Università degli Studi di Padova

Dipartimento di Fisica e Astronomia "Galileo Galilei"
Corso di Laurea in:
Fisica

Crittografia quantistica a variabili continue: dalla teoria alle implementazioni sperimentali

Relatore: Prof. Giuseppe Vallone

Laureando: Sebastiano Forner

Anno Accademico 2014/2015

Indice

Prefazione

Questo lavoro ha l'obiettivo di dare una panoramica sulla distribuzione di chiave quantistica (*Quantum key distribution*, QKD) attraverso l'uso di variabili quantistiche continue. Dopo aver definito che cos'è la crittografia quantistica e descritto le principali pietre miliari, si passerà ad una descrizione teorica della QKD a varibili continue con particolare riguardo alla sicurezza. Verranno infine analizzate delle implementazioni pratiche della *Continous Variable* QKD mettendo in luce le prestazioni di sicurezza e velocità che sono state raggiunte.

Capitolo 1

Introduzione alla Crittografia quantistica

1.1 Crittografia: obiettivi e introduzione

La crittografia è la disciplina che studia e realizza sistemi ed algoritmi atti a nascondere un messaggio a chiunque non sia autorizzato a leggerlo.
Introduciamo fin da subito una situazione fittizia, ma che è facilmente adattabile ad un contesto reale: immaginiamo che la persona A, Alice, voglia trasmettere un messaggio segreto ad un'altra persona B, Bob; la crittografia è lo strumento di cui Alice necessita. Il modo più intuitivo per nascondere un messaggio è mediante una parola chiave: due certi algoritmi, uno per così dire l'inverso dell'altro, cifrano e decifrano il messaggio in base alla chiave inserita, un tale approccio alla crittografia è detto simmetrico. Due aspetti sono quindi cruciali: la bontà degli algoritmi che effettivamente cifrano il messaggio e la segretezza della chiave.
Per quanto riguarda la bontà dell'algoritmo esistono oggi diversi algoritmi considerati sicuri [1] o addirittura perfetti [2]. In questo lavoro non ci si occuperà di questo aspetto, considerando l'algoritmo di cifratura sempre sicuro. Citiamo tuttavia l'algoritmo di cifratuara *One Time Pad* (OTP) nel quale per ogni messaggio da scambiare si crea una nuova chiave della stessa lunghezza del messaggio stesso, tale algoritmo è infatti perfetto: dato un messaggio cifrato è impossibile risalire a quello originale senza la totalità della chiave, a priori tutte le possibili combinazioni di quella lunghezza sono equiprobabili. La cifratura è ottenuta sommando bit a bit (modulo 2) la chiave e il messagio da cifrare.
La segretezza della chiave è tutt'altro problema, si può avere la migliore cassaforte del mondo, ma se la chiave è condivisa da tutti allora l'utilità ne viene certamente meno. È di questo aspetto che si occupa la crittografia quantistica con la distribuzione di chiave quantistica (QKD): rendere sicura e quindi segreta la chiave condivisa tra Alice e Bob.

1.2 Crittografia Quantistica: le basi

Lo schema tipico e più generale della QKD prevede due canali di trasmissione: un canale quantistico e un canale classico autenticato. Sul canale quantistico è possibile ogni tipo di operazione da parte di chiunque. Il canale classico deve invece essere autenticato, tutti cioè possono ascoltare o vedere ciò che viene trasmesso senza però poter alterare la trasmissione.
Allo schema che prevede Alice e Bob si usa aggiungere un terzo soggetto Eve (dall'inglese

eavesdropper, colui che origlia) intenzionata ad accedere ai segreti di Alice e Bob e quindi a conoscere la chiave. Eve ha dunque pieno accesso al canale quantistico, ove però l'ascolto (cioè la misura di uno stato quantistico) comporta inevitabilmente una modifica dello stato e quindi una distorsione della trasmissione quantistica. È questa la chiave di volta della crittografia quantistica: il solo ascolto, la sola intercettazione della chiave la modifica inevitabilmente e questa alterazione è ovviamente rilevabile da Alice e Bob. Questi, rilevando l'intrusione, possono valutare l'eventuale mancanza di sicurezza e, nel caso, annullare la trasmissione.
Nella pratica il suddetto canale quantistico può comporsi di un qualsiasi mezzo o particella che obbedisce alle leggi della meccanica quantistica: elettroni, ioni, luce, eccetera. È ovvio però che nel caso più generale possibile la trasmissione fra Alice e Bob può avvenire a grande distanza. Il mezzo più pratico per realizzare il canale quantistico è quindi senz'altro la luce, scelta nella sostanziale totalità delle implementazioni della QKD.
Nel 1984 C. H. Bennet e G. Brassard introdussero il primo protocollo di QKD basato appunto sulla luce e che porta il loro nome, il protocollo BB84 [3]. Il protocollo BB84 è uno di quei protocolli detti variabile discreta ove si utilizza un operatore quantistico a spettro discreto, nella fattispecie del BB84 si utilizza la polarizzazione di un singolo fotone.

1.3 Un breve sguardo al protocollo BB84

Come detto alla fine della precedente sezione il protocollo BB84 utilizza la polarizzazione di un fotone come variabile discreta quantistica per lo scambio della chiave. L'idea è quella di utilizzare due basi non ortogonali fra loro per codificare l'informazione. Nel caso specifico del BB84 si utilizzano le basi:

$$B_+ = \left\langle \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\rangle \qquad e \qquad B_\times = \frac{1}{\sqrt{2}} \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle$$

Ove il primo vettore di ciascuna base codifica per il bit 0 e il secondo vettore per il bit 1. In sostanza si avrà la seguente corrispondenza fra stati e bit:

- $|e_1\rangle \equiv |H\rangle$ codifica per il bit 0_+
- $|e_2\rangle \equiv |V\rangle$ codifica per il bit 1_+
- $|e_1 + e_2\rangle \equiv |+45\rangle$ codifica per il bit $0_\times$
- $|e_1 - e_2\rangle \equiv |-45\rangle$ codifica per il bit $1_\times$

Alice sceglie in modo casuale una delle due basi e codifica, mediante un polarizzatore, il bit voluto che poi invia a Bob. Questi, non sapendo quale base ha utilizzato Alice, sceglierà di nuovo casualmente una base tramite la quale effettuare la misura della polarizzazione del fotone. Se Bob scegliesse la stessa base che ha utilizzato Alice, egli otterrebbe certamente il bit corretto, altrimenti avrebbe il risultato giusto solo nella metà dei casi. Infatti, supponiamo che Alice mandi uno stato $|H\rangle$ e che Bob misuri con la base $B_\times$, la probabilità di ottenere il bit 0 sarà:

$$Prob\,(bit\,0) = \frac{\langle H|P_{0\times}|H\rangle}{\langle H|H\rangle} = \frac{1}{2}$$

Ove $P_{0\times}$ indica il proiettore corrispondente al bit 0 nella base $B_\times$. La probabilità del bit 1 sarà ovviamente anch'essa 1/2.

Dopo aver ripetuto N volte ciò di cui sopra, ovvero quando Alice ha inviato N stati a Bob, comincia la fase cosiddetta di *sifting*. In questa fase del protocollo Alice, mediante il canale classico, comunica a Bob la base che ha utilizzato per ciascuno degli N bit; egli andrà a scartare quei bit che ha ottenuto misurando con la base sbagliata. Alla fine di questa fase Alice e Bob condivideranno all'incirca una chiave di $N/2$ bit detta *chiave grezza*.
Una volta ottenuta la chiave grezza Alice e Bob si scambiano alcuni bit, scelti casualmente, della chiave per controllare l'effettiva corrispondenza; se questa mancasse anche per un solo bit vorrebbe dire che Eve ha intercettato la comunicazione, in caso contrario, ovvero in assenza di errori, la chiave grezza sarebbe la chiave sicura, definitiva. Se Eve avesse intercettato dei bit, compiendo delle misure -inevitabilmente- nella base sbagliata, avrebbe appunto modificato gli stati che sarebbero poi arrivati a Bob. L'analisi della correzione a posteriori [4] esula da questa trattazione.

1.4 I protocolli a variabile continua

Come detto precedentemente, il protocollo BB84 è un protocollo cosiddetto a variabile discreta, questi protocolli necessitano di un'apparecchiatura hardware dedicata quali sorgenti a singolo fotone, linee di trasmissione dedicate e detector appositi. L'efficienza e il costo di questi apparati sono i principali limiti di questo tipo di protocolli.
Un'altra famiglia di protocolli è quella dei protocolli a variabile continua (CVQKD) che possono utilizzare le linee di trasmissione standard e apparati di trasmissione e ricezione molto efficienti, capaci di operare ben oltre quanto richiesto tipicamente da un implementazione di CVQKD [5]. I protocolli a variabile continua che saranno qui trattati sono di due tipi: *Switching* e *No-Switching* e saranno trattati in modo completo nei prossimi capitoli.
È importante sottolineare che anche in questi protocolli si assume sempre che Eve non possa andare a modificare i canali classici, in particolare si assume che l'*oscillatore locale*, oggetto che definiremo nel prossimo capitolo, non possa mai essere disturbato da Eve.

Capitolo 2

La QKD a variabili continue

Prima di andare ad analizzare i protocolli veri e propri, vediamo un elemento indispensabile della CVQKD che li accomuna. La misura omodina è la tecnica con la quale Bob riceve i segnali inviatigli da Alice. In entrambi i protocolli che andremo ad analizzare, infatti, Alice invia a Bob due tipi di fasci: uno a bassa intensità, quantistico, che codifica le informazioni e uno ad alta intensità, considerato classico, con una differenza di fase costante con quello a bassa intensità detto *oscillatore locale* (LO, dall'inglese *local oscillator*). Con questi presupposti, le cui implementazioni saranno descritte in seguito, andiamo ad analizzare la misura omodina.

2.1 La misura omodina

2.1.1 La luce

La teoria classica della luce prevede che essa sia rappresentabile come sovrapposizione di onde elementari del tipo:

$$\alpha e^{i(\omega t - kx)}$$

dove ω è la frequenza, k il vettore d'onda (ovviamente $k^2 = \omega^2/c^2$) e α un numero complesso il cui modulo è l'ampiezza dell'onda e l'anomalia la fase dell'onda.
La teoria quantistica della luce (qui descritta come in [6]) va a trattare la funzione oscillante classica come un oscillatore armonico quantistico, sostanzialmente si va a sostituire il numero complesso α con l'operatore $\hat{a}$ di distruzione dell'oscillatore armonico quantistico. Si possono dunque introdurre due operatori $\hat{x}$ e $\hat{p}$ che non sono altro che una sorte di "parte reale" e "parte immaginaria" dell'ampiezza quantistica $\hat{a}$.

$$\hat{x} = \frac{1}{\sqrt{2}}\left(\hat{a} + \hat{a}^\dagger\right) \qquad \hat{p} = \frac{i}{\sqrt{2}}\left(\hat{a}^\dagger - \hat{a}\right)$$

che hanno la seguente relazione di commutazione:

$$[\hat{x}, \hat{p}] = i$$

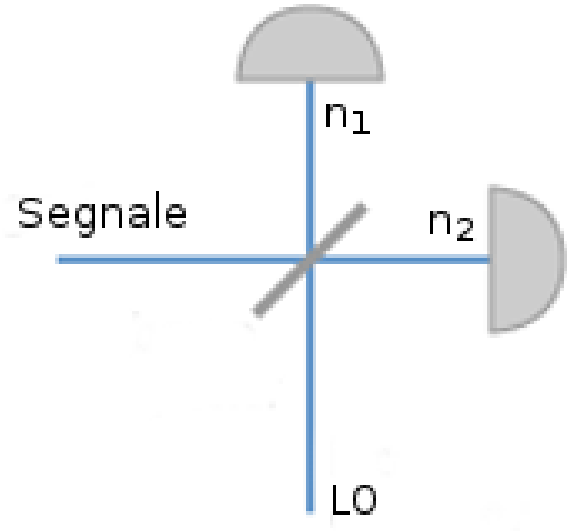
essendo $\hbar = 1$ e $\left[\hat{a}, \hat{a}^\dagger\right] = 1$. Questi due operatori vengono detti quadrature e sono assimilabili al concetto di posizione e momento dell'oscillatore elettromagnetico (l'onda).
Diremo che lo stato $|\alpha\rangle$ è uno *stato coerente* se esso è autostato dell' operatore $\hat{a}$ di autovalore (complesso) α:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle$$

e sarà il tipo di stato (non lo dimostriamo) che trasporterà il segnale in entrambi i protocolli.

2.1.2 L'apparato e la misura vera e propria

La misura omodina consente di misurare le due quadrature, $\hat{x}$ oppure $\hat{p}$, di un impulso laser in arrivo. Nella pratica si fanno incidere il fascio quantistico del segnale e il LO su di uno specchio semi-riflettente 50/50 (che verrà qui considerato ideale) e verranno poi misurate le intensità dei due fasci uscenti mediante due detector. La differenza fra queste intensità darà una quantità proporzionale ad una quadratura. Quale quadratura viene effettivamente misurata, lo decide la fase presente fra i due fasci incidenti sullo splitter.



Vediamo la cosa più in dettaglio: siano I_1 e I_2 le intensità dei due fasci uscenti, combinazione del segnale e del LO. Le intensità $I_{1,2}$ saranno proporzionali al numero N di fotoni che arrivano ai detector, scriviamo dunque, con un leggero abuso di notazione:

$$\Delta = I_2 - I_1 = \hat{n}_2 - \hat{n}_1$$

Gli operatori numero $\hat{n}$ saranno dati, come nel caso del'oscillatore armonico da:

$$\hat{n}_i = \widehat{a'}_i^{\dagger}\widehat{a'}_i \qquad i = 1, 2$$

Il fatto che gli operatori di creazione e distruzione siano primati sta ad indicare che sono quelli in uscita dallo splitter, infatti, detti $\hat{a}$ l'operatore associato al segnale e α_{LO} l'ampiezza complessa (classica) del LO, si avrà:

$$\widehat{a'}_1 = \frac{1}{\sqrt{2}}\left(\hat{a} - \alpha_{LO}\right) \qquad \widehat{a'}_2 = \frac{1}{\sqrt{2}}\left(\hat{a} + \alpha_{LO}\right)$$

e ovviamente gli aggiunti saranno:

$$\widehat{a'}_1^{\dagger} = \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger} - \alpha_{LO}^{*}\right) \qquad \widehat{a'}_2^{\dagger} = \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger} + \alpha_{LO}^{*}\right)$$

Si ricavano dunque $\hat{n}_1$ e $\hat{n}_2$:

$$\hat{n}_1 = \frac{1}{2}\left(\hat{a} - \alpha_{LO}\right)\left(\hat{a}^\dagger - \alpha_{LO}^*\right) = \frac{1}{2}\left(\hat{a}\hat{a}^\dagger - \alpha_{LO}^*\hat{a} - \alpha_{LO}\hat{a}^\dagger + |\alpha_{LO}|^2\right)$$

$$\hat{n}_2 = \frac{1}{2}\left(\hat{a} + \alpha_{LO}\right)\left(\hat{a}^\dagger + \alpha_{LO}^*\right) = \frac{1}{2}\left(\hat{a}\hat{a}^\dagger + \alpha_{LO}^*\hat{a} + \alpha_{LO}\hat{a}^\dagger + |\alpha_{LO}|^2\right)$$

Da cui:

$$\Delta = \alpha_{LO}^*\hat{a} + \alpha_{LO}\hat{a}^\dagger$$

Scriviamo ora α_{LO} in termini di modulo ed anomalia come $|\alpha|e^{i\phi}$, il Δ sarà quindi:

$$\Delta = |\alpha|e^{-i\phi}\hat{a} + |\alpha|e^{i\phi}\hat{a}^\dagger$$

Gli operatori di creazione e distruzione possono essere scritti in funzione delle quadrature $\hat{x}$ e $\hat{p}$:

$$\hat{a} = \frac{1}{\sqrt{2}}\left(\hat{x} + i\hat{p}\right) \qquad \hat{a}^\dagger = \frac{1}{\sqrt{2}}\left(\hat{x} - i\hat{p}\right)$$

Con alcuni passaggi si arriva dunque a scrivere:

$$\Delta = \sqrt{2}|\alpha|\left(\hat{x}\cos\left(\phi\right) + \hat{p}\sin\left(\phi\right)\right) \equiv \sqrt{2}|\alpha|\hat{q}_\phi \propto \hat{q}_\phi$$

Che è ciò che si voleva, per $\phi = 0, \pi, 2\pi, \ldots, k\pi$ si va a misurare la quadratura $\hat{x}$, per $\phi = \frac{\pi}{2}, \frac{3\pi}{2}, \ldots, (2k+1)\frac{\pi}{2}$ si misura invece la quadratura $\hat{p}$.

2.2 I protocolli Switching

Dapprima descriveremo qui il protocollo Switching assumendo, per semplicità, che non ci siano attacchi in atto da parte di Eve. Attacco che invece sarà presente quando si andrà ad analizzare la sicurezza del protocollo. I calcoli espliciti dei rate d'informazione saranno svolti solo per un particolare tipo di attacco detto *incoerente*.

2.2.1 Descrizione del protocollo

L'apparato di base della CVQKD prevede che Alice e Bob comunichino sul canale quantistico mediante impulsi laser coerenti. Non appena nella postazione di Alice viene generato l'impulso laser questo viene splittato mediante uno specchio semi-riflettente in due fasci, uno di intensità molto maggiore dell'altro (tipicamente almeno in rapporto 90/10). Il fascio di intensità maggiore sarà l'oscillatore locale e viene mandato a Bob così com'è. Il fascio di intensità minore sarà invece quello che codifica l'informazione vera e propria: Alice modula ampiezza e fase di ciascun pacchetto in base a una coppia di variabili casuali che seguono una distribuzione gaussiana centrata in zero e di varianza ben definita. Una volta modulato l'impulso viene spedito a Bob. È da questi numeri casuali che si andrà poi ad estrarre una chiave binaria applicando ad esempio una funzione:

$$f : \mathbb{R} \longrightarrow \{0, 1\}$$

La più semplice e pratica funzione soddisfante questa condizione è la funzione θ di Heaviside:

$$\theta(x) = \begin{cases} 0 & \text{se } x < 0 \\ 1 & \text{se } x \geq 0 \end{cases}$$

Questo tipo di funzione ovviamente è la più semplice possibile, ha però il limite di associare alla quantità continua uno ed un solo bit d'informazione. Nella pratica, se non c'è troppo rumore si riescono ad associare più bit per singolo dato associando ad ogni regione di "dominio" di x una certa stringa di bit di lunghezza n.
Nella postazione di Bob arrivano quindi due fasci, il LO e il pacchetto quantistico modulato. Questi fasci, essendo stati generati dallo stesso impulso avranno una differenza di fase $\tilde{\phi}$ ben definita e costante, condizione essenziale per la misura omodina. Nella sua postazione Bob può variare la fase $\tilde{\phi}$ in una fase $\phi = \tilde{\phi} + \phi_{ext}$ scelta a piacere. La differenza di fase fra il segnale e l'oscillatore locale sarà dunque arbitraria ma costante per tutta la durata della misura. A questo punto Bob la misura omodina ottenendo un numero reale che rappresenta la quadratura $\hat{x}$ o $\hat{p}$, in base, ripetiamolo, alla fase ϕ che ha scelto.
Dopo aver ripetuto N volte questi passaggi, Alice e Bob avranno ciascuno un set di N numeri reali (e quindi bit) misurati ciascuno in una specifica quadratura. Se la linea di trasmissione fosse perfetta, le codifiche e le misure pure fossero perfette, a questo punto Alice e Bob condividerebbero una chiave di N bit. Nella pratica ciò non è vero, c'è sempre una certa quantità di rumore introdotto dalla linea o naturale, del vuoto. C'è quindi bisogno di una fase di "pulitura" della chiave che darà alla fine una frazione β degli N bit inizialmente in possesso di Alice e Bob.

Scriviamo ora in modo preciso quali sono gli stati che vengono inviati da Alice e ricevuti da Bob, analisi che sarà utile in seguito. Innanzitutto, per snellire la notazione d'ora in poi scriveremo $\hat{q}^+$ al posto di $\hat{x}$ e $\hat{q}^-$ anziché $\hat{p}$. Viene inoltre cambiata leggermente la definizione

degli operatori, viene omettesso il fattore di normalizzazione $1/\sqrt{2}$:

$$\hat{q}^+ = \hat{a} + \hat{a}^\dagger \qquad \hat{q}^- = i\left(\hat{a}^\dagger - \hat{a}\right) \qquad \left[\hat{q}^+, \hat{q}^-\right] = 2i$$

Come visto nelle sezioni precedenti, Alice invia a Bob uno stato le cui quadrature sono state modulate secondo una coppia di numeri casuali con distribuzine gaussiana, chiamiamo $S^\pm$ questi numeri. Come detto sarà $\langle S^\pm \rangle = 0$ e dunque la varianza sarà semplicemente $v_S^\pm = \left\langle (S^\pm)^2 \right\rangle$. Gli stati che Alice invia sono dunque rappresentabili come:

$$\hat{q}_A^\pm = S^\pm + \hat{N}_A^\pm$$

$$\hat{v}_A^\pm = v_S^\pm + 1$$

ove $\hat{N}_A^\pm$ è l'operatore associato allo stato di vuoto iniziale $|0\rangle$ il quale ha varianza sempre pari a 1, dimostriamolo ad esempio per la quadratura $\hat{x}$, ricordando che il valor medio è sempre nullo e che si assumono gli stati normalizzati:

$$v_{NA}^+ = \langle \hat{x}^2 \rangle_{|0\rangle} - \left(\langle \hat{x} \rangle_{|0\rangle}\right)^2 = \langle 0|\left(\hat{a} + \hat{a}^\dagger\right)^2|0\rangle = \langle 0|\hat{a}^2 + \hat{a}^{\dagger 2} + \hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}|0\rangle = \langle 0|\hat{a}\hat{a}^\dagger|0\rangle = \langle 0|0\rangle = 1$$

Sia ora η la trasmittività del canale e $\hat{q}_N$ l'operatore associato al rumore del canale di trasmissione quantistico, a Bob arriveranno degli stati rappresentabili da [6]:

$$\hat{q}_B^\pm = \sqrt{\eta}\,\hat{q}_A^\pm + \sqrt{1-\eta}\,\hat{q}_N$$

$$v_B^\pm = \eta\, v_A^\pm + (1-\eta)\; v_N$$

Nella prima equazione, il primo termine a secondo membro è semplicemente il segnale di partenza riscalato di un fattore $\sqrt{\eta}$ che rappresenta l'assorbimento di una frazione $(1-\eta)$ di fotoni e il secondo addendo si rende necessario per mantenere invariate le relazioni di commutazione descirtte in precedenza [6].

2.2.2 Cos'è l'informazione

Prima di descrivere entro quali limiti il protocollo è sicuro, andremo a descrivere brevemente la teoria dell'informazione che viene utilizzata per fare un'analisi quantitaiva di "quanta chiave" condividono Alice e Bob. Il discorso che faremo qui sarà altresì valido per il protocollo Non-Switching.
La teoria dell'informazione di Shannon [7] prevede che l'informazione condivisa fra, nel nostro caso, Alice e Bob sia data da:

$$I\left(B:A\right) = H(B) - H(B|A)$$

ove $H(B)$ è l'entropia di Shannon di Bob e $H(B|A)$ è l'*entropia condizionata* di Alice relativa alla misura di Bob, questa misura quanto in media Alice sia incerta sull'esito della misura di Bob.
Introducendo anche la figura di Eve si dovrà tener conto dell'informazione che Eve condivide con Bob:

$$I\left(B:E\right) = H(B) - H(B|E)$$

E si avrà ovviamente che l'informazione totale "buona" sarà la differenza fra l'informazione condivisa fra Alice e Bob e l'informazione condivisa fra Eve e Bob:

$$\Delta I = I\left(B:A\right) - I\left(B:E\right) = H(B|E) - H(B|A)$$

La teoria di Shannon prevede che l'entropia condizionata sia funzione di un'altra quantità, la *varianza condizionata*, in particolare per due eventi qualsiasi X e Y:

$$H(X|Y) = \frac{1}{2}\log_2\left(V_{X|Y}\right)$$

Nello specifico, $V_{A|B}$, la varianza condizionata fra Alice e Bob, rappresenta l'incertezza sulla stima che Alice fa del risultato della misura di Bob. Analogo discorso vale per $V_{E|B}$, la varianza condizionata fra Eve e Bob. Ancora, per due eventi generici X e Y aventi media nulla e legati da una relazione lineare (e sarà il caso di nostro interesse) la varianza condizionata $V_{X|Y}$ è data da [8]:

$$V_{X|Y} = \min_g \langle (X - gY)^2 \rangle$$

ove le parentesi angolate indicano l'operazione di valor medio e g è un parametro da stimare. La formula di cui sopra è una scrittura compatta che riduce ad una semplice operazione di minimo la ricerca del miglior stimatore della correlazione fra gli eventi X e Y.
Proviamo ora ad eseguire l'operazione di minimo prendendo la derivata dell'espressione di cui sopra rispetto a g e ponendola a zero:

$$0 = \frac{\partial}{\partial g}\langle (X - gY)^2 \rangle = \frac{\partial}{\partial g}\langle X^2 + g^2Y^2 - gXY - gYX \rangle = 2g\langle Y^2 \rangle - \langle XY \rangle - \langle YX \rangle$$

Supponiamo ora che $\langle XY \rangle = \langle YX \rangle$ ovvero, nel caso di operatori X e Y quantistici, che il loro commutatore sia nullo, si avrà:

$$g = \frac{\langle XY \rangle}{\langle Y^2 \rangle}$$

Ed è effettivamente un minimo in quanto un'ulteriore derivazione rispetto a g dà un valore positivo (il doppio del valor medio di Y^2, ovviamente positivo).
Sostituendo il valore di g trovato nell'espressione della varianza condizionata si trova:

$$V_{X|Y} = \left\langle \left(X - \frac{\langle XY \rangle}{\langle Y^2 \rangle} Y \right)^2 \right\rangle = \langle X^2 \rangle + \frac{\langle XY \rangle^2}{\langle Y^2 \rangle^2}\langle Y^2 \rangle - 2\langle XY \rangle \frac{\langle XY \rangle}{\langle Y^2 \rangle} = \langle X^2 \rangle - \frac{\langle XY \rangle^2}{\langle Y^2 \rangle}$$

2.2.3 Informazione del protocollo

Per porre un limite inferiore all'informazione fra Alice e Bob immaginiamo che Eve possa conoscere in modo perfetto entrambe le quadrature e che il rumore introdotto sulla linea di trasmissione sia tutto imputabile a lei. Questa situazine ovviamente non è fisicamente realizzabile, ma è anche una situazione molto favorevole a Eve da cui un sicuro limite inferiore all'informazine fra Alice e Bob. Andiamo ora a calcolare la varianza condizionata fra Alice e Bob $V^{\pm}_{A|B}$, ricordando che tutti gli operatori in gioco hanno media nulla e sono legati da relazioni lineari:

$$V^{\pm}_{A|B} = v^{\pm}_B - \frac{\left\langle S^{\pm}\hat{X}^{\pm}_B \right\rangle^2}{v^{\pm}_S}$$

Calcoliamo ora, ricordando che $\langle S^{\pm} \rangle = 0$ e che esso è un operatore classico, la quantità:

$$\left\langle S^{\pm} \hat{X}_B^{\pm} \right\rangle = \left\langle S^{\pm} \left(\sqrt{\eta}\, \hat{q}_A^{\pm} + \sqrt{1-\eta}\, \hat{q}_N \right) \right\rangle =$$

$$= \left\langle S^{\pm} \left(\sqrt{\eta}\, S^{\pm} + N_A^{\pm} + \sqrt{1-\eta}\, \hat{q}_N \right) \right\rangle = \sqrt{\eta} \left\langle \left(S^{\pm} \right)^2 \right\rangle = \sqrt{\eta}\, v_S^{\pm}$$

Sostituendo si ha quindi:

$$V_{A|B}^{\pm} = \eta + (1-\eta)\, v_N$$

Dovremo ora calcolare la varianza condizionata fra Eve e Bob $V_{E|B}^{\pm}$ e cercare di porvi dei limiti attraverso la $V_{A|B}^{\pm}$. Per fare ciò scriviamo degli operatori che denotano l'inferenza di Alice ed Eve sullo stato di Bob prima dello splitter, una sorta di operatore "padre" della varianza condizionata:

$$\hat{q}_{A|B}^{\mp} = \hat{q}_B^{\mp} - g_A^{\mp} \hat{q}_A^{\mp}$$

$$\hat{q}_{E|B}^{\pm} = \hat{q}_B^{\pm} - g_E^{\pm} \hat{q}_E^{\pm}$$

Questi operatori, ricordando che operatori di diversi spazi Hilbertiani commutano, avranno la seguente relazione di commutazione:

$$\left[\hat{q}_{E|B}^{\pm},\, \hat{q}_{A|B}^{\mp} \right] = \left[\hat{q}_B^{\pm} - g_E^{\pm} \hat{q}_E^{\pm},\, \hat{q}_B^{\mp} - g_A^{\mp} \hat{q}_A^{\mp} \right] = \left[\hat{q}_B^{\pm},\, \hat{q}_B^{\mp} \right] = 2i$$

Da cui dalla relazione di indeterminazione di Heisenberg:

$$V_{E|B}^{\pm} V_{A|B}^{\mp} \geq 1$$

Supponiamo, solo per ora, che gli stati che Alice invia siano stato *squeezed*, ovvero stati per cui il suo principio di indeterminazione sia saturato e che quindi valga l'uguaglianza, in questi casi si scrive dunque una nuova varianza $v_A^{\pm}$ [9]:

$$\hat{v}_A^{\pm} = v_S^{\pm} + v_{sqz}^{\pm}$$

col vincolo:

$$v_{sqz}^{\mp} \geq \frac{1}{v_A^{\pm}}$$

Rifacendo i conti di cui sopra si trova:

$$V_{A|B\,sqz}^{\pm} = \eta v_{sqz}^{\pm} + (1-\eta)\, v_N$$

Sarà dunque:

$$V_{A|B}^{\mp} \geq V_{A|B\,min}^{\mp} = \frac{\eta}{v_A^{\mp}} + (1-\eta)\, v_N$$

Ricordando la relazione di indeterminazione si potrà dare un limite alla varianza condizionata di Eve:

$$V_{E|B}^{\pm} \geq \frac{1}{\eta / v_A^{\mp} + (1-\eta)\, v_N}$$

e dunque, ricordano le definizioni precedenti:

$$\Delta I = \frac{1}{2} \log_2 \left(\frac{V_{E|B}^{\pm}}{V_{A|B}^{\pm}} \right) \geq \frac{1}{2} \log_2 \left(\frac{1}{\left(\eta / v_A^{\mp} + (1-\eta)\, v_N \right) \left(\eta + (1-\eta)\, v_N^{\pm} \right)} \right)$$

Normalemente si pone $v_A^{\pm} = v_A$ e quidni in definitiva si avrà:

$$\Delta I \geq \frac{1}{2} \log_2 \left(\frac{1}{(\eta / v_A + (1-\eta)\, v_N)\,(\eta + (1-\eta)\, v_N)} \right)$$

Come detto questo è solo un limite inferiore all'informazione ottenibile, un'analisi più dettagliata mostra in effetti che l'informazione ΔI avrà una forma del tipo:

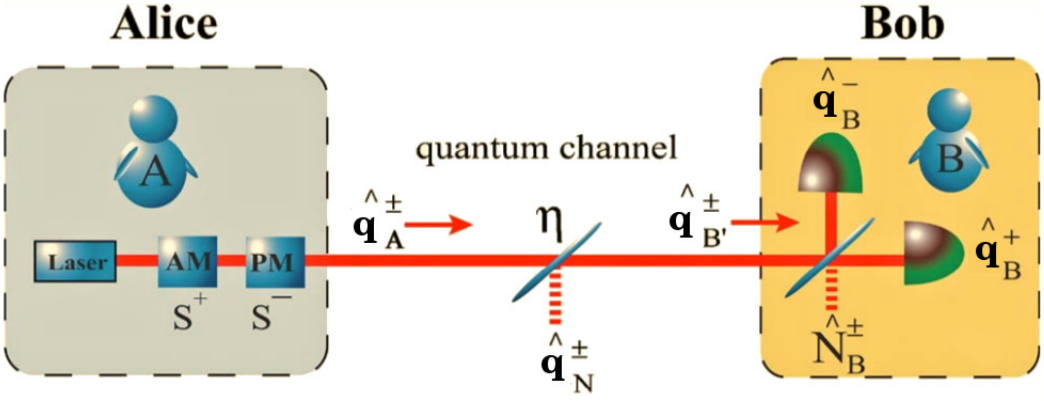
$$\Delta I = \beta I(A:B) - \Gamma(B:E)$$

con β un parametro minore di 1 che rappresenta l'efficienza degli algoritmi usati e Γ una qualche funzione che descrive l'informazione fra Eve e Bob che si ha in uno specifico tipo di attacco.

Saranno analizzati i risultati sperimentali di alcune implementazioni del protocollo Switching nel capitolo 3.

2.3 Il protocollo Non-Switching

Ciò che differenzia il protocollo Non-Switching da quello Switching è il fatto che vengono misurate entrambe le quadrature del segnale anziché una sola. Questo è reso possibile sdoppiando il sengale con uno splitter 50/50 ed eseguendo due misure omodine sui due fasci in uscita dallo splitter. Lo sdoppiamento del sengale non può però avvenire senza dover pagare un dazio quntistico: lo splitting introduce nei due sengali in uscita una certa quantità di rumore che va disturbare i risultati delle misure delle quadrature [6]. Lo splitter è infatti modellizzato come uno specchio semi-riflettente sul quale interferiscono lo stato del segnale e lo stato di vuoto, risultano quindi due fasci che sono combinazione del segnale proveniente da Alice e il rumore di vuoto.



Come nel caso precedente Alice prepara degli stati del tipo:

$$\hat{q}_A^{\pm} = S^{\pm} + N_A^{\pm}$$

$$v_A^{\pm} = V_S^{\pm} + 1$$

Alla postazione di Bob *prima* dello splitter arriverà uno stato descrivibile come:

$$\hat{q}_{B'}^{\pm} = \sqrt{\eta}\,\hat{q}_A^{\pm} + \sqrt{1-\eta}\,\hat{q}_N$$

$$v_{B'}^{\pm} = \eta\, v_A^{\pm} + (1-\eta)\; v_N$$

Dopo lo splitter, come detto, gli stati di Bob saranno sovrapposizione dello stato di cui sopra e del rumore di vuoto, mantendento la normalizzazione si avrà:

$$\hat{q}_B^{\pm} = \frac{1}{\sqrt{2}}\left(\sqrt{\eta}\,\hat{q}_A^{\pm} + \sqrt{1-\eta}\,\hat{q}_N + \hat{N}_B^{\pm}\right)$$

$$v_B^{\pm} = \frac{1}{2}\left(\eta\, v_A^{\pm} + (1-\eta)\; v_N + 1\right)$$

In questo protocollo l'informazione ΔI effettiva fra Alice e Bob (al netto dell'informazione di Eve) avrà due componenti ΔI_+ e ΔI_-, corrispondenti rispettivamente al contributo di informazione della quadratura $\hat{x}$ e $\hat{p}$. Ciascun contributo non sarà tuttavia uguale al corrispettivo del protocollo Switching a causa ancora una volta del rumore di vuoto introdotto dallo splitter. Trattando allo stesso modo le due quadrature si avrà che l'informazione totale sarà:

$$\Delta I = 2\,(H(B|E) - H(B|A))$$

2.3.1 Informazione del protocollo

Si cerca innanzitutto di porre un limite inferiore alla quantità di informazione fra Alice e Bob ΔI. Per fare ciò si immagina un attacco molto semplice da parte di Eve, anche se non realizzabile fisicamente. Si ipotizza che Eve possa utilizzare uno splitter ideale per misurare in modo perfetto entrambe le quadrature e che, come al solito, tutto il rumore sulla linea di trasmissione sia dovuto a lei.
Iniziamo con il calcolare la varianza condizionata $V^{\pm}_{A|B}$ fra Alice e Bob:

$$V^{\pm}_{A|B} = v^{\pm}_B - \frac{\left\langle S^{\pm}\hat{X}^{\pm}_B \right\rangle^2}{v^{\pm}_S}$$

Calcoliamo ora, ricordando che $\langle S^{\pm}\rangle = 0$ e che esso è un operatore classico, la quantità:

$$\left\langle S^{\pm}\hat{X}^{\pm}_B \right\rangle = \left\langle S^{\pm}\left[\frac{1}{\sqrt{2}}\left(\sqrt{\eta}\,\hat{q}^{\pm}_A + \sqrt{1-\eta}\,\hat{q}_N + \hat{N}^{\pm}_B\right)\right]\right\rangle =$$

$$= \left\langle S^{\pm}\left[\frac{1}{\sqrt{2}}\left(\sqrt{\eta}\,S^{\pm} + N^{\pm}_A + \sqrt{1-\eta}\,\hat{q}_N + \hat{N}^{\pm}_B\right)\right]\right\rangle = \sqrt{\frac{\eta}{2}}\left\langle \left(S^{\pm}\right)^2\right\rangle = \sqrt{\frac{\eta}{2}}v^{\pm}_S$$

La varianza condizionata sarà dunque, andando a sostituire le varie espressioni:

$$V^{\pm}_{A|B} = \frac{1}{2}\left[\eta + (1-\eta)\,v_N + 1\right]$$

Cerchiamo ora di legare la varianza condizionata fra Eve e Bob prima e dopo lo splitter di Bob:

$$V^{\pm}_{E|B} = \left\langle \left(\hat{q}^{\pm}_B - g^{\pm}_E\hat{q}^{\pm}_E\right)^2\right\rangle = \left\langle \left(\frac{1}{\sqrt{2}}\left(\hat{q}^{\pm}_{B'} + \hat{N}^{\pm}_B\right) - g^{\pm}_E\hat{q}^{\pm}_E\right)^2\right\rangle = \frac{1}{2}\left(1 + \left\langle \left(\hat{q}^{\pm}_{B'} - \sqrt{2}\,g^{\pm}_E\hat{q}^{\pm}_E\right)^2\right\rangle\right) =$$

$$= \frac{1}{2}\left(1 + \left\langle \left(\hat{q}^{\pm}_{B'} - g^{\pm}_{E'}\hat{q}^{\pm}_E\right)^2\right\rangle\right) = \frac{1}{2}\left(1 + V^{\pm}_{E|B'}\right)$$

Si procede ora esattamente con nel caso del protocollo switching, vale anche qui, prima dello splitter:

$$V^{\mp}_{A|B} \geq V^{\mp}_{A|B\,min} = \frac{\eta}{v^{\pm}_A} + (1-\eta)\,v_N$$

$$V^{\pm}_{E|B'} \geq \frac{1}{\eta/v^{\mp}_A + (1-\eta)\,v_N}$$

E quindi si avrà:

$$V^{\pm}_{E|B} \geq \frac{1}{2}\left(1 + \frac{1}{\eta/v^{\mp}_A + (1-\eta)\,v_N}\right)$$

Da cui:

$$\Delta I = \frac{1}{2}\log_2\left(\frac{V^{\pm}_{E|B}}{V^{\pm}_{A|B}}\right) \geq \log_2\left(\frac{1\left[\left(\eta/v^{\mp}_A + (1-\eta)\,v_N\right)^{-1} + 1\right]}{\eta + (1-\eta)\,v_N}\right)$$

E quindi:

$$\Delta I \geq \log_2\left(\frac{\left(\eta/v_A + (1-\eta)\,v_N\right)^{-1} + 1}{\eta + (1-\eta)\,v_N}\right)$$

Da confrontare col ΔI_{Sw} trovato nel caso dei protocolli Switching:

$$\Delta I_{Sw} \geq \frac{1}{2} \log_2 \left(\frac{1}{(\eta / v_A + (1-\eta)\, v_N)\, (\eta + (1-\eta)\, v_N)} \right)$$

Valgono le stesse considerazioni fatte in precedenza, in un applicazione reale il vero rate di informazione sarà una frazione β dello specifico ΔI di quell'implementazione.

2.4 La sicurezza dei protocolli

La nozione ideale di sicurezza di una chiave è quella che normalmente viene chiamata *sicurezza perfetta* ove, ogni chiave S è ugualmente plausibile agli occhi di una persona non autorizzata, Eve. In altre parole la distribuzione di probabilità $P(S)$ nello spazio di tutte le possibili chiavi è uniforme. Questa nozione di sicurezza implica che Eve non abbia nessun tipo di informazione sulla chiave S, situazione difficilmente realizzabile. Si passa quindi ad una nozione di sicurezza di tipo probabilistico basata appunto sullo studio dell'informazione condivisa fra le tre parti in gioco richiedendo che l'informazione che Eve possiede sulla chiave sia minore di un certo ε in modo tale che la chiave sia sicura con probabilità $1 - \varepsilon$.

I limiti inferiori d'informazione sopra descritti sono per un particolare tipo di attacco detto *incoerente*. In questo tipo di attacchi, Eve compie sempre lo stesso tipo di operazione su tutti i dati che transitano per il canale quantistico. Tutte le misure quantistiche che uno specifico tipo di attacco incoerente prevede devono essere effettuate prima della fase di postprocessing classico. Eve in questo tipo di attacchi non ha "memoria quantistica", non può immagazzinare lo stato quantistico e misurarlo in seguito. Questo non è certamente il tipo di attacco più generale possibile, ma si possono appunto calcolare facilmente i limiti d'informazione.
Si dimostra che un attacco qualsiasi tende asintoticamente (con la lunghezza della chiave) ad un tipo di attacco detto *collettivo* che si differenzia da quello incoerente per il fatto che Eve qui può effettuare le misure quantistiche quando meglio crede, anche dopo o durante il postprocessing classico. In questo caso Eve possiede dunque memoria quantistica.
Per questi attacchi la formula per calcolare l'informazione ha la formula generale vista nella sezione precedente:

$$\Delta I = \beta I(A : B) - \Gamma(B : E)$$

Ove βI è definita come al solito e Γ si dimostra essere della forma:

$$\Gamma(B : E) = g(\lambda_1) + g(\lambda_2) - g(\lambda_3)$$

Con

$$g(x) = (x + 1)\log_2(x + 1) - x\log_2(x)$$

e λ_i funzioni dei parametri fisici dell'apparato: trasmittività, efficienza della misura omodina, rumore introdotto dalla linea di trasmissione e della varianza delle quadrature v_A.
Nella pratica quindi, e lo vedremo nel prossimo capitolo, c'è un limite di rumore oltre il quale si ha un ΔI negativo dal quale non è possibile estrarre una chiave sicura e la trasmissione deve essere annullata.

2.4.1 La sicurezza composable

Torniamo per un momento nel contesto teorico dell'informazione classica, non quantistica. Detto M il messaggio da trasmettere e C il messaggio cifrato mediante la chiave S, se anche Eve conoscesse una frazione del messaggio in chiaro M (ad esempio conoscendo l'intestazione utilizzata da Alice sul messaggio per Bob), utilizzando l'algoritmo di cifratura OTP, descritto al capitolo 1, Eve conoscerebbe solo la frazione della chiave S relativa a quella parte di messaggio e nulla di più, non inficiando la sicurezza della trasmissione.
Passando al contesto quantistico è possibile dimostrare che ciò non è più vero [12]: la conoscenza

di una frazione del messaggio M, porta più informazione di quanto quella singola porzione di messaggio codifichi. È possibile infatti, conoscendo una frazione k di n bit del messaggio in chiaro, ottenere una certa frazione δ degli $n - k$ bit rimanenti della chiave S e quindi del messaggio M, inficiando notevolmente la sicurezza.
Per quantificare la sicurezza di una trasmissione alla luce di questo fenomeno quantistico si introduce la nozione di *sicurezza composable*, in cui una chiave è detta $\varepsilon-$sicura se:

$$\frac{1}{2}|\rho_{SE} - \omega \otimes \rho_E| \leq \varepsilon$$

ove $\rho_{SE} \in S \otimes H_E$ è lo stato, appartenente allo spazio prodotto fra lo spazio delle chiavi e quello quantistico di Eve, che rappresenta la chiave S e lo stato quantistico E di Eve, $\omega \in S$ è la sovrapposizione completa di tutte le possibili chiavi (in modo equiprobabile) e $\rho_E \in H_E$ è lo stato di Eve. La disequazione di cui sopra significa cioè che la chiave è sicura con probabilità $1 - \varepsilon$ se la distanza fra lo stato ottenuto e uno stato "qualsiasi", scelto in modo equiprobabile fra tutte le chiavi possibili (equivalente al non avere informazione da parte di Eve), è minore di ε.

Recentemente (febbraio 2015) si è dimostrata la sicurezza composable dalla CVQKD attaccata con attacchi di tipo collettivo e quindi, nel limite di grandi lunghezze di chiave n, da ogni tipo di attacco. [13]

Capitolo 3

Risultati e prestazioni odierne

In questo capitolo andreamo ad esporre i risultati sperimentali di due implementazione di protocolli di QKD. tutti e due i lavori si sono svolti nello scorso quinquennio e cercano di essere ognuno lo "stato dell'arte" di quel periodo. Saranno entrambe implementazioni di un protocollo di tipo Switching. [10][11]

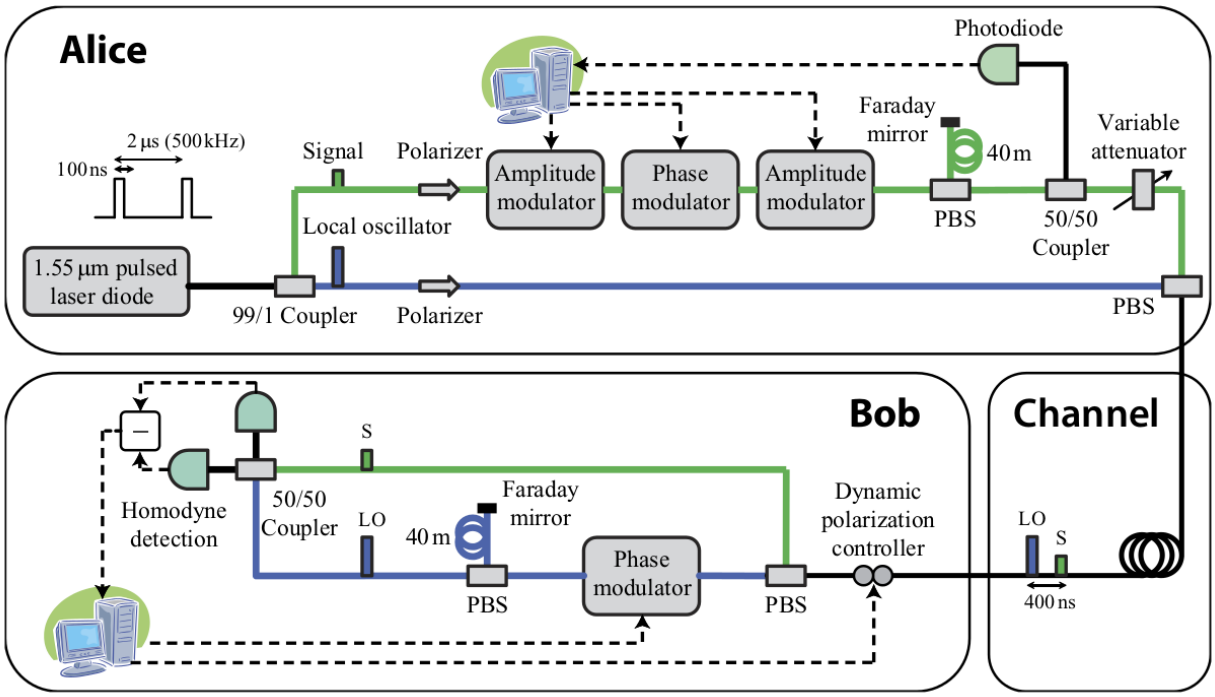
3.1 Implementazione Switching di 15 km nel 2009

In questo lavoro è stato implementato un protocollo di tipo Switching mediante laser con lunghezza d'onda di 1550 nm. Questa lunghezza d'onda, assieme a quelle intorno ai 1300 nm, è quella normalmente scelta per le telecomunicazioni su fibra ottica in quanto il materiale vitreo della fibra presenta dei minimi di assorbimento a queste due lunghezze d'onda nell'infrarosso ove si ha un assorbimento pari a 0.2 dB/km.

3.1.1 Apparato sperimentale

Alice nella sua postazione genera impulsi laser ad una frequenza di 500 kHz. ogni impulso dura 100 ns. La luce viene fatta passare in uno splitter che genera due fasci con rapporto 1/99 che saranno rispettivamente il sengale quantistico e l'oscillatore locale, entrambi sono successivamente polarizzati lungo una direzione ottima trovata automaticamente in modo stocastico dal sistema in fase di inizializzazione.
Il segnale quantistico viene ora modulato casualmente in ampiezza e fase secondo due distribuzioni gaussiane generate da un generatore di numeri quantistico, allo scopo di avere veri numeri casuali e non pseudocasuali che inficierebbero certamente la sicurezza del protocollo.
A questo punto il segnale viene multiplato con l'oscillatore locale per poter utilizzare una sola linea di trasmissione ottica. A tal scopo al segnale viene data una latenza di 400 ns (ricordiamo che ogni impulso è distante dall'altro di $1/500kHz = 2\mu$s) e ne viene ruotata la polarizzazione di 90 gradi mediante uno specchio di Faraday. Questo riduce al minimo gli effetti di *cross-talk* e quindi di interferenza fra i due segnali. A questo punto il segnale multiplato viene spedito a Bob tramite una linea di fibra ottica lunga 15km corrispondente ad un'attenuazione di 3 dB.
Nella postazione di Bob il segnale totale viene demultiplato e quindi vengo separati il sengale quantistico e l'oscillatore locale. Dopo aver imposto la fase scelta all'oscillatore locale per la misura omodina, subisce gli stessi passaggi che ha subito il segnale quantistico nella postazione di Alice: viene ritardato di 400 ns e viene anche qui ruotata la polarizzazione di 90 gradi, in

questo modo l'oscillatore locale si trova, rispetto al segnale quantistico, nelle stesse condizioni "pre-multiplazione", solo con una differenza di fase ben definita (che, come detto sarà quella che determinerà quale delle due quadratura verranno misurate).
Si procede quindi con la misura omodina del segnale il cui risultato è salvato in un computer per la successiva fase di post-processing.
In entrambe le postazioni sono presenti dei controlli di *feedback* che correggono i parametri sperimentali dei polarizzatori e degli altri apparati al fine di eliminare i disturbi dovuti a variazioni di temperatura, vibrazioni e altri fattori esterni che andrebbero a disturbare tutte le calibrazioni. Tutto l'apparato è sostanzialmente controllato da due computer. L'intera fase di inizializzazione dell'apparato dura all'incirca un minuto, durante il quale si assume, ed è ragionevole farlo, che tutti i parametri esterni rimangano costanti.



Prima di comiciare la QKD, Alice e Bob devono stimare i parametri relativi a trasmittività (globale) ed efficienza del loro apparato in modo tale da poter in seguito stimare il loro ΔI.
Fatto questo si passa alla fase di QKD vera e propria in cui Alice e Bob si scambiano $n = 2 \cdot 10^6$ impulsi, ciascuno darà, come visto, un valore continuo. Ogni valore continuo scambiato rappresenta qui 4 bit di chiave grezza, il dominio della gaussiana è diviso in 16 parti ($2^{4\,bit} = 16$ combinazioni) in modo tale che ciascuna regione (e quindi combinazione di bit) sia equiprobabile:

$$\int_{\Delta_i} Gauss(x;\sigma)\,dx = \frac{1}{16} \qquad \forall \Delta_i \qquad i = 1, ..., 16$$

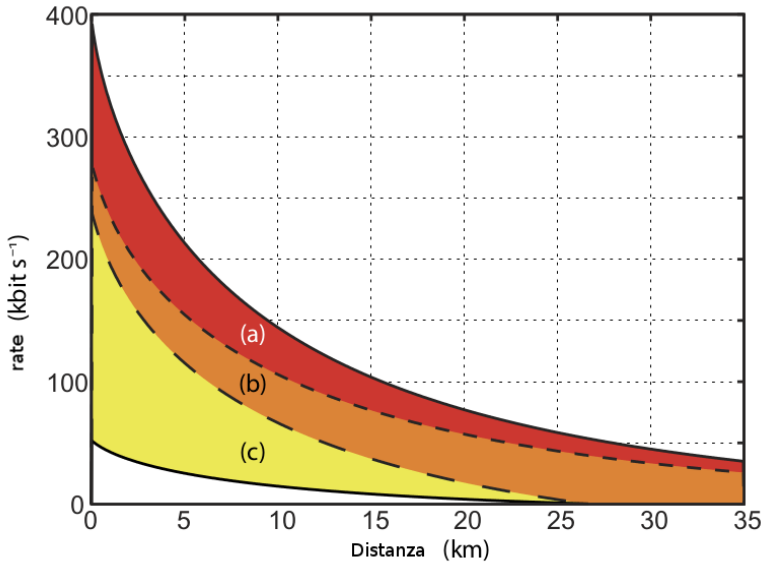
La funzione f (al capitolo 2 avevamo supposto fosse una $\theta(x)$) che associa quindi una stringa binaria ad ogni valore continuo è del tipo:

$$f(x) = \begin{cases} 0000 & \text{se } x \in \Delta_1 \\ 0001 & \text{se } x \in \Delta_2 \\ ... & \\ 1110 & \text{se } x \in \Delta_{15} \\ 1111 & \text{se } x \in \Delta_{16} \end{cases}$$

Una volta scambiati i $4n$ bit si procede a valutare la "bontà della canale" e quindi a stimare il ΔI (si assumono possibili attacchi da parte di Eve con memoria quantistica), per fare questo vengono usati metà degli impulsi scambiti, 1 milione. Se il ΔI risultante è positivo si procede alla fase di correzione degli errori. È importante notare che, in questa fase, sul canale classico devono transitare $32 \cdot n/2$ bit, la fase e l'ampiezza di metà degli impulsi che Alice invia a Bob sono codificati ciascuno in 16 bit.
L'algoritmo di correzione degli errori qui utilizzato è detto *low-density parity-check* di cui non ci occuperemo. Diremo solo che questa fase richiede numerose piccole comunicazioni sul canale classico che ha però una certa latenza, anche se piccola. Questa piccola latenza moltiplicata però per il gran numero di trasmisioni singole comporta un certo tempo sprecato, a svantaggio del rate K = *lunghezza chiave/tempo totale impiegato* che è il principale indice di prestazioni delle implementazioni QKD.
Finita la fase di correzione degli errori Alice e Bob condivideranno una chiave identica e Eve avrà inevitabilmente alcune porzioni di essa (compatibilmente col ΔI calcolato in precedenza). Si procede ora alla *privacy amplification* ove Alice e Bob applicano una funzione di hashing alla loro chiave grezza per ottenere la chiave finale sicura. La lunghezza finale media della chiave è in questo caso pari a 150 kbit.

3.1.2 Risultati e prestazioni

I parametri strumentali di efficienza e trasmittività qui presenti consentono una rate teorica di 100 kbit/s, valore che però è diminuito di circa un ordine di grandezza da vari fattori.
In primo luogo una diminuzione del rate è dato da una componente variabile di rumore che va ad influenzare sostanzialmente la fluttuazione del numero di fotoni che giungono a Bob, andando a disturbare inevitabilmente l'ampiezza del segnale. Questa componente di rumore varia dal 0 al 10% del rumore totale e il rate di QKD scende con andamento grossomodo lineare.
Un secondo motivo di riduzione del rate è l'efficienza non perfetta degli algoritmi di correzione degli errori, il β di questa implementazione risulta essere 0.9, ovvero un'efficienza del 90%.
L'ultima e più importante causa di riduzione della rate sta nella lentezza di esecuzione degli algoritmi di correzione degli errori e nella latenza di comunicazione sul canale classico, la trasmissione quantistica dura in tutto circa 5 secondi, la fase di correzione degli errori circa 24 secondi e la privacy amplification altri 5 secondi. Il rate effettivo della chiave, si calcola, è quindi 6 volte più basso rispetto al rate ottico di trasmissione, rivelando il vero collo di bottiglia attuale della QKD. È stato inoltre eseguito l'algoritmo di correzione degli errori su di una CPU a 4 core riducendo il tempo totale di eleborazioine di circa un fattore 2.
Durante le 57 ore di esperimento, che dimostrano un'indubbia stabilità del sistema, si sono generate chiavi il rate medio di 8 kbit/s.



Nell'immagine sopra la linea continua rappresenta il rate teorico, la linea (a) la diminuzione dovuta al rumore esterno, la linea (b) la riduzione dovuta all'efficienza < 1 *degli algoritmi di correzione degli errori e la linea (c) rappresenta la diminuzione dovuta alla lentezza degli algoritmi che comporta la non generazione della chiave in tempo reale rispetto alla trasmissione ottica.*

Dai risultati qui esposti si vede come 25 km sembrano rappresentare, al momento, il limite massimo per la CVQKD. Limitazione dovuta, ripetiamolo, più che alla trasmissione ottica hardware all'imperfezione degli algoritmi di correzione degli errori e alla lentezza della loro esecuzione. Questo è il principale svantaggio rispetto alla QKD a variabili discrete che, richiedendo una fase di correzione degli errori meno importante è meno affetta da questo problema, ma è limitata più sull'hardware di trasmissione ottica.

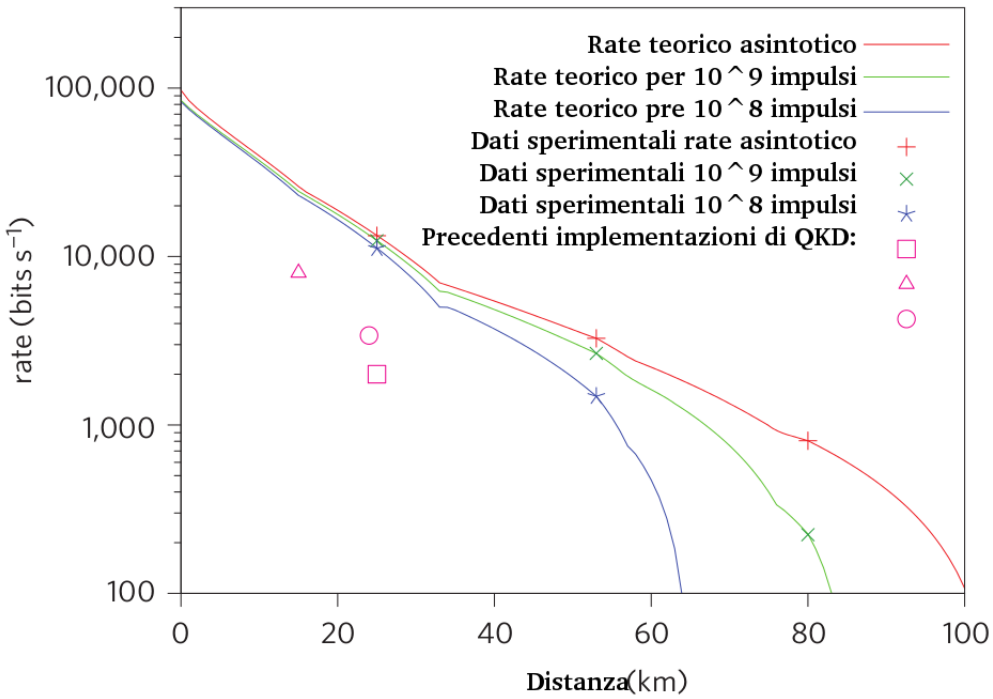
3.2 Implementazione Switching di 80 km nel 2013

3.2.1 Apparato sperimentale

L'apparato sperimentale è molto simile al precedente, la struttura è esattamente la stessa, con degli accorgimenti per sfondare la barriera dei 25 km ed arrivare ad una trasmissione su un canale ottico di ben 80 km.
Viene raddoppiata la frequenza di emissione degli impulsi laser che passa da 500 kHz a 1 MHz e viene contestualmente dimezzata la distanza temporale per la multiplazione di oscillatore locale e segnale quantistico che passa da 400 ns a 200 ns.
Si è passati inoltre ad un treno di 10^8 e poi 10^9 impulsi contro i $2{\cdot}10^6$ dell'esperimento precedente, questo è importante perchè si è più vicini al contesto asintotico dove sono calcolati i vari rate d'informazoine teorici senza dover tenr conto di effetti "di bordo" dovuti alla finitezza della chiave che incidono negativamente sul rate stesso.
Sono usati degli algoritmi di correzione degli errori che garantiscono qui un $\beta = 0.95$ al costo di una maggiore complessità computazionale. Quest'ultima limitazione è mitigata dal fatto che gli algoritmi qui utilizzati sono altamente parallelizzabili e sono qui eseguiti su di una GPU (Graphics Processor Unit) implementati tramite linguaggio *OpenCL*. Si sfruttano infatti il gran numero di unità di elaborazione presenti nelle moderne GPU, numero dell'ordine di 10^3, contro le massime 8/16 delle CPU. L'hardware qui utilizzato riesce a gestire circa 10 Mbit/s di chiave grezza.
La fase di privacy amplification è ancora eseguita su di una normale CPU che comunque, per questo algoritmo, raggiunge un rate di 40 Mbit/s, al prezzo di ridurre di un fattore 10^3 la lunghezza della chiave. Tutto questo permette di eseguire gli algoritmi di error-correction e quindi, in sostanza, di generare la chiave finita quasi in tempo reale rispetto alla trasmissione ottica.
Da notare anche qui che la stabiltà dell'apparato è qui eccelsa in quanto permette uno scambio continuo di chiave per anche 10^9 segnali. Una acquisizione di tal numero di dati dura infatti circa un'ora in cui l'apparato deve lavorare in modo continuativo. Sono ovviamente anche qui presenti tutta una serie di controlli automatici sull'apparato che regolano in continuazione i parametri di polarizzazione e attenuazione dei segnali.

3.2.2 Risultati e prestazioni

I risultati dell'esperimento sono ben riassumibili dall'immagine seguente ove vengono mostrati i rate teorici e misurati in funzione della distanza di trasmissione:



Si nota un netto miglioramento rispetto al precedente esperimento, spostando il limite massimo pratico ad una distanza intorno ai 100 km, quadruplicando di fatto il limite precedente. Si vede dal grafico che si riescono a raggiungere le prestazioni della precedente implementazione (ordine del kbit/s) per distanze quasi quattro volte maggiori: quasi 55 km contro 15.
I diversi rate previsti (ed effettivamente misurati) per diverse dimensioni di chiave sono dati da "fenomeni di bordo" dovuti alla finitezza della chiave di cui in questo esperimento si è tenuto conto. A 80 km non è posibile trasmettere una chiave sicura a partire da blocchi di 10^8 segnali, si ha un rate di circa 300 bit/s per blocchi di 10^9 segnali e il rate asintotico è intorno al kbit/s.

Anche un'implementazione di questo tipo non raggiunge tuttavia la prestazioni velocistiche di implementazioni di QKD a variabili discrete. È indubbio però che al costo di una maggiore lentezza di trasferimento, la CVQKD qui presentata è meno onerosa in termini di risorse hardware ottiche, si possono utilizzare in modo semplice le linee di trasmissione in fibra ottica già presenti semplicemente andando a modificare ciò che si invia e ciò che si riceve per sfruttare appunto le proprietà quantistiche della luce.

3.2.3 Possibili miglioramenti

Possibili fronti di miglioramento sono rappresentati da un ulteriore aumento della frequenza di invio dei segnali, superando la qui implementata soglia del MHz. Contestualmente si può migliorare l'efficienza degli algoritmi di correzione degli errori che vanno a "sprecare" qui molti bit di chiave grezza per distillare la chiave finale, la mole di dati che poi viene scambiata sul canale classico rischia di diventare così massiccia da saturare lo stesso.
Sono inoltre in fase di studio delle tecniche di *noiseless amplification* [14] e *virtual amplification* [15] (di cui non ci occuperemo), che cercano di amplificare il segnale (nel senso quantistico, probabilisitico) al fine di ridurre il rumore di linea, garantendo meno errori da correggere nella chiave grezza. Diremo solo che con queste tecniche assumento un parametro g rappresentante il guadagno di amplificazione, si dimostra essere possibile allungare (a parità di rumore) la linea di un fattore proporzionale a $\log_{10} g$.
È da valutare se le complicazioni che l'implementazione di protocolli di tipo Non Switching indubbiamente porterebbero, sono compensate da un rate sostanzialmente maggiore.

Capitolo 4

Conclusioni

In questo lavoro si è cercato di dare una panoramica sulla situazione attuale della distribuzione di chiave quantistica mediante l'uso di variabili quantistiche a spettro continuo. Questa variante della QKD "classica", basata su variabili quantistiche a spettro discreto, ha avuto uno sviluppo molto recente ed è tuttora in fase di studio. Si è visto dal punto di vista terico su quali presupposti si basa e come di recente si siano realizzate diverse implementazioni che hanno dimostrato di funzionare secondo le attese, implementazioni che per ora rimangono solo a livello di prototipo.
Se da un lato la CVQKD ha il vantaggio di poter sfruttare infrastrutture di trasmissione ottica pre-esistenti e apparecchi hardware molto veloci ed efficienti, essa trova il suo limite nella (non) efficienza degli algoritmi di *error-correction*, necessari all'estrazione della chiave finale. Come più volte ribadito, per la CVQKD servono algoritmi di correzione degli errori più sofisticati in quanto bisogna correggere sempre il rumore di linea. Questi algoritmi portano a diversi possibili colli di bottiglia, dalla lentezza nella loro esecuzione, al numero di bit di chiave grezza che "sprecano" o alla grande mole di dati che affolla il canale classico.
Questa situazione è per così dire speculare a quella della QKD a variabili discrete dove il principale limite attuale sta nella costruzione e nella gestione dell'hardware, che deve lavorare a singolo fotone. Non essendoci rumore di linea "di base" non sono qui necessari algoritmi di error-correction sofisticati e quindi questi non vanno a limitare le prestazioni di QKD.
Allo stato attuale delle cose la CVQKD è indietro in termini prestazionali alla QKD a variabili discrete che ha dalla sua un periodo di sviluppo sia teorico che sperimentale più lungo. Resta il fatto che in generale la QKD è una tecnica di crittografica decisamente recente ed è una delle applicazioni "a grande scala" della Meccanica Quantistica.
In futuro è possibile che le tecniche di QKD saranno utilizzate in quegli ambienti in cui la sicurezza è cruciali se gli attuali meccanismi crittografici si rivelassero non più adeguati.

Bibliografia

[1] Rijndael, AES Standard, 2001

[2] Shannon, C. E., 1949, Bell Syst. Tech. J. 28, 656.

[3] Bennett, C. H. and G. Brassard, 1984, Proceedins IEEE International Conference on Computers, Systems and Signal Processing

[4] Bennett, C. H., G. Brassard, and J.-M. Robert, 1988, SIAM J., Comput. 17, 210.

[5] S. Fossier, E. Diamanti, P. Grangier, Field test of a continuous-variable quantum key distribution prototype, New Journal of Physics 11 (2009) 045023

[6] Measuring the Quantum State if Light, U. Leonhardt, Cambridge University press, 1997

[7] C. E. Shannon, Bell Syst. Tech. J. 27, 623 1948.

[8] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information Cambridge University Press, Cambridge, U.K., 2000

[9] Weedbrook Phys. Rev. A 73, 022316 (2006)

[10] Fossier, Grangie,r New Journal of Physics 11 (2009) 045023

[11] Jouguet, Leverrier, Grangier, DOI: 10.1038/NPHOTON.2013.63

[12] Konig, Renner, 98, 140502 (2007) Phys. Rev. Letter

[13] Anthony Leverrier, Phys. Rev. Letter 114, 070501 (2015)

[14] Blandino, R. et al. Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier.Phys. Rev. A 86, 012327 (2012).

[15] Fiurasek, J. Cerf, N. J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys. Rev. A 86, 060302(R) (2012)