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

Uno stato coerente fornisce una descrizione classica della luce in termini di onde elettromagnetiche, nonstante siano stati costruiti a partire dalla meccanica quantistica. Viene comunemente rappresentato $|\alpha_j\rangle = |q_j + ip_j\rangle$ attraverso la notazione introdotta da Paul Dirac che prende il nome di *bra-ket*. Come si può notare uno stato coerente presenta due componenti q e p dette componenti di quadratura le quali non hanno una valore esatto ma sono 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.

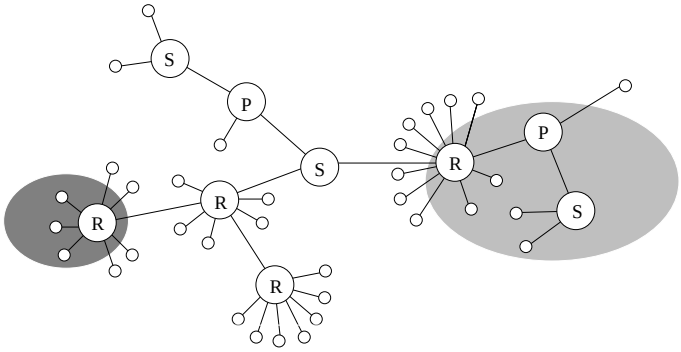


Figura 1.1: Figura da inserire—> Stato coerente

1.2 Cosa succede in fase di misura

In fase di misura Bob riceve una stato coerente con la forma vista in figura 1.1, ci aspettiamo che nel momento della ricezione il valore della deviazione standard delle gaussiane che descrivono lo stato coerente sia aumentato rispetto a quello che avevano in fase di trasmissione. L'aumento di incertezza è dovuto al rumore che viene introdotto dal canale di trasmissione, ma di questo parleremo più nel dettaglio nel capitolo 2.

Una volta ricevuto il segnale quantistico Bob effettua la misura che consiste nell'estrarre, in base al tipo di misura adottato, uno o due valori che corrispondono ad una delle due componenti di quadratura o entrambe, con pobabilità gaussiana. Dopo questa fase di misura termina la porzione

quantistica del protocollo ottenendo dati classici su i quali verrano effettuate altro operazioni per ottenere, in caso di successo, una chiave crittografica sicura con la quale codificare messaggi che verranno scambiati su un canale di comunicazione classico.

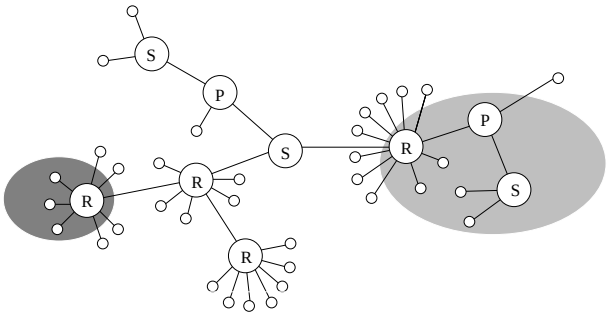


Figura 1.2: Figura da inserire—> comparare stato coerente e gaussina dalla quale bob misura

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 una spia (Eve) nella trasmissione su canale quantistico tra Alice (mittente) e Bob (destinatario).

La rilevazione è dovuta la fatto che durante la misura da parte de Eve lo stato quantistico viene alterato introducendo del rumore e quindi dell'incertezza. In pratica Eve intercetta lo stato coerente, rappresentato come in figura 1.1, ne effettua la misura e lo ritrasmette sul canale. Bob riceverà uno stato coerente con del rumore aggiunto, cioè la varianza della gaussiana che lo rappresenta è maggiore

di quella stimata prendendo anche in considerazione in rumore aggiunto dal canale di trasmissione. La detection però, viene effettuata in una fase successiva a quella di trasmissione, durante la quale vengono stimati dei parametri 2.1.2 e confrontati con quelli attesi. Nel caso in cui il confronto non vada a buon fine, i parametri stimati e quello attesi differiscono più di un certo limite stabilito a priori, 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 questo 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 è 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 Trasmissione e misura

Alice prepara gli stati coerenti andando a estrarre da una distribuzioni normale centrata in zero i valori dell componenti di quadratura q e p. Dopo la preparazione Alice trasmette a Bob gli stati coerenti

attraverso un canale quantistico.

Il canale è caratterizzato da un certo valore di trasmittanza e di rumore. 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 variaza delle gaussiane così da accrescere l'incertezza nelle misure da parte di Bob.

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 con distribuzione di probabilità uniforme.
- **misura eterodina**: vengono misurare contemporaneamente entrambe le componenti.

In caso di misura omodina è necessaria un'operazione addizionale cioé il sifting. Questa operazione consiste nel riverare ad Alice, su canale classico publico, per ogni round quale componente è stata misurata da Bob; Alice prende nota delle componenti misurare e scarta le altre.

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 di Eve χ. Nel caso in cui χ risulti essere maggiore di I_{AB} 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 i dati primari che vengono inviati ad Alice la quali 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 però è da tenere in considerazione che più bassa è la trasmittanza più sarà distruttivo l'effetto del rumore del canale.

In questa fase utilizzando la riconciliazione inversa viene generata una chiave crittografica sicura, Bob attraverso dei codici di LDPC (low-density-parity-check) produce una stringa di bit con la quale modulare i propri dati scelti per creare la chiave. Trasmette su canale publico senza errori i propri dati ad Alice la quale li decodifica per ottenere la chiave prodotta da Bob.

2.2 Perché funziona, rilevazione di un'eventuale spia

Questo protocollo è particolarmente sicuro prercé consentente il rilevamento di un eventuale spia (Eve), questo è possibile grazie a principi delle fisica quantistica. Nel protocollo si assume che Eve sia in possesso di un computer quantistico e che abbia accesso completo al canale di comunicazione e comunque 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 effettuare una misura collettiva si può potenzialmente ricavare più informazione che dalla misura del singolo stato.

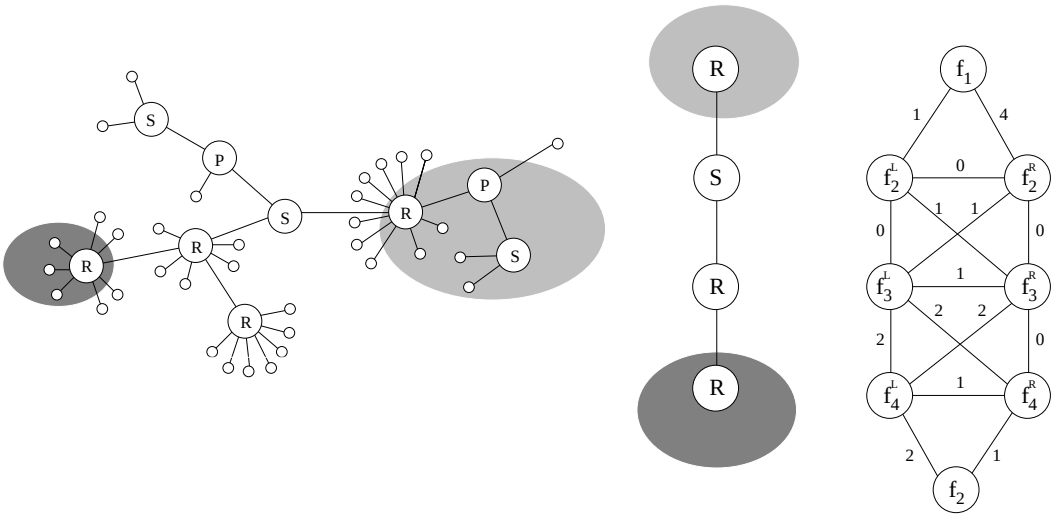
- **attacchi coerenti**: **Da chiedere al professore.**

Tornando al motivo per cui effettivamente si riesce a rilevare Eve possiamo dire anche questa volta che è merito dei principi della fisica quantistica. Questo perchè in caso di misura da parte di Eve lo stato coerente trasmesso verrà alterato, quello che avviene in pratica è una diminuzione dei fotoni del segnale, quindi per come è stato definito il numero di fotoni la rappresentazione dello stato sul piano di Gauss si troverà più vicina all'origine. Inoltre durante la misura viene aggiunto del rumore che comporta una aumento della varianze delle gaussiane che descrivono lo stato e quindi una maggiore incertezza nella misura da parte di Bob.

Tutte questa 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 portano a pensare che una spia si sia intromessa nella comunicazione.

Ancora del testo

Come si evince dalle Figure 2.1.a e 2.1.b non si capisce molto.



(a) (b)

Figura 2.1: SPQR-tree di un grafo. (a) L'albero di allocazione della faccia esterna. (b) Il cammino notevole di cui si parla tanto nella Sezione **??**.

Capitolo 3

Simulazione

Conclusioni e sviluppi futuri

La tesi è finita

Bibliografia