UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria

Corso di Laurea in Ingegneria Informatica

Tesi Di Laurea

Simulazione GM-CVQKD

Laureando

Kevin Santodonato

Matricola 548019

Relatore

Prof. Matteo Rosati

Anno Accademico 2022/2023

Questa è la dedica

Ringraziamenti

Grazie a tutti

Introduzione

Questa è l'introduzione

Indice

Elenco delle figure

Capitolo 1

Descrizione quantistica di un segnale

1.1 Stati coerenti e le loro proprietà

I segnali elettromagnetici possono essere descritti sia attraverso onde che attraverso particelle, ovvero fotoni. Ad esempio, il segnale prodotto da un LASER è ben rappresentato da uno stato quantistico detto stato coerente. Esso comunemente è rappresentato $|\alpha_j\rangle = |q_j + ip_j\rangle$ attraverso la notazione introdotta da Paul Dirac che prende il nome di *bra-ket*. Dal punto di vista della fisica classica, il numero complesso α è strettamente legato all'ampiezza di oscillazione del campo elettrico corrispondente al segnale. Esso è costituito da due componenti reali, q e p, dette componenti di quadratura. Dal punto di vista della fisica quantistica, tuttavia, non è possibile assegnare un valore preciso a queste grandezze. Infatti, i valori di q e p che utilizziamo per rappresentare lo stato coerente sono solo valori medi. Quando proviamo a fare una misurazione delle grandezze fisiche associate, che indichiamo con $\hat{q}$ e $\hat{p}$, esse si comportano come variabili aleatorie che rispondono alla stessa distribuzione di probabilità gaussiana che, in oppurtune unità di misura, ha varianza unitaria. Il motivo per cui non rappresentano un valore esatto è perché, a differenza fisica classica, nel fisica quantistica le quantitá, anche scalari, sono degli operatori che assumono una valore esatto solamente in fase di misura.

Ogni stato coerente presenta un numero medio di fotoni che può essere calcolato nel seguente modo:

$$\langle n_j \rangle = |a_j|^2 = q^2 + p^2 \tag{1.1}$$

Il numero medio di fotoni di uno stato coerente è associato all'energia del segnale di luce che viene inviato, maggiore è il numero di fotoni maggiore è l'energia del segnale.

Come detto precedentemente, nel nostro caso gli stati coerenti si presentano come una distribuzione di probabilità gaussiana e possono essere rappresentati graficamento nel piano di Gauss come una nuvola di punti i quali avranno appunto probabilità gaussiana di essere estratti.

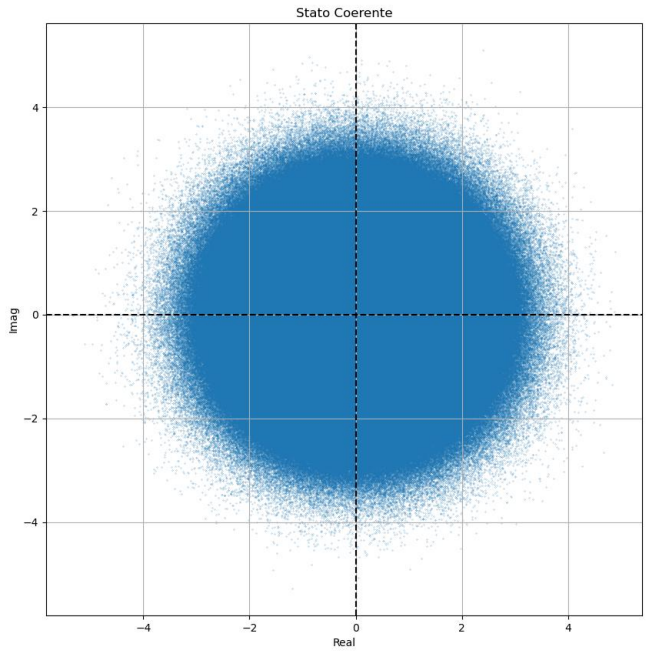

Figura 1.1: Figura da inserire—> Stato coerente –>Da apportare modifica consigliata dal professore

1.2 Misurazione dei segnali e incertezza quantistica

Partendo dal caso ideale, in cui il canale di comunicazione è perfetto e quindi non aggiunge rumore durante la trasmissione, Bob riceverà uno stato coerente con la forma vista in figura 1.1. Da notare che l'incertezza della misura è presente anche nel caso di un canale di comunicazione ideale, questo perché non è dovuta solamente al rumore esterno, come ci si aspetterebbe in un canale di comunicazione classico, ma è una caratteristica intriseca di uno stato quantistico la quale non può essere rimossa **((o attenuata) da chiedere al professore)** in base al principio di indeterminazione di Heisenberg. Questa incertezza si presenta proprio in fase di misura, perché come detto nella sezione 1.1, i valori di quadratura q e p sono solamente valori medi mentre i valori $\hat{q}$ o $\hat{p}$ che otteniamo da una misura 2.1.1 si comportano come variabili aleatorie con distribuzione di probabilità gaussiana.

In un trasmissione reale, l'aggiunta di rumore esterno è inevitabile e in questo rumore è presente anche quello prodotto ad un eventuale spia (Eve) che tenta anch'essa di misurare il segnale modificandolo, questo rende la misura di Bob ancora più incerta.

Per concludere possiamo dire che le QKD utlizzano le caratteristice dei segnali quantistici per cui c'è un incertezza nella misura anche in assenza di rumore esterno e che una misura introduce rumore proprio per determinare l'eventuale intromissione di Eve nella comunicazione e quindi la possibilità o meno di creare una chiave crittografica sicura.

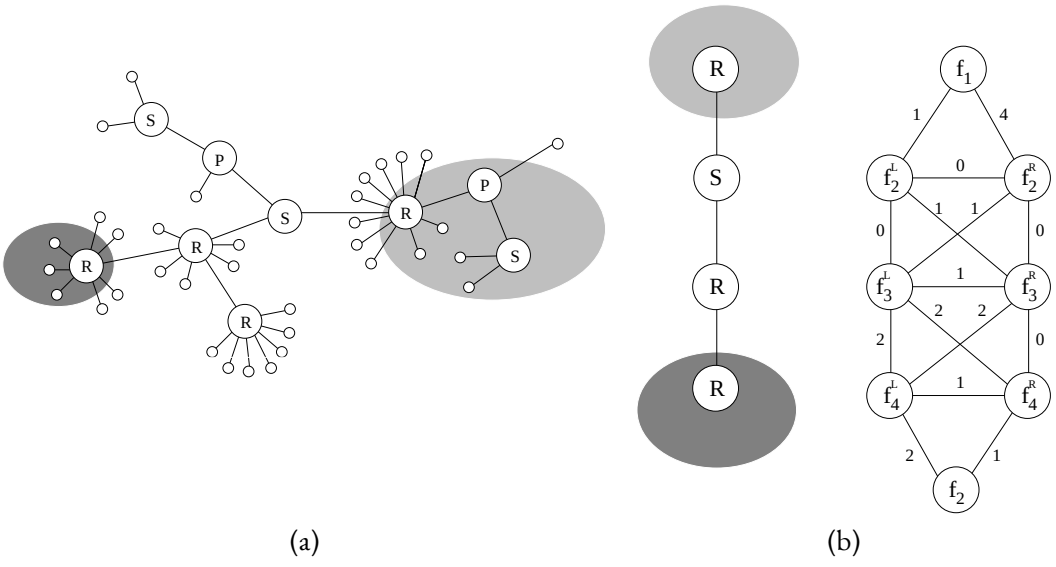

Figura 1.2: Figura da inserire—> confronto tra gaussiano con spia e senza spia

Capitolo 2

Quantum Key Distribution

La QKD (Quantum Key distribution), o Distribuzione Quantistica delle Chiavi, è una tecnologia di crittografia quantistica che permette la distribuzione di chiavi crittografiche con un livello di sicurezza inattacabile anche da computer quantistici. La QKD può essere suddivisa in due macro-classi DV-QKD e CV-QKD. Nella DV-QKD (Descrete Variable Quantum Key Distribution) le informazioni vengono trasmesse utilizzando stati quantici discreti, ad esempio la polarizzazione degli fotoni, che viene misurata attravarso apposite apparecchiature per ogni fotone; al contrario nella CV-QKD (Continous Variable Quantum Key Distribution) vengono misurate variabili continue delle onde elettromagnatiche come ad esempio la fase.

La sicurezza é garantita dai principi delle fisica quantistica che ci permettono di rilevare eventuali intercettazioni da parte di Eve (spia) nella trasmissione su canale quantistico tra Alice (mittente) e Bob (destinatario).

La rilevazione è dovuta al fatto che durante la misura da parte di Eve lo stato quantistico viene alterato facendo diminuire l'energia del segnale e introducendo del rumore, quindi dell'incertezza. All'atto pratico Eve intercetta lo stato coerente, rappresentato come in figura 1.1, ne effettua una misura per poi ritrasmetterlo sul canale. Bob riceverà uno stato coerente con del rumore aggiunto e un minor

numero di fotoni, ciò comporta che la gaussiana che lo rappresenta sarà caratterizzata da una varianza superiore a quella stimata e un valor medio più vicino allo zero. Per questo motivo, si effettuano numerosi run di trasmissione quantistica. In una fase preliminare si utilizza un certo numero di run per stimare i parametri di rumore del canale e, da essi, decidere se la trasmissione sta avvenendo in modo sicuro oppure no (si veda Sez. 2.1.2). Nel caso in cui il controllo non vada a buon fine, la trasmissione corrente viene abbortita perché non è possibile garantire la sicurezza della chiave crittografica.

2.1 CV-QKD con modulazione gaussiana

Il protocollo di distribuzione quantistica di chiavi a variabili continue con modulazione gaussiana è un protocollo molto indicato per lo sviluppo e l'utilizzo su larga scala nel mondo reale data la sua affinità con le infrastrutture oggi già esistenti, come ad esempio, i canali di comunicazione in fibra ottica. Come enunciato all'inizio del capitolo con questo protocollo si effettuano misure su variabili continue delle onde elettromagnetiche e in particolare nei protocolli con modulazione gaussiana gli stati coerenti da trasmettere sul canale di comunicazione vengono estratti da una distribuzione normale centrata in zero e una certa deviazione standard che viene definita in base ad alcuni fattori.

Il protocollo può essere suddiviso un due sezioni: la prima parte ha effettivamente a che fare con segnali quantistici mentre la seconda parte opera con segnali e dati classici. La prima sezione comprende la scelta e la trasmissione degli stati coerenti su fibra ottica da parte di Alice e termina nel momento in cui Bob effettua la misura; la seconda parte comprende il sifting, la stima dei parametri e la riconciliazione.

2.1.1 Produzione, trasmissione e ricezione del segnale quantistico

Alice prepara gli stati coerenti andando a estrarre i valori delle componenti di quadratura q e p da una distribuzione normale centrata in zero ($Q \sim P \sim N(0, V_{mod})$) [LPF+18]. Da notare che la

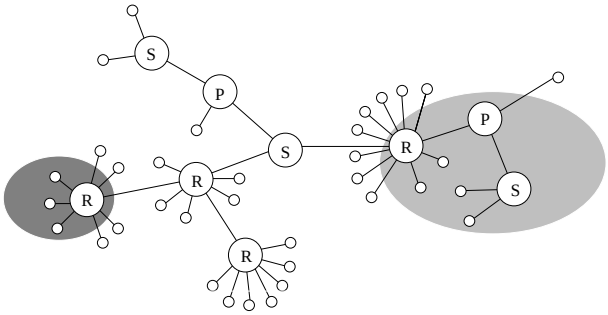

Figura 2.1: Schema che descrive le fasi del protocollo facendo particolare attenzione al canale quantistice e canale classico.

distribuzione normale dalla quale Alice estrae le componenti di quadratura non ha nulla a che fare con le distribuzioni normali che caratterizzano gli stati coerenti ma rappresenta in modo in cui i dati vengono modulati. Dopo la preparazione Alice trasmette a Bob gli stati coerenti attraverso un canale quantistico.

Il canale è caratterizzato da un certo valore di trasmittanza T e di rumore ξ. A causa della trasmittanza durante la trasmissione il segnale perde potenza quindi le gaussiane che descrivono lo stato coerente saranno centrata in un valore più vicino allo zero rispetto al momento della preparazione, mentre il rumore che viene introdotto fa aumentare la varianza delle gaussiane così da accrescere l'incertezza nelle misure da parte di Bob.

Per dare una rappresentazione matematica di quello che avviene ad uno stato coerente durante la trasmissione, possiamo andare a cosiderare un generico stato scelto da Alice $|a_i\rangle = |q_A + ip_A\rangle$. Come abbiamo detto nella sezione 1.1 le componenti di quadratura rispondono ad una distribuzione

di probabilià normale, quindi avremo:

$$\begin{aligned} q_A &\sim N(q_A, 1) \\ p_A &\sim N(p_A, 1) \end{aligned} \tag{2.1}$$

In ricezione, a causa del canale, Bob andrà ad effettuare la misura su uno stato coerente alterato $|b_i\rangle = |q_B + ip_B\rangle$ dove le componenti di quadratura rispondono alle seguenti distribuzioni gaussiane:

$$\begin{aligned} q_B &\sim N(\sqrt{T}q_B, 1 + \xi) \\ p_B &\sim N(\sqrt{T}p_B, 1 + \xi) \end{aligned} \tag{2.2}$$

Per la misura dello stato coerente possono essere adottati due metodi diversi:

- **misura omodina**: Bob decide se misurare la componente di quadratura q o p, la decisione viene presa attraverso una distribuzione di probabilità uniforme.
- **misura eterodina**: questa misura permette di misurare entrambe le componenti contemporaneamente, però c'è un prezzo da pagare perché effettuando questa misura viene aggiunto del rumore e la varianza delle distribuzioni normali ha un incremento di 1.

In caso di misura omodina è necessaria un'operazione addizionale cioé il sifting. A questo punto del protocollo Alice è in posseso del doppio dei dati di Bob (in quanto Bob misura solo una della due componenti per ogni round) e per far si che abbiano la stessa quantità di dati correlati Bob rivela ad Alice, su canale classico publico, quale componente ha misurato ad ogni round; Alice prende nota della componenti misurate e scarta le altre.[MFZG18]

2.1.2 Stima dei parametri

Dopo avere terminato la fase di trasmissione degli stati, Alice e Bob rivelano una porzione random di dati in modo tale da confrontare ciò che è stato effetivamente inviato da Alice con le misure di Bob. Da questo confronto sono in grado di stimare l'effettiva trasmittanza e rumore in eccesso del

canale di trasmissione e con queste stime possono calcolare l'informazione mutua I_{AB} (informazione mutua tra Alice e Bob) e l'informazione mutua tra Eve e Bob χ_{EB}. Nel caso in cui χ_{EB} risulti essere maggiore di βI_{AB} [1] il protocollo viene abbortito.

2.1.3 Riconciliazione delle informazioni

Se la stima dei parametri ha avuto successo Alice e Bob effettuano una correzione degli errori dei segnali scambiati. La riconciliazione può avvenire in due forme:

- **diretta**: i dati di Alice sono i dati primari e Bob corregge i suoi dati di conseguenza.
- **inversa**: in questo caso sono i dati di Bob ad essere primari, vengono inviati ad Alice la quale li utilizza per correggere i propri dati.

La riconciliazione diretta presenta un problema: non può essere utilizzata per valori di trasmittanza troppo bassi, questo perché Eve avrebbe piú informazione sui dati di Alice rispetto a Bob e quindi risulterà impossibile creare una chiave crittografica sicura. D'altro canto la riconciliazione inversa non presenta questo problema quindi è possibile utilizzarla anche con valori bassi di trasmittanza, però è da tenere in considerazione che più bassa è la trasmittanza più sarà distruttivo l'effetto del rumore del canale.[LPF+18]

A questo punto del protocollo Alice e Bob sono possesso del subset di dati non utilizzati per la stima dei parametri che andiamo a chiamare $\mathbf{X}_0$ e $\mathbf{Y}_0$; prima di effettuare la reconciliazione vengono prodotte, a partire dai dati in loro possesso, altre due sequenze di dati correlati.

Quello che ci aspettiamo è che le varianze dei dati il possesso ad Alice e Bob siano rispettivamente:

$$\begin{aligned} V_{X_0} &= V_{mod} + 1 \\ V_{Y_0} &= TV_{mod} + 1 + \xi \end{aligned} \tag{2.3}$$

[1] β rappresenta l'accuratezza nel procesare i dati dopo la trasmissione e viene calcolata come il rapporto tra il code-rate scelto e la mutua informazione tra Alice e Bob

Detto questo possiamo normalizzare $\mathbf{X}_0$ e $\mathbf{Y}_0$ in questo modo:

$$\begin{aligned} \mathbf{X} &= \frac{\mathbf{X}_0}{\sqrt{V_{mod}}} \\ \mathbf{Y} &= \frac{\mathbf{Y}_0}{\sqrt{TV_{mod} + 1 + \xi}} \end{aligned} \tag{2.4}$$

Così facendo abbiamo ottenuto altre due sequenze di dati $\mathbf{X}$ e $\mathbf{Y}$, correlate tra loro dall'equazione $\mathbf{X} = \mathbf{Y} + \mathbf{Z}$, dove $\mathbf{Z}$ è una variabile aleatoria che risponde ad una distribuzione normale centrata in zero e con variaza $V_z = \frac{1}{V_{mod}}$. Quindi normalizzando in questo modo abbiamo ottenuto lo stesso effetto che avremmo avuto se Bob avesso inviato ad Alice i proprio dati normalizzati $\mathbf{Y}$ su un canale che aggiunge solamente rumore gaussiano[MFZG18].

Il passo successivo per Bob sarà quello di generare una stringa di bit random $\underline{s} \in \{0,1\}^k$. Attraverso algoritmi di codifica LDPC viene calcolata una matrice $\mathbf{H}$ necessaria per aggiungere alla stringa $\underline{s}$ dei bit ridondanti di parità ottenendo la stringa $\underline{c} \in \{0,1\}^n$ dove n corrisponde alla lunghezza della sottosequenza di dati non utilizzati per la stima dei parametri.

Successivamente $\underline{c}$ viene utilizzata per modulare il segno della sequenza $\mathbf{Y}$ ottendo così un nuovo messaggio $\underline{m}$ tale che $m_i = Y_i(-1)^{c_i}$ per $i = 1, 2, \ldots, n$.

Il messaggio $\underline{m}$ viene trasmesso ad Alice su canale classico publico che assumiamo non introduca errori. Alice estrae da $\underline{m}$ un messaggio fittizio $\underline{r}$ con $r_i = \frac{m_i}{\mathbf{X}_i}$ che corrisponde alla trasmisione su un canale Gaussiano con rumore di varianza $V_i = \frac{V_z}{|\mathbf{X}_i|}$.

Infine verà utilizzato un algoritmo LDPC di decodifica per ottenere una stima $\underline{\hat{s}}$ della stringa $\underline{s}$ prodotta da Bob.

2.2 Discussione della sicurezza contro attacchi di lettura del segnale

Questo protocollo è particolarmente sicuro perché consentente il rilevamento di un eventuale spia (Eve). Nel protocollo si assume che Eve sia in possesso di un computer quantistico e che abbia acces-

so completo al canale di comunicazione ed anche con queste assunzioni si è in grado di garantire la sicurezza per diversi tipi di attacchi.

Gli attacchi presi in considerazione tipicamente sono tre e differiscono per la loro efficacia:

- **attacchi individuali**: Eve effettua operazioni singolarmente su ogni segnale che viene scambiato tra Alice e Bob.
- **attacchi collettivi**: Eve salva nella memoria del suo computer quantistico un certo numero di stati sui quali effettua una misura collettiva. Questo attacco è più potente del precedente perchè secondo i pricipi della fisica quantistica effettuando una misura collettiva si può potenzialmente ricavare più informazione che dalla misura del singolo stato.
- **attacchi coerenti**: sono attacchi più potenti dei collettivi perché Eve, oltre alla lettura collettiva, può utilizzare delle correlazioni quantistiche, cioé entanglement, per mettere in relazione gli stati di più run.

Tornando al motivo per cui effettivamente si riesce a rilevare Eve possiamo, anche questa volta, dare il merito ai principi della fisica quantistica. Questo perchè in caso di misura da parte di Eve lo stato coerente trasmesso verrà alterato. Due esempio di attacchi che Eve può mettere in atto e le loro conseguenze sono:

- sottrarre una parte del segnale per effettuare una misura sullo stesso, questo comporta una diminuzione di fotoni del segnale ricevuto da Bob
- misura il segnale attraverso una misura eterodina per stimare entrambe le componenti di quadratura. Utilizzando le componenti misurate come valori medi, realizza un nuovo stato coerente che trasmette a Bob. In questo modo siccome vengono misurati dei valori randomici e siccome la misura eterodina stessa introduce ulteriore rumore la varianza degli stati coerenti ricevuti da Bob sarà superiore a quella originaria.

In entrambi i casi, un attacco da parte di Eve non va a far altro che aumentare gli effetti distruttivi del canale di trasmissione.

Tutte queste alterazione, in fase di stima dei parametri, produrranno dei valori indesiderati come $\chi > I_{AB}$. Queste incongruenza tra le stime e ciò che ci si aspettava dalla scelta dei paramettri iniziali portano a pensare che una spia si sia intromessa nella comunicazione.

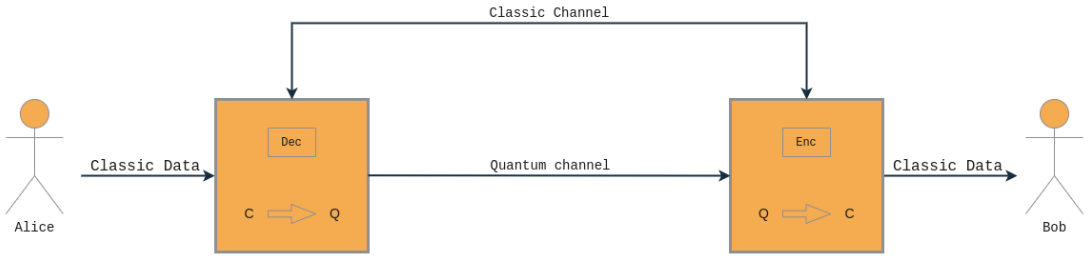

Figura 2.2: Schema di comunicazione tra Alice e Bob Sezione **??**.

Come si evince dalle Figure 2.2.a e 2.2.b non si capisce molto.

Capitolo 3

Simulazione

Conclusioni e sviluppi futuri

La tesi è finita

Bibliografia

[LPF+18] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[MFZG18] Mario Milicevic, Chen Feng, Lei M. Zhang, and P. Glenn Gulak. Key Reconciliation with Low-Density Parity-Check Codes for Long-Distance Quantum Cryptography. *npj Quantum Inf*, 4(1):21, April 2018. arXiv:1702.07740 [quant-ph].