})$, P è la probabilità di rilevare il segnale, $P = \sum_{n=1}^{\infty} \frac{\mu^{\mathrm{n}}}{n!} e^{-\mu}[1 - (1 - tt_{\mathrm{B}}\eta)^{\mathrm{n}}] = 1 - e^{-\mu t t_{\mathrm{B}}\eta}$, e P_{d} è la probabilità che il rilevatore riveli un falso positivo, $P_{\mathrm{d}} = 2p_{\mathrm{d}} \sum_{n=0}^{\infty} \frac{\mu^{\mathrm{n}}}{n!} e^{-\mu}(1 - tt_{\mathrm{B}}\eta)^{\mathrm{n}} = 2p_{\mathrm{d}} e^{-\mu t t_{\mathrm{B}}\eta}$, con pd percentuale di segnale di background. Il termine ε_1, ovvero la percentuale di errore sul segnale in cui viene inviato un fotone, risulta $\varepsilon_1 = \frac{Q}{Y_1}$, con $Q = (\varepsilon P + \frac{P_{\mathrm{d}}}{2})\frac{\nu_{\mathrm{S}}}{R}$, cioè il Qber. Il key rate totale si trova facilmente da questo come somma su tutti i K^ξ. Di questo protocollo si utilizzano principalmente due varianti: weak decoy state e vacuum+weak decoy state. La particolarità della prima variante risiede nel fatto che vengono utilizzati due ξ diversi nella procedura, chiamiamoli ν_1 e ν_2, tali che $\nu_1 + \nu_2 < \mu$, dove μ è il valore medio del fascio laser. La seconda invece constiste nell'applicare la prima mandando però uno dei due valori a 0, quindi utilizzando il fondo come altro decoy state.

Nel grafico seguente si riporta l'andamento del Key rate in funzione della distanza raggiungibile. Per un'analisi più dettagliata si fa inoltre un confronto tra due setup sperimentali diversi, riportati in tabella.

Dai grafici si evince come, modificando l'apparato sperimentale, in particolare migliorando la qualità della fibra usata e introducendo un rilevatore più efficiente, si riesce a incrementare di molto la distanza raggiungibile. Nel grafico successivo invece si utilizzano i dati del Set 1 per confrontare la previsione teorica ideale di fotone singolo con quella del decoy state appena ricavata.

Tabella 2.1: Dati di due apparati sperimentali differenti

Parameter	Set 1	Set 2
μ (mean intensity)	0.5	0.5
V (visibility)	0.99	0.99
t_B (transmission in Bob's device)	1	1
η (detector efficiency)	0.1	0.2
p_d (dark counts)	10^{-5}	10^{-6}

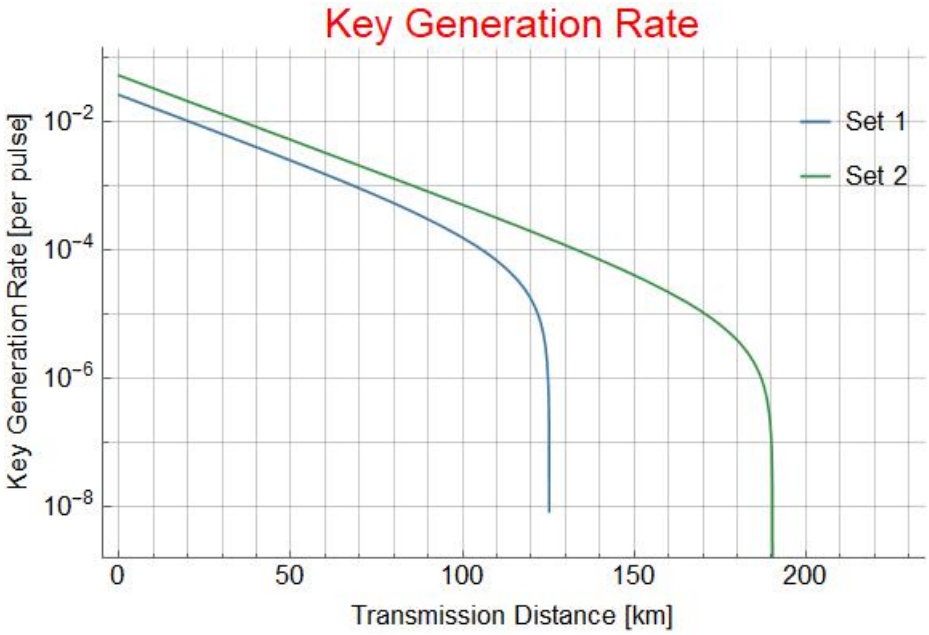


Figura 2.2: Confronto dei *Key generation rate* di due implementazioni differenti di BB84 decoy-states

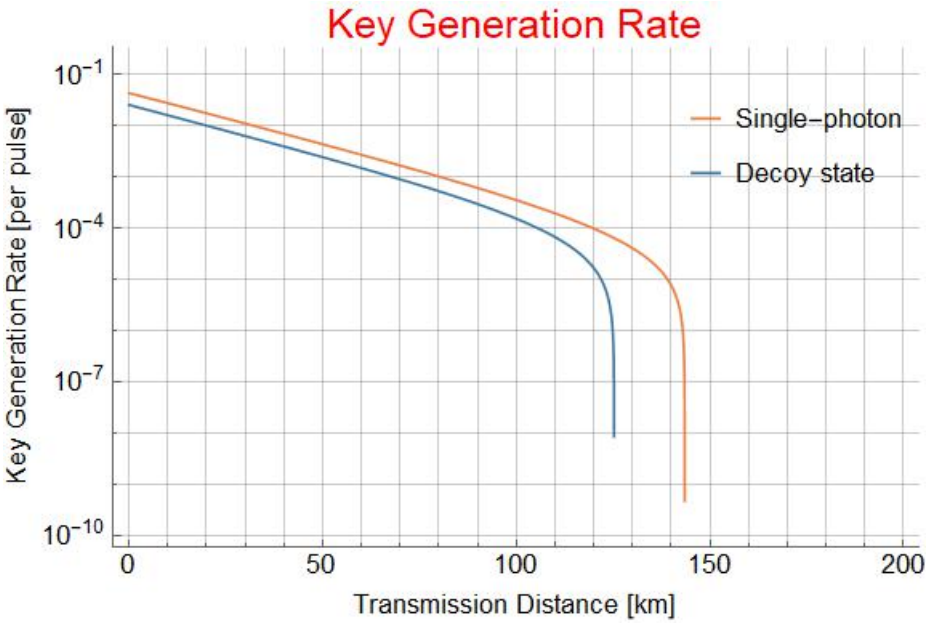


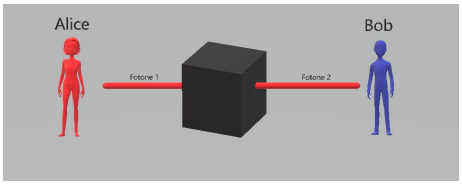
Figura 2.3: Confronto dei *Key generation rate* tra il protocollo a singolo fotone e quello decoy-states

Capitolo n. 3

Entangled Base

Vengono chiamati protocolli EB, entangled base, i protocolli che, invece della procedura P&M, fanno uso di una procedura che prevede l'utilizzo di coppie di fotoni entangled. Per quanto riguarda le sorgenti utilizzate per la produzione di coppie entangled si rimanda al paragrafo 1.3.2. I protocolli possono prevedere diverse posizioni per la sorgente: mentre nella procedura P&M la sorgente veniva utilizzata o da Alice o da Bob che dovevano provvedere a preparare il fotone in un determinato stato, nella procedura EB la sorgente può essere posta in varie posizioni, cioè può essere tenuta o da Alice o da Bob come nel P&M, o potrebbe anche essere posta a metà del canale quantistico. Questa possibilità di scelta nella posizione della sorgente dipende dalla particolarità dell'utilizzo della base entangled: i due partner anche compiendo la misurazione sui fotoni indipendentemente l'uno dall'altro, la misura di uno influenza automaticamente la misurazione dell'altro, nel senso che se i due operatori misurano nella stessa base si ha la misurazione perfettamente correlata, altrimenti si hanno risultati scorrelati e random.

BB84 Entangled base



Il protocollo rimane identico nelle sue parti, l'unica modifica risiede nella posizione della sorgente e nel tipo di segnale utilizzato. Il segnale consta di una coppia di fotoni entangled, un fotone diretto ad Alice e l'altro a Bob. Essi provvedono separatamente a effettuare la misurazione sui fotoni, nelle basi descritte nella parte generale. Il protocollo che viene qui presentato è quello che prevede la sorgente posta nel mezzo del canale quantistico, quindi la distanza in funzione della

quale vengono espressi i *key generation rate* è la metà della distanza totale. Si potrebbe pensare che questa scelta comporti un maggior rischio, offrendo a Eva possibilità in più di carpire informazioni. Tuttavia è stata dimostrata la sicurezza anche per questo scenario (X. Ma, C. F. Fung, and H. Lo, 2007, [6]). Infatti anche se la sorgente fosse in mano all'intercettatore, pensando all'apparato di Alice come ad una scatola, quando Eva mette un fotone preparato in un determinato stato nella scatola di A, non ha nessun modo di prevedere quale sarà il risultato di una misura fatta da questa, perchè la matrice di densità di stati all'esterno della scatola è indipendente dal risultato della misura all'interno.

Visto che la procedura del protocollo rimane inalterata, le formule 2.2 e 2.3 rimangono ancora valide. si arriva quindi alla formula:

$$K = R[1 - h(Q) - leak(Q)] \tag{3.1}$$

che, utilizzando nuovamente l'approssimazione in cui l'intercettatore nella sua misurazione introduce l'errore minore possibile, porge:

$$K = R[1 - 2h(Q)] \tag{3.2}$$

Dove R e Q presentano ora una forma diversa. Prima di arrivare alle espressioni analitiche però ci fermiamo per constatare un risultato molto importante. Formalmente la 2.10 è identica alla formula ideale di fotone singolo e questo è un risultato molto importante: si può tenere conto di tutte le possibili deviazioni da una sorgente a due fotoni perfetta, quindi, in questo caso, di tutti i contributi di multifotone, misurando il parametro Q, Qber. Questo risultato deriva da un argomento del tutto generale riguardante le sorgenti non caratterizzate e il caso in cui non se ne abbia il controllo, dimostrato da M. Koashi e J. Preskill (M. Koashi and J. Preskill, Phys. Rev. Lett. Vol 90, No 5 (2003), [3]). Arrivano infatti a dimostrare che qualsiasi sia lo stato che Eva riesce a ottenere compiendo misurazioni a partire dal fotone diretto a uno dei due utenti, non ha in alcun modo possibilità di avere informazioni sulla chiave finale scelta dai due.

Tornando quindi alle espressioni per R e Q, bisogna innanzitutto partire dal capire quale sia la probabilità che la sorgente emetta una coppia di n fotoni. Dalla formula 1.4 dello stato generico emesso tramite PDC, si ricava che la probabilità è:

$$P(n) = \frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{3.3}$$

Un'altra constatazione necessaria per giungere al risultato è notare che ora le efficienze dei due operatori contribuiscono entrambe al calcolo del rate di generazione della chiave, dato che sia Alice sia Bob effettuano delle misurazioni. In particolare l'efficienza totale per un coppia di n fotoni può essere scritta come il prodotto delle singole efficienze ovvero:

$$\eta_{\mathrm{n}} = [1 - (1 - tt_{\mathrm{A}}\eta_{\mathrm{A}})^{\mathrm{n}}][1 - (1 - tt_{\mathrm{B}}\eta_{\mathrm{B}})^{\mathrm{n}}] \tag{3.4}$$

e ricordando come si era definito Y_{n} ($\frac{R_{\mathrm{n}}}{R}$), si ricava che può essere scritto come:

$$Y_{\mathrm{n}} = [1 - (1 - pd_{\mathrm{A}})(1 - tt_{\mathrm{A}}\eta_{\mathrm{A}})^{\mathrm{n}}][1 - (1 - pd_{\mathrm{B}})(1 - tt_{\mathrm{B}}\eta_{\mathrm{B}})^{\mathrm{n}}]. \tag{3.5}$$

Quindi si può ora scrivere la formula per R:

$$R = \sum_{n=0}^{\infty} P(n)Y_{\mathrm{n}} = \sum_{n=0}^{\infty}[1-(1-pd_{\mathrm{A}})(1-tt_{\mathrm{A}}\eta_{\mathrm{A}})^{\mathrm{n}}][1-(1-pd_{\mathrm{B}})(1-tt_{\mathrm{B}}\eta_{\mathrm{B}})^{\mathrm{n}}]\frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}. \tag{3.6}$$

Infine, dato che $Q = \sum_n Y_{\mathrm{n}}\varepsilon_{\mathrm{n}}$, c'è bisogno di capire cosa usare come ε_{n}. Questo termine rappresenta l'errore nel ricevere il segnale. Nel caso n=0 l'errore è solo quello casuale del fondo, che quindi è $\frac{1}{2}$, mentre nel caso n=1, l'errore introdotto è rappresentato da quello casuale di fondo a cui va a sottrarsi però l'errore sui segnali casuali di fondo che vengono persi per causa dell'apparato strumentale (detector, fibra ecc...), che nella formula si indicheranno con e, normalizzati ai segnali rivelati. Nella stima dell'errore però, dal risultato discusso precedentemente, ci si può fermare a n=1, tutti i contributi successivi possono essere trascurati dato che nel caso reale questi comunque non porterebbero alcun vantaggio a Eva, tenendo conto inoltre che i primi termini della sommatoria sono quelli più pesanti. Si esprime quindi ε_{n} così:

$$\begin{aligned} \varepsilon_0 &= \frac{1}{2}P(0) \\ \varepsilon_1 &= \left[\frac{1}{2} - \frac{(\frac{1}{2} - e)(tt_{\mathrm{A}}\eta_{\mathrm{A}})(tt_{\mathrm{B}}\eta_{\mathrm{B}})}{Y_1}\right]P(1) \end{aligned} \tag{3.7}$$

Arriviamo quindi a esprimere il QBER come:

$$Q = \frac{1}{R}\left\{\frac{1}{2}P(0)Y_0 + P(1)\left[\frac{1}{2}Y_1 - \left(\frac{1}{2} - e\right)(tt_{\mathrm{A}}\eta_{\mathrm{A}})(tt_{\mathrm{B}}\eta_{\mathrm{B}})\right]\right\} \tag{3.8}$$

Avendo ricavato le formule nel caso generale ora si può introdurre una ragionevole approssimazione per semplificare i conti. Infatti non è così difficile a livello sperimentale scegliere un setup in modo tale che Alice e Bob abbiano parametri simili per quanto riguarda le caratteristiche di fibre ottiche e detector. Allora, ponendo $pd_{\mathrm{A}} = pd_{\mathrm{B}}$, $t_{\mathrm{A}} = t_{\mathrm{B}}$, $\eta_{\mathrm{A}} = \eta_{\mathrm{B}}$, le formule diventano:

$$\begin{aligned} R &= \sum_{n=0}^{\infty} P(n)Y_{\mathrm{n}} = \sum_{n=0}^{\infty}[1-(1-pd_{\mathrm{A}})(1-tt_{\mathrm{A}}\eta_{\mathrm{A}})^{\mathrm{n}}]^2\frac{(n+1)\lambda^n}{(1+\lambda)^{n+2}}, \\ Q &= \frac{1}{R}\left\{\frac{1}{2}P(0)pd^2 + P(1)\left[\frac{1}{2}Y_1 - \left(\frac{1}{2} - e\right)(tt_{\mathrm{A}}\eta_{\mathrm{A}})^2\right]\right\}. \end{aligned} \tag{3.9}$$

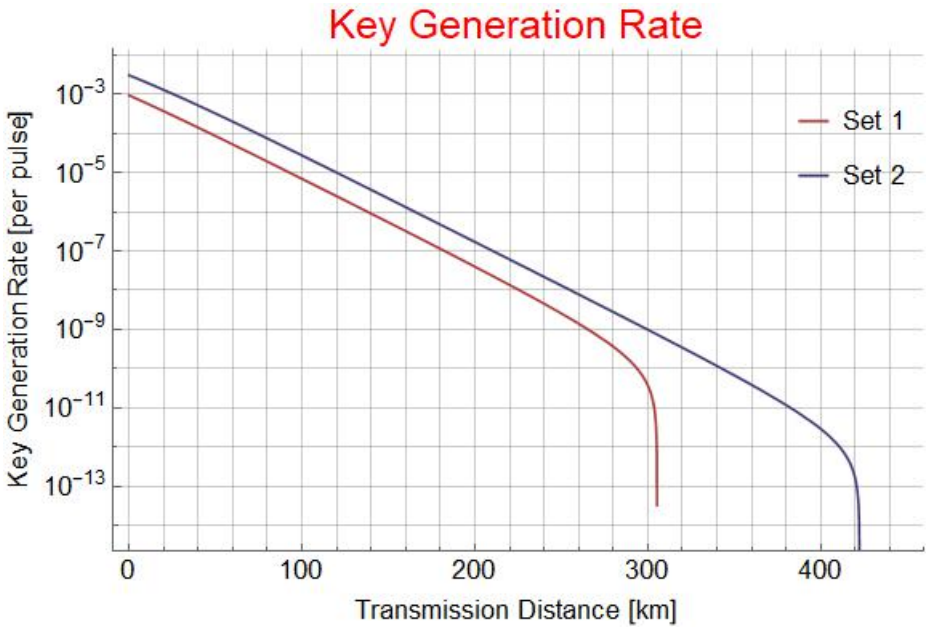


Figura 3.1: Confronto dei *Key generation rate* di due implementazioni differenti di BB84 entangled base (vengono utilizzati i dati della tabella 2.1)

Come fatto per il BB84 P&M con il decoy state, si presenta un confronto tra i due set di dati sperimentali di tabella 2.1, per mostrare come varia la distanza raggiungibile in relazione a un miglioramento del setup.

Capitolo n. 4

Conclusioni

Nel capitolo precedente sono state presentate le forme analitiche per il calcolo del Key rate nelle due implementazioni oggetto della tesi. Ora si porrà l'attenzione a chiarire le differenze fondamentali che portano l'implementazione EB ad essere quella migliore. Le ragioni sono conseguenza diretta del tipo di sorgente. L'utilizzo di una sorgente di fotoni entangled infatti permette di garantire che vengano inviati contemporaneamente fotoni, di cui si conosce la correlazione, a due partner differenti. Questo comporta il vantaggio che, pur senza diminuire la sicurezza del protocollo, la sorgente possa essere posta nel mezzo tra Alice e Bob. Ne consegue un altro notevolissimo vantaggio che è quello della distanza raggiungibile, la quale risulta raddoppiata rispetto ad una configurazione P&M. Un altro aspetto importante, che deriva anche questo dal fatto che sia permesso a tutti e due gli utenti di effettuare la misurazione, è il livello in cui il segnale iniviato si confonde con il rumore. Si nota dal grafico in figura 4.1 che il "gomito" della curva è molto più basso. Una spiegazione si può ricavare proprio dalla formula 3.8 sul QBER. Nella formula appare infatti il termine Y_0 che, facendo il conto nell'approssimazione usata sopra, risulta essere uguale a pd^2. Questo indica che per avere dei falsi positivi che influenzino effettivamente la chiave finale, i due detector di A e B devono registrare un evento di darkcount contemporaneamente, quindi la probabilità risulta bassisima. Se nella prima implementazione la probabilità di dark count dipende unicamente dalla rivelazione di Bob, nella seconda dipende da entrambi i partner. Infatti, perchè venga selezionato come "buono" il qubit relativo ad un dark count, deve essere stato rilevato un fotone da entrambi i detector, nel caso in cui un detector rivelasse un fotone falso positivo e l'altro no, nella procedura di analisi a posteriori non ci sarebbe corrispondenza tra la lista posseduta da Alice e Bob, quindi andrebbe scartato.

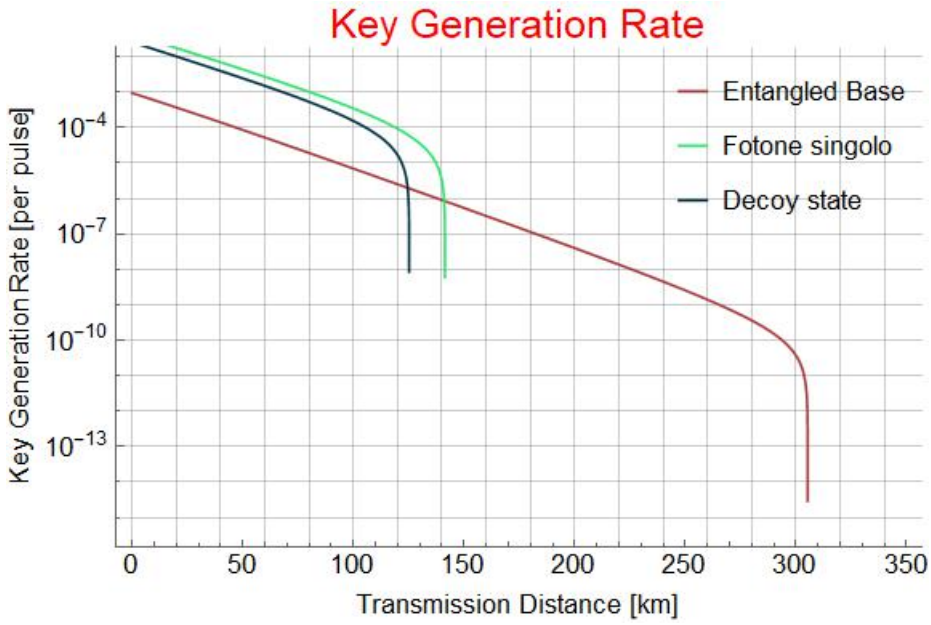


Figura 4.1: Confronto finale dei *Key generation rate* dell'implementazione decoy-states e di quella entangled base. Per maggiore chiarezza si riporta anche la curva relativa al caso ideale.

Nel grafico vengono presentati, con i dati del Set 1 della tabella 2.1, gli andamenti del Key rate per il BB84 con decoy state o con entangled base, e viene inoltre inserito, come riferimento, il limite asintotico a cui tendono le implementazioni P&M nel caso ideale di singolo fotone. La procedura con entangled base raggiunge una distanza nettamente maggiore come spiegato sopra. La procedura EB risulta quindi essere un notevole miglioramento nel protocollo BB84 in termini di distanza raggiunta, senza però averne compromesso la sicurezza.

Bibliografia

[1] Giuliano Benenti, Giulio Casati, Giuliano Strini, *Principles of Quantum Computation and Information*, World Scientific, 2005;

[2] Li Xi-Han, Li Chun-Yan, Deng Fu-Guo, Zhou Ping, Liang Yu-Jie, and Zhou Hong-Yu, Chin. Phys. Soc. Vol 16 No 8, August 2007;

[3] Masato Koashi and John Preskill, Phys. Rev. Lett. Vol 90, No 5 (2003);

[4] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, Momtchil Peev, *The security of practical quantum key distribution*, Review of Modern Physics, Vol 81, July-September 2009;

[5] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, Phys. Rev. A 72, 012326 (2005);

[6] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo, Phys. Rev. A 76, 012307 (2007);