



UNIVERSITÀ DEGLI STUDI ROMA TRE

Dipartimento di Ingegneria

Corso di Laurea in Ingegneria Informatica

Tesi Di Laurea

Sviluppo di un simulatore per la crittografia quantistica a variabili continue

Laureando

Kevin Santodonato

Matricola 548019

Relatore

Prof. Matteo Rosati

Anno Accademico 2022/2023

Questa è la dedica

Ringraziamenti

Grazie a tutti

Indice

Indice	iv
Elenco delle figure	vi
Introduzione	vii
1 Descrizione quantistica di un segnale ottico	1
1.1 Stati coerenti e le loro proprietà	1
1.2 Misurazione dei segnali e incertezza quantistica	2
2 Breve storia della QKD	5
2.1 CV-QKD con modulazione gaussiana	6
2.1.1 Produzione, trasmissione e ricezione del segnale quantistico	7
2.1.2 Stima dei parametri	9
2.1.3 Riconciliazione delle informazioni	10
2.2 Discussione della sicurezza contro attacchi di lettura del segnale	14
3 Simulazione	17
3.1 Preparazione, trasmissione e misura	18
3.1.1 Preparazione dello stato coerente	18

3.1.2	Trasmissione su canale rumoroso	18
3.1.3	Misura omodina del segnale	18
3.2	Sifting	19
3.3	Stima dei parametri	19
3.4	Riconciliazione	20
3.4.1	Algoritmi Sum-Product e classic PEG	21
Conclusioni e sviluppi futuri		23
Bibliografia		24

Elenco delle figure

1.1	Questa figura è una gaussiana vista dall'alto che viene ottenuta simulando molte volte la produzione dello stesso	
1.2	Figura da inserire—> confronto tra gaussiano con spia e senza spia	4
2.1	Schema di comunicazione tra Alice e Bob Sezione.	7
2.2	Schema attacco individuale.	14
2.3	Schema attacco collettivo.	15
2.4	Schema attacco coerente.	15
2.5	Schema che descrive le fasi del protocollo facendo particolare attenzione al canale quantistico e canale classico.	

Introduzione

La crittografia, da migliaia di anni, ha costituito il fondamento delle comunicazioni segrete e della protezione dei dati sensibili. Nel corso della storia umana, dall'antico Egitto fino alla metà del secolo scorso, la crittografia veniva considerata un'arte e tutti i sistemi crittografici e cifrari che venivano realizzati erano considerati sicuri fino al momento in cui qualcuno riusciva a trovare una falla nel sistema e decifrare il messaggio senza una chiave.

Nel 1949, grazie a Claude Shannon, inizia l'era moderna della crittografia la quale, da questo punto in poi della storia, viene considerata oltre che un'arte anche una scienza. Shannon nel '49 pubblica un articolo denominato "Communication Theory of Secrecy Systems"[Sha49] nel quale comprova, per la prima volta, la sicurezza del cifrario di Vernam (comunemente chiamato One Time Pad) attraverso dimostrazioni matematiche.

Il cifrario di Vernam si basa su un concetto molto semplice: per trasmettere un messaggio cifrato tra due parti, che vengono comunemente chiamate Alice e Bob, viene prodotta una chiave della lunghezza del messaggio che si vuole trasmettere. La chiave deve essere condivisa un modo sicuro tra le due parti, ad esempio Alice e Bob possono incontrarsi e scambiare la chiave. Successivamente la chiave viene utilizzata da Alice per codificare il messaggio e da Bob per decodificarlo, a questo punto la chiave va scartata e per trasmettere un nuovo messaggio è necessario produrre una nuova chiave.

Questo tipo di cifrario rientra nella classe dei crittosistemi simmetrici (a chiave privata) nei quali per codifica e decodifica viene utilizzata la stessa chiave. Di questa classe di crittosistemi la sicurezza è

garantita da quanto dimostrato da Shannon però si può subito notare un problema non indifferente: la chiave deve essere condivisa in qualche modo tra Alice e Bob. Condividere una chiave, in alcune situazioni, potrebbe risultare un'operazione molto dispendiosa ed è per questo che nel 1976 sono state gettate le basi per una nuova classe di crittosistemi denominati crittosistemi asimmetrici [DH76].

L'idea alla base dei crittosistemi asimmetrici (a chiave pubblica) è quella di utilizzare due chiavi diverse per la codifica e la decodifica. La prima implementazione di un protocollo che rientra in questa classe è stata realizzata nel 1978 e prende il nome di RSA [RSA78], il quale oggi è ampiamente utilizzato. In crittosistemi a chiave pubblica se Bob vuole ricevere dei messaggi codificati con una chiave pubblica per prima cosa deve generare per sé stesso una chiave privata. Da questa chiave produce una chiave pubblica che rivela ad Alice la quale utilizza la chiave pubblica per codificare il messaggio e trasmetterlo a Bob. Una volta ricevuto il messaggio Bob lo decodifica utilizzando la propria chiave privata.

La sicurezza di questi sistemi, a differenza di quelli a chiave privata, non si basa su dimostrazioni matematiche ma solamente sulla complessità computazionale. Questo perché per la produzione delle chiavi vengono utilizzate delle funzioni matematiche molto semplici da calcolare ma molto difficili da invertire. In termini di complessità computazionale difficile sta a significare che il tempo necessario per eseguire un'operazione cresce esponenzialmente con la lunghezza della chiave, mentre per operazioni semplici il tempo di esecuzione è polinomiale rispetto alla lunghezza della chiave. Ad esempio, la sicurezza del protocollo RSA si basa proprio sulla difficoltà di fattorizzazione di interi molto grandi.

Non essendoci prove matematiche che garantiscano la sicurezza dei crittosistemi a chiave pubblica non è da escludere la probabilità che sia possibile realizzare un algoritmo classico che abbia una complessità computazionale polinomiale per la fattorizzazione di grandi interi. Di fatto la sicurezza di questa classe di protocolli è già minacciata da un algoritmo per computer quantistici, ideato da Peter Shor nel 1994, che permette la fattorizzazione di grandi interi con complessità polinomiale [Sho94].

Per questo al giorno d'oggi è sempre più importante la ricerca su protocolli di distribuzione quantistica di chiavi (QKD) che utilizzano principi della fisica quantistica con lo scopo di condividere chiavi su canali pubblici. Questi protocolli rientrano nella classe di crittosistemi simmetrici perché la codifica e la decodifica dei messaggi trasmessi viene effettuata con una chiave privata comune ad Alice e Bob. Il potere della QKD risiede nel fatto che grazie alla fisica quantistica si ha la possibilità di determinare se la condivisione dei messaggi necessari per la produzione della chiave è avvenuta in modo sicuro o meno, in parole povere si è in grado di determinare se una spia (Eve) è venuta in possesso di questi messaggi.

Il primo protocollo ad essere stato proposto per la distribuzione quantistica di chiavi è il BB84 che prende il nome dai suoi ideatori Charles H. Bennett e Gilles Brassard che lo hanno realizzato nel 1984 [BB14]. Questo protocollo per realizzare la comunicazione utilizza due canali di trasmissione, uno classico e pubblico e l'altro quantistico e privato. Alice trasmette sul canale quantistico a Bob una sequenza di fotoni polarizzati in modo casuale in due basi, ognuna delle quali ha due gradi di polarizzazione. Nella prima base il fotone può essere polarizzato a 0 o 90 gradi e verrà considerato come un bit 0, mentre nella seconda a 45 o 135 gradi e verrà considerato come bit 1. In ricezione Bob effettuerà la misura della polarizzazione del fotone scegliendo una base con probabilità uniforme dalle due basi disponibili. Alla fine della trasmissione Bob sarà in possesso dei gradi di polarizzazione misurati i quali verranno convertiti in 0 e 1 seguendo la stessa convenzione di Alice. Da notare che parte dei dati di Bob differiranno da quelli inviati da Alice perché Bob ha effettuato la misura utilizzando la base sbagliata. Successivamente Bob comunicherà ad Alice quale base ha utilizzato per la misura di ogni fotone ed Alice scarterà tutti quei fotoni la cui base di trasmissione e misura non combaciano, e lo comunicherà a Bob. Fatto ciò Alice e Bob saranno in possesso, almeno in teoria, della stessa stringa random di bit. Quello che potrebbe succedere è che durante la trasmissione Eve intercetti i fotoni inviati da Alice per effettuarne una misura e poi inviare il risultato della propria misura a Bob.

Tuttavia questo altererebbe il risultato della misura di Bob perchè Eve non può sapere con quale base è stato polarizzato il fotone, e di conseguenza non può sapere con quale base misurarlo. Misurando un fotone con la base sbagliata nel momento in cui lo ritrasmetterà a Bob egli riceverà un fotone polarizzato in modo differente rispetto a quello inviato da Alice. Questo permetterà ad Alice e Bob di determinare la presenza di una spia andando a confrontare una porzione di bit misurati con la stessa base utilizzata in trasmissione e quindi ritenuti uguali. Durante il confronto se si riscontrano bit diversi si determina la presenza di una spia. Se Eve ha intercettato troppi fotoni non viene prodotta nessuna chiave e si ricomincia il protocollo da capo, in caso contrario si utilizzano i bit rimasti segreti come chiave crittografica[Zha18]. La sicurezza di questo ed altri protocolli QKD si basa proprio sulle peculiarità della misura di segnali quantistici.

In questa tesi studieremo un protocollo di QKD che utilizza una codifica non nei singoli fotoni ma piuttosto nella fase di un segnale quantistico. La tesi è strutturata nel seguente modo: nel capitolo 1 1 introdurremo gli stati coerenti con le loro proprietà e la misura di segnali quantistici, nel capitolo 2 2 discuteremo dei protocolli QKD ed in particolare del protocollo CV-QKD con modulazione gaussiana, nel capitolo 3 3 illustreremo una possibile implementazione del protocollo discusso nel capitolo precedente ed infine, nel capitolo 4 discuteremo le conclusioni.

Capitolo I

Descrizione quantistica di un segnale ottico

I.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 opportune unità di misura, ha varianza unitaria. Il motivo per cui non rappresenta-

no un valore esatto è perché, a differenza della fisica classica, nella fisica quantistica le quantità, anche scalari, sono degli operatori che assumono un valore esatto solamente in fase di misura.

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

$$\langle n_j \rangle = |a_j|^2 = q_j^2 + p_j^2 \quad (1.1)$$

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, gli stati coerenti si presentano come una distribuzione di probabilità gaussiana e possono essere rappresentati graficamente in un piano cartesiano, che riporta i valori misurabili di q e p , come una nuvola di punti i quali avranno appunto probabilità gaussiana di essere estratti.

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 1.1e proverà a misurarlo, con una data incertezza. 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 intrinseca di uno stato quantistico la quale non può essere rimossa in base al principio di indeterminazione di Heisenberg. Questa incertezza si presenta proprio in fase di misura, perché come detto nella sezione 1.1, il valore di quadratura q e p sono solamente valori medi mentre il valore q o 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 da un eventuale spia (Eve) che tenta anch'essa di misurare il segnale

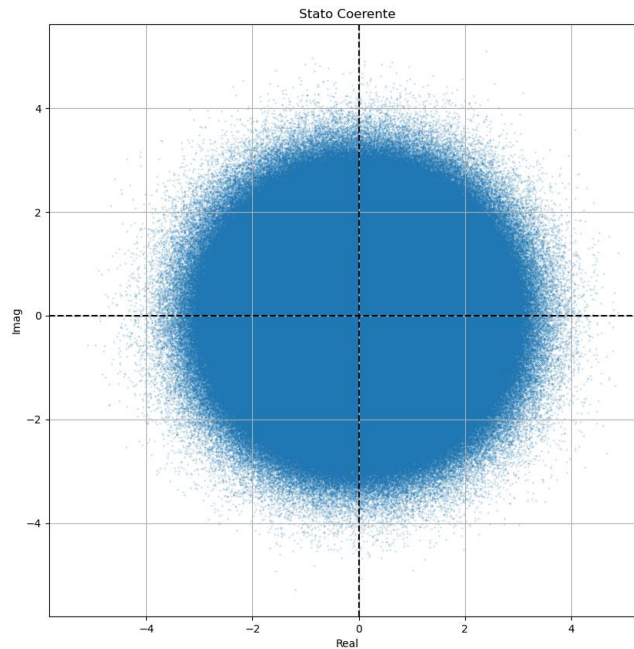


Figura 1.1: Questa figura è una gaussiana vista dall'alto che viene ottenuta simulando molte volte la produzione dello stesso stato coerente e la misura della grandezza \hat{q} o \hat{p} . La gaussiana è rappresentata su un piano cartesiano riportante sulle ascisse le misure della componente q mentre sulle ordinate le misure della componente p

modificandolo, questo rende la misura di Bob ancora più incerta.

Per concludere possiamo dire che i protocollo di QKD utilizzano due fondamentali caratteristiche dei segnali quantistici:

- vi è un'incertezza nella misura anche in assenza di rumore esterno;
- una misura di un segnale introduce rumore nel segnale stesso.

Tali proprietà risultano cruciali per determinare l'eventuale intromissione di Eve nella comunicazione e quindi la possibilità o meno di creare una chiave crittografica sicura.

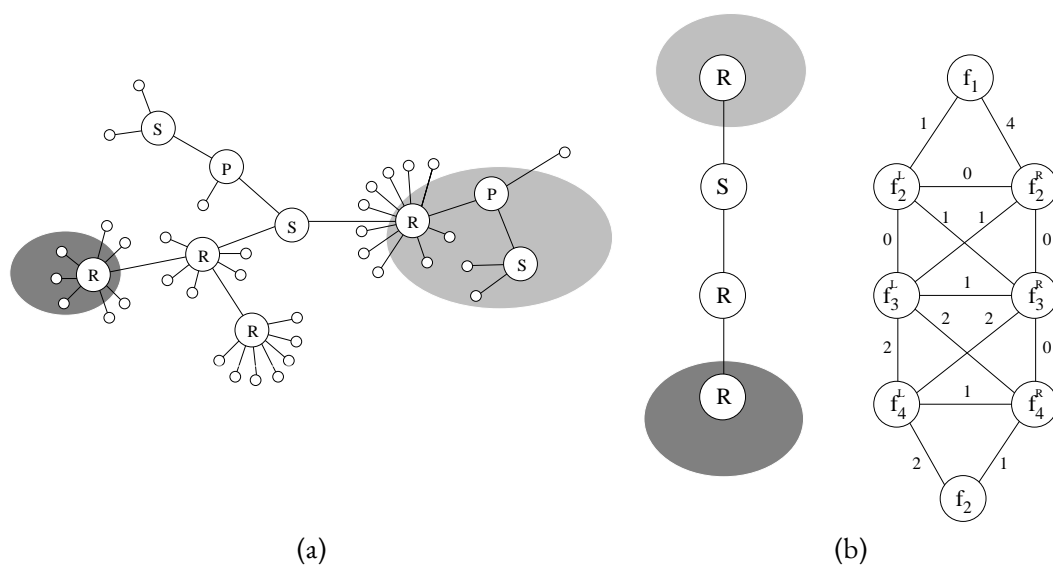


Figura 1.2: Figura da inserire—> confronto tra gaussiano con spia e senza spia

Capitolo 2

Breve storia della QKD

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 inattaccabile anche da computer quantistici. La QKD può essere suddivisa in due macro-classi DV-QKD e CV-QKD. Nella DV-QKD (Discrete-Variable Quantum Key Distribution) le informazioni vengono trasmesse utilizzando stati quantici discreti, ad esempio la polarizzazione degli fotoni, che viene misurata attraverso apposite apparecchiature per ogni fotone; al contrario nella CV-QKD (Continuous-Variable Quantum Key Distribution) vengono utilizzate variabili continue delle onde elettromagnetiche come ad esempio la fase.

La sicurezza è garantita dai principi della 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 se questo non viene amplificato¹ e introducendo del rumore, quindi dell'incertezza. All'atto pratico Eve intercetta lo stato coerente, rappresentato come

¹Un'amplificazione, pur riportando il livello di energia del segnale a quello iniziale, introdurrà ulteriore rumore.

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 abortita perché non è possibile garantire la sicurezza della chiave crittografica e si comincia con un nuovo round.

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 in due sezioni: la prima sezione ha effettivamente a che fare con segnali quantistici mentre la seconda sezione 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.

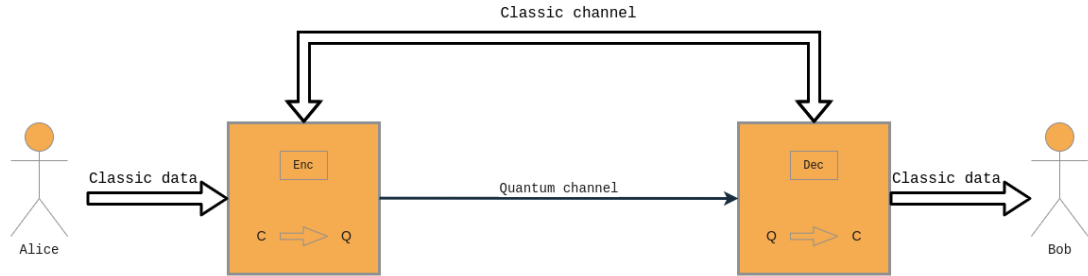


Figura 2.1: Schema di comunicazione tra Alice e Bob Sezione.

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 ($q \sim \mathcal{N}(0, V_{mod})$ e $p \sim \mathcal{N}(0, V_{mod})$) [LPF⁺18]. Da notare che la 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 di comunicazione, ad esempio una fibra ottica, che può essere anch'esso rappresentato come 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 centrate 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 considerare un generico stato scelto da Alice $|\alpha_A\rangle = |q_A + ip_A\rangle$. Come abbiamo detto nella sezione 1.1 le componenti di quadratura rispondono ad una distribuzione

di probabilità normale, quindi avremo:

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

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

$$\begin{aligned} Q_B &\sim \mathcal{N}(\sqrt{T}q_A, 1 + \xi) \\ P_B &\sim \mathcal{N}(\sqrt{T}p_A, 1 + \xi) \end{aligned} \tag{2.2}$$

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 cioè il sifting. Infatti, a questo punto del protocollo Alice è in possesso del doppio dei dati di Bob (in quanto Bob misura solo una delle due componenti per ogni round) e per far sì che abbiano la stessa quantità di dati correlati Bob rivela ad Alice, su canale classico pubblico, quale componente ha misurato ad ogni round; Alice prende nota della componenti misurate e scarta le altre[MFZG18]. Notare che questa operazione non compromette la sicurezza: Eve saprà solo quale tipo di misura ha eseguito Bob ad ogni round, ma non il risultato ottenuto né il valore vero inviato da Alice.

2.1.2 Stima dei parametri

Dopo avere terminato la fase di trasmissione, Alice e Bob rivelano una porzione random di dati in modo tale da confrontare ciò che è stato effettivamente inviato da Alice con le misure di Bob. Da questo confronto sono in grado di stimare l'informazione mutua I_{AB} (informazione mutua tra Alice e Bob) e l'informazione mutua tra Eve e Bob χ_{EB} . Prima della effettiva stima delle mutue informazioni è necessario stimare trasmittanza e rumore del canale e calcolare altre quantità che verranno utilizzare nel calcolo delle mutue informazioni.

Secondo l'articolo [LPF⁺18] l'equazione per il calcolo di I_{AB} è:

$$I_{AB} = \frac{\mu}{2} \log_2(1 + SNR) \quad (2.3)$$

con $\mu = 1$ se la misura è omodina e $\mu = 2$ per la misura eterodina. Mentre per il calcolo dell' SNR abbiamo che:

$$SNR = \frac{\frac{1}{\mu} TV_{mod}}{1 + \frac{1}{\mu} \xi} \quad (2.4)$$

Per la stima di rumore e trasmittanza del canale abbiamo bisogno dei parametri a , b e c che rappresentano le entry della matrice di covarianza Σ_{AB} .

$$\Sigma_{AB} = \begin{pmatrix} a \mathbb{1}_2 & c \mathbb{1}_2 \\ c \mathbb{1}_2 & b \mathbb{1}_2 \end{pmatrix} \quad (2.5)$$

Le equazioni per il calcolo dei parametri vengono ancora una volta prese dai risultati dell'articolo [LPF⁺18]:

$$\begin{aligned} a &= V_{mod} + 1 \\ b &= \frac{\langle q_B^2 \rangle + \langle p_B^2 \rangle}{2} \\ c &= \sqrt{\frac{V_{mod} + 2}{V_{mod}}} \cdot \left(\frac{\langle q_A q_B \rangle + \langle p_A p_B \rangle}{2} \right) \end{aligned} \quad (2.6)$$

Calcolati i parametri a , b e c possiamo andare a stimare il rumore e la trasmittanza:

$$\begin{aligned} T &= \frac{c^2}{V_{mod}^2 + 2V_{mod}} \\ \xi &= b - TV_{mod} - 1 \end{aligned} \quad (2.7)$$

Ora non ci resta che calcolare le quantità ν_1 , ν_2 e ν_3 alle quali verrà applicata una funzione $g(\nu)$ che ci porterà al calcolo della mutua informazione fra Eve e Bob. Possiamo calcolare i valori di ν utilizzando i parametri calcolati in precedenza in questo modo:

$$\begin{aligned} \nu_1 &= \frac{1}{2}[z + (b - a)] \\ \nu_2 &= \frac{1}{2}[z - (b - a)] \\ \nu_3 &= \sqrt{a(a - \frac{c^2}{b})} \end{aligned} \quad (2.8)$$

con $z = \sqrt{(a + b)^2 - 4c^2}$.

Finalmente è giunto in momento di calcolare anche χ_{EB} in questo modo:

$$\chi_{EB} = g(\nu_1) + g(\nu_2) - g(\nu_3) \quad (2.9)$$

con

$$g(\nu) = \left(\frac{\nu + 1}{2}\right) \log_2\left(\frac{\nu + 1}{2}\right) - \left(\frac{\nu - 1}{2}\right) \log_2\left(\frac{\nu - 1}{2}\right) \quad (2.10)$$

In fine, dopo aver calcolato l'informazione mutua tra Alice e Bob e quella tra Eve e Bob vengono confrontati i risultati e nel caso in cui χ_{EB} risulti essere maggiore di βI_{AB} ² il protocollo viene abortito.

2.1.3 Riconciliazione delle informazioni

Se la stima dei parametri ha avuto successo Alice e Bob sono in possesso di due stringhe di numeri reali diversi ma correlati, a causa degli errori introdotti durante la trasmissione sul canale e la misurazione

² β rappresenta l'accuratezza nel processare i dati dopo la trasmissione e viene calcolata come il rapporto tra il code-rate del codice classico scelto e la mutua informazione tra Alice e Bob

di Bob. Devono pertanto effettuare una riconciliazione fra queste due stringhe, per assicurarsi di ottenere una sola stringa condivisa da entrambi. La riconciliazione può avvenire in due forme:

- **diretta:** Alice produce un messaggio fittizio codificando i suoi dati (correlati a quelli di Bob) con una chiave. Bob basandosi sulle misure effettuate in fase di trasmissione cerca di estrarre la chiave dal messaggio fittizio;
- **inversa:** la procedura è la stessa della riconciliazione diretta solamente che vengono scambiate le parti, Bob produce il messaggio fittizio ed Alice cerca di estrarre la chiave.

La riconciliazione diretta presenta un problema: non può essere utilizzata per valori di trasmittanza troppo bassi, questo perché Eve avrebbe più informazione sui dati di Alice rispetto a Bob e quindi risulterebbe 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].

Prima della riconciliazione vera e propria i dati in possesso ad Alice e Bob vengono normalizzati in modo tale da ottenere dei dati correlati. Se chiamiamo \mathbf{X} i dati in possesso ad Alice e \mathbf{Y} i dati in possesso a Bob, la relazione fra questi dati sarà $\mathbf{X} = \mathbf{Y} + \mathbf{Z}$, dove \mathbf{Z} è una variabile aleatoria che risponde ad una distribuzione normale centrata in zero con varianza $\frac{1}{V_{mod}}$. Attraverso questa normalizzazione in pratica, si ottiene lo stesso risultato che avremmo ottenuto se avessimo inviato ad Alice i dati di Bob attraverso un canale classico che aggiunge solamente rumore gaussiano.

A questo punto del protocollo Alice e Bob sono in 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 riconciliazione 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 in possesso di Alice e Bob siano rispettivamente:

$$\begin{aligned} V_{X_0} &= V_{mod} + 1 \\ V_{Y_0} &= TV_{mod} + 1 + \xi \end{aligned} \tag{2.11}$$

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

$$\begin{aligned} \mathbf{X} &= \frac{\mathbf{X}_0}{\sqrt{V_{mod}}} \\ \mathbf{Y} &= \frac{\mathbf{Y}_0}{\sqrt{TV_{mod} + 1 + \xi}} \end{aligned} \tag{2.12}$$

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 varianza $V_z = \frac{1}{V_{mod}}$. Quindi normalizzando in questo modo abbiamo ottenuto lo stesso effetto che avremmo avuto se Bob avesse inviato ad Alice i proprio dati normalizzati \mathbf{Y} su un canale classico e pubblico che aggiunge solamente rumore gaussiano [MFZG18]. Questo è il prototipo di canale di comunicazione classico utilizzato sin dai tempi di Shannon, detto canale di rumore bianco gaussiano additivo - Additive White Gaussian Noise Channel (AWGN). Per la trasmissione dati sull'AWGN è quindi possibile sfruttare una vasta gamma di codici studiati a partire dagli anni '60 [Gal72]-[RU08].

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

Dopodiché vengono utilizzati dei codici LDPC (Low-Density Parity-Check) [BS] che rappresentano una classe di codici correttori di errori utilizzati nell'ambito delle telecomunicazioni. Una delle ragioni per cui questi codici sono largamente utilizzati è la loro abilità di raggiungere prestazioni vicine alla capacità teorica del canale di comunicazione, nota come il limite di Shannon. I codici LDPC possono essere rappresentati in due modi:

- come una matrice di dimensioni $M \times N$ dove N rappresenta la dimensione del messaggio che si vuole codificare ed $M = N - k$ con k ottenuto dal prodotto tra N e il code-rate. Questa matrice è prevalentemente composta da zeri e contiene un numero limitato di uno.
- come un grafo bipartito rappresentato da nodi check e nodi variabile; facendo riferimento alla rappresentazione matriciale il numero di nodi check è M (numero di righe della matrice) e quello di nodi variabile è N (numero di colonne della matrice). Gli uno contenuti nella matrice, nel grafo, sono denotati dagli archi che collegano un nodo variabile ad un nodo check.

Attraverso gli algoritmi LDPC viene calcolata una matrice \mathbf{H} che sarà della forma $[-P_{(M \times k)}^T | I_{N-k}]$:

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad (2.13)$$

Esempio di una matrice con $M = 3$ ed $N = 6$.

Dalla matrice \mathbf{H} possiamo ottenere la matrice generatore $\mathbf{G} = [I_k | P_{(k \times M)}]$ da una matrice identità di dimensione k e la trasposta della matrice $P_{(M \times k)}^T$:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \quad (2.14)$$

Successivamente tramite il prodotto matriciale $\mathbf{s} \times \mathbf{G}$ tra la stringa \mathbf{s} e la matrice generatore \mathbf{G} si ottiene la stringa \mathbf{c} che verrà utilizzata per modulare il segno della sequenza \mathbf{Y} ottenendo così un nuovo messaggio \mathbf{m} tale che $m_i = Y_i(-1)^{c_i}$ per $i = 1, 2, \dots, n$.

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

Infine Alice utilizzerà un algoritmo LDPC di decodifica per ottenere una stima \mathbf{c}' della stringa \mathbf{c} prodotta da Bob.

2.2 Discussione della sicurezza contro attacchi di lettura del segnale

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

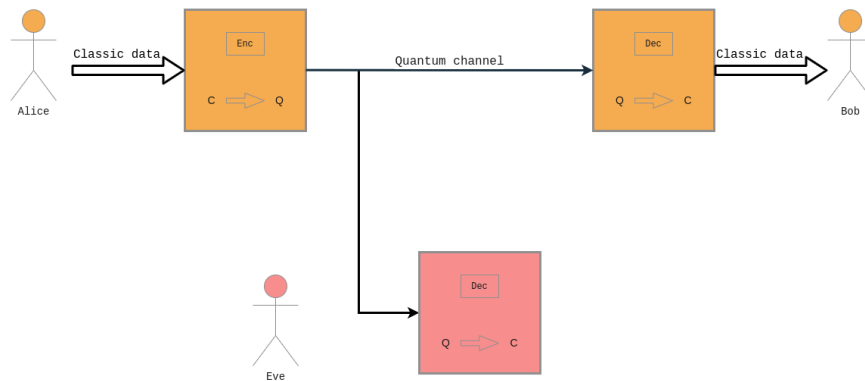


Figura 2.2: Schema attacco individuale.

- **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 perché secondo i principi della fisica quantistica effettuando una misura collettiva si può potenzialmente ricavare più informazione che dalla misura del singolo stato.

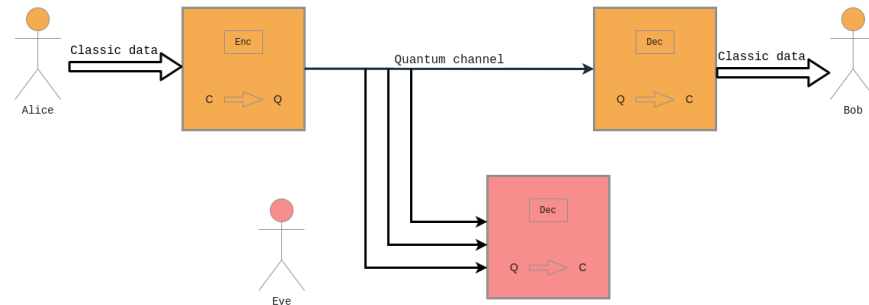


Figura 2.3: Schema attacco collettivo.

- **attacchi coerenti:** sono attacchi più potenti dei collettivi perché Eve, oltre alla lettura collettiva, può utilizzare delle correlazioni quantistiche, cioè entanglement, per mettere in relazione gli stati di più run.

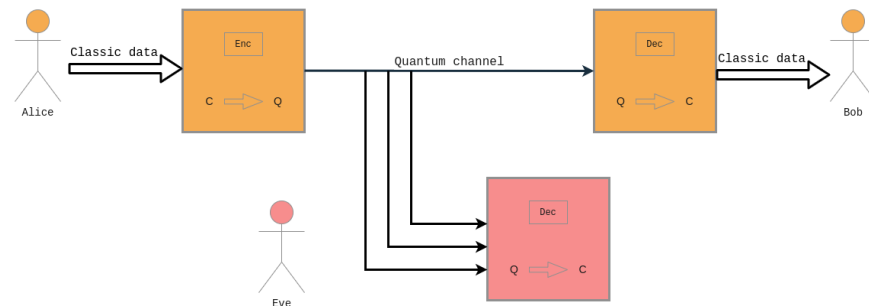


Figura 2.4: Schema attacco coerente.

Tornando al motivo per cui effettivamente si riesce a rilevare Eve possiamo, anche questa volta, dare il merito ai principi della fisica quantistica. Questo perché in caso di misura da parte di Eve lo stato coerente trasmesso verrà alterato. Due esempi 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 alterazioni, in fase di stima dei parametri, produrranno dei valori indesiderati come $\chi_{EB} > I_{AB}$. Questa incongruenza tra le stime e ciò che ci si aspettava dalla scelta dei parametri iniziali portano a pensare che una spia si sia intromessa nella comunicazione.

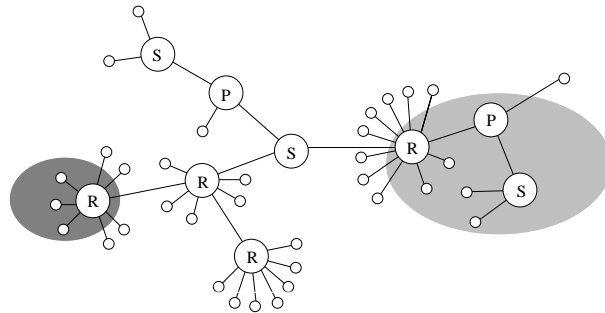


Figura 2.5: Schema che descrive le fasi del protocollo facendo particolare attenzione al canale quantistico e canale classico.

Capitolo 3

Simulazione

La realizzazione di questo simulatore per la distribuzione quantistica di chiavi con modulazione gaussiana di prefigge lo scopo di realizzare una chiave crittografica sicura condivisa tra due parti, la quale successivamente potrà essere utilizzata per la codifica e decodifica di un messaggio trasmesso su un canale pubblico classico.

Come tecnologia è stato utilizzato il linguaggio di programmazione C++. I motivi principali di questa scelta sono tre: la velocità del linguaggio di programmazione, la disponibilità di librerie che implementano le distribuzioni di probabilità necessarie alla simulazione e la presenza di librerie esterne che implementano due algoritmi indispensabili per la correzione degli errori.

Anche se il progetto è stato realizzato utilizzando C++ è stato deciso di illustrare quanto è stato fatto attraverso dello psdeudo-codice in modo tale da non legare la simulazione ad uno specifico linguaggio di programmazione ed agevolarne la rimplementazione in qualunque linguaggio di programmazione si voglia utilizzare.

Prima di addentrarci nella descrizione delle fasi della simulazione, è bene andare a definire delle costanti necessarie per il corretto funzionamento del simulatore. Le costanti in questione sono il rumore e la trasmittanza del canale, rispettivamente $\xi = 0.005$ e $T = 0.1$, la varianza $V_{mod} = 5.226$ della

modulazione ed il code-rate $R = 0.3$. I valori per queste costanti sono stati scelti in base ai risultati ottenuti negli articoli [LPF⁺18] e [FNZG22].

3.1 Preparazione, trasmissione e misura

3.1.1 Preparazione dello stato coerente

Per la realizzazione degli stati coerenti da trasmettere sul canale vengono scelti due valori che rappresentano i valori medi delle due gaussiane con varianza unitaria che caratterizzano lo stato. I valori vengono estratti a loro volta da una distribuzione di probabilità normale centrata in zero e con varianza V_{mod} . Queste informazioni sono salvate in una struttura dati che oltre a contenere tutte le informazioni necessaria per caratterizzare lo stato coerente presenta dei tag che verranno utilizzati nella sottosezione ?? per distinguere le componenti di quadratura p e q .

3.1.2 Trasmissione su canale rumoroso

Per ogni stato coerente prodotto si simula la trasmissione in un canale rumoroso. Le operazioni che vengono effettuate in pratica sono: il prodotto dei valori medi della gaussiane per la radice quadrata della trasmittanza e la somma di ξ alla varianza. Quindi le componenti di quadratura saranno descritte dalle seguenti distribuzioni normali:

$$\begin{aligned} q &\sim \mathcal{N}(\sqrt{T}q_B, 1 + \xi) \\ p &\sim \mathcal{N}(\sqrt{T}p_B, 1 + \xi) \end{aligned} \tag{3.1}$$

3.1.3 Misura omodina del segnale

Per la misurazione del segnale verrà effettuata una misura omodina che consiste in due fasi. Per prima cosa si decide quale delle componenti di quadratura misurare, la decisione viene presa attraverso

una distribuzione di probabilità uniforme. Questo significa che le componenti q e p hanno la stessa probabilità di essere misurate.

Successivamente avviene l'effettiva misura che consiste nell'estrarre un valore da una distribuzione normale inizializzata come nell'equazione 3.1.

3.2 Sifting

Prima di procedere con l'effettiva stima dei parametri è necessario effettuare il sifting (vaglio delle informazioni). A questo punto della simulazione si hanno gli stati coerenti inviati e l'insieme delle misure delle componenti. Dal momento che viene effettuata la misura di una sola componente per ogni round di trasmissione, i dati trasmessi sono il doppio di quelli misurati. L'operazione che viene effettuata è molto semplice: per ogni misura effettuata viene determinata quale componente è stata misurata, questo grazie al tag di cui abbiamo parlato nella sottosezione 3.1.1; per il round di trasmissione corrispondente vengono mantenute solamente le informazioni di valore medio e tag relative alla componente misurata scartando di resto.

Questa operazione viene effettuata per ogni coppia di dati trasmessi e misurati.

3.3 Stima dei parametri

La stima dei parametri è una fase indispensabile del protocollo perché permette di determinare se la trasmissione è stata sicura oppure è avvenuta l'intromissione di una spia. Per la stima dei parametri Alice e Bob dovrebbero scambiarsi un subset random dei dati trasmessi ma per semplicità nella simulazione utilizziamo i primi n dati trasmessi. In un'applicazione reale del protocollo questa è una pessima scelta, perché se Eve venisse in possesso di questa informazione potrebbe non intercettare i primi n segnali andando a misurare solo la restante parte. Così facendo Eve non verrebbe rilevata pur

avendo intercettato la parte piú importante della comunicazione, cioè i dati che verranno utilizzati per distillare la chiave.

Chiamiamo i subset di dati dopo il sifting di Alice e Bob utilizzati per la stima dei parametri Q_A e Q_B per la componente di quadrature q e P_A e P_B per la componente di quadratura p .

Svolte tutte le operazioni illustrate dall'algoritmo 1 per ottenere la stima dell'informazione mutua tra Alice e Bob I_{AB} e di quella tra Eve e Bob χ_{EB} le andiamo a confrontare. Nel caso in cui I_{AB} risulti minore di χ_{EB} la simulazione si interrompe e deve ricominciare da capo.

Algorithm 1 : Stima dei parametri

- 1: **Step 1:** Stima dei parametri a , b e c

$$a \leftarrow V_{mod} + 1$$

$$b \leftarrow \frac{\langle Q_B^2 \rangle + \langle P_B^2 \rangle}{2}$$

$$c \leftarrow \sqrt{\frac{V_{mod}+2}{V_{mod}}} \cdot \frac{\langle Q_B Q_A \rangle + \langle P_B P_A \rangle}{2}$$
 - 2: **Step 2:** Stima del rumore e della trasmittanza del canale

$$T \leftarrow \frac{c^2}{V_{mod}^2 + 2V_{mod}}$$

$$\xi \leftarrow b - TV_{mod} - 1$$
 - 3: **Step 3:** Calcolo dei ν

$$\nu \leftarrow nuCalc()$$

▷ vengono utilizzare le equazioni 2.8
 - 4: **Step 4:** Calcolo I_{AB}

$$SRN \leftarrow signalNoiseRatio()$$

▷ viene utilizzata l'equazione 2.4

$$I_{AB} \leftarrow mutualInfoAliceBob(SNR)$$

▷ viene utilizzata l'equazione 2.3
 - 5: **Step 5:** Calcolo χ_{EB}

$$\chi_{EB} \leftarrow g(\nu_1) + g(\nu_2) - g(\nu_3)$$

▷ la funzione $g(\nu)$ 2.10
 - 6: **Step 6:** Confronto tra I_{AB} e χ_{EB}

$$\beta \leftarrow \frac{R}{I_{AB}}$$

▷ R rappresenta in code-rate
 - 7: **if** $\beta I_{AB} < \chi_{EB}$ **then**
 - 8: $abort()$

▷ la simulazione si interrompe
 - 9: **end if**
-

3.4 Riconciliazione

A questo punto della simulazione si è in 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 da questi dati, altre due sequenze di dati correlati che chiameremo \mathbf{X} e \mathbf{Y} come illustrato nell'equazione 2.12.

Poi viene prodotta la stringa \mathbf{s} la quale viene codificata attraverso l'algoritmo PEG (Progressive Edge Growth) per ottenere la stringa \mathbf{c} . Utilizziamo la stringa \mathbf{c} per modulare il segno della sequenza di dati \mathbf{Y} di Bob per produrre il messaggio \mathbf{m} che verrà inviato ad Alice. Da messaggio \mathbf{m} Alice estrarrà una messaggio fittizio \mathbf{r} che le permetterà, attraverso l'utilizzo dell'algoritmo *sum-product* 3, di ottenere una stima della stringa di bit \mathbf{c} prodotta originariamente da Bob.

Tutte queste operazione vengono illustrate nell'algoritmo 2 facendo riferimento alla sottosezione 2.1.3.

Algorithm 2 : Riconciliazione

- 1: **Step 1:** Genera string di bit random
 - 2: $\mathbf{s} \leftarrow \text{generaStringaBit}()$ $\triangleright \mathbf{s} \in \{0, 1\}^k$
 - 3: **Step 2:** Crea la matrice \mathbf{H} e la matrice \mathbf{G}
 - 4: $\mathbf{H} \leftarrow \text{peg}(M, N, \lambda)$ \triangleright l'algoritmo PEG prendo come parametri il grado dei
 - 5: \triangleright nodi variabile, il numero di righe e di colonne
 - 6: $\mathbf{G} \leftarrow \text{generaG}(\mathbf{H})$
 - 7: **Step 3:** Genera la code-word
 - 8: $\mathbf{c} \leftarrow \mathbf{s} \times \mathbf{G}$
 - 9: **Step 4:** Viene modulato il segno dei dati di Bob
 - 10: $\mathbf{m} \leftarrow \text{modulazione}(\mathbf{Y})$
 - 11: **Step 5:** Estrazione del messaggi fittizio da parte di Alice e calcolo LLR
 - 12: $\mathbf{r} \leftarrow \text{messaggioFittizio}(\mathbf{m})$
 - 13: $\mathbf{LLR} \leftarrow \text{calcoloLLR}(\mathbf{r}, \mathbf{X})$
 - 14: **Step 6:** Stima della code-word
 - 15: $\mathbf{c}' \leftarrow \text{sumProd}(\mathbf{LLR}, \mathbf{H})$
-

3.4.1 Algoritmi Sum-Product e classic PEG

Algorithm 3 : Sum-product decoding algorithm

Step 1: Inizializzazione dei messaggi dei nodi variabile $L(q_{i,j})^{(0)}$

for $i \leftarrow 0; M$ **do**

for $j \leftarrow 0; N$ **do**

$L(q_{i,j})^{(0)} \leftarrow LLRs_i$

end for

end for

for $k \leftarrow 1; maxRound$ **do**

Step 2: Calcola messaggi di check

for $i \leftarrow 0; N$ **do**

$tmp \leftarrow 1$

for $j \leftarrow 0; M$ **do**

for each $w \in C_i$ **do**

if $w \neq i$ **then**

$tmp \leftarrow tmp * \tanh\left(\frac{1}{2}L(q_{w,j})^{(k-1)}\right)$

end if

end for

$L(r_{j,i})^{(k)} \leftarrow 2 \tanh^{-1}(tmp)$

end for

end for

Step 3: Aggiorna i messaggi dei nodi variabile

for $i \leftarrow 0; N$ **do**

for $j \leftarrow 0; M$ **do**

$tmp \leftarrow 0$

for each $w \in V_i$ **do**

if $w \neq i$ **then**

$tmp \leftarrow tmp + L(r_{w,i})^{(k)}$

end if

end for

$L(q_{i,j})^{(k)} \leftarrow LLRs_i + tmp$

end for

end for

Step 4: Aggiorna LLRs aggiornate

for $i \leftarrow 0; LLRs.size()$ **do**

$tmp \leftarrow 0$

for each $j \in V_i$ **do**

$tmp \leftarrow tmp + L(r_{i,j})^{(k)}$

end for

$L(Q_i) \leftarrow LLRs_i + tmp$

end for

end for

Step 5: Stima C

for $i \leftarrow 1; LLRs.size()$ **do**

if $LLRs_i \geq 0$ **then**

$C_i \leftarrow 0$

else

$C_i \leftarrow 1$

end if

end for

Conclusioni e sviluppi futuri

La tesi è finita

Bibliografia

- [BB14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, dec 2014.
- [BS] Saumya Borwankar and Dhruv Shah. Low Density Parity Check Code (LDPC Codes) Overview.
- [DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.
- [FNZG22] Xiaodong Fan, Qianhao Niu, Tao Zhao, and Banghong Guo. Rate-compatible ldpc codes for continuous-variable quantum key distribution in wide range of snrs regime. *Entropy*, 24(10), 2022.
- [Gal72] Robert Gallager. *Information Theory and Reliable Communication*. Springer Vienna, 1972.
- [GET⁺21] Kadir Gümüş, Tobias A Eriksson, Masahiro Takeoka, Mikio Fujiwara, Masahide Sasaki, Laurent Schmalen, and Alex Alvarado. A novel error correction protocol for continuous variable quantum key distribution. *Scientific reports*, 11(1):10465, 2021.
- [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].
- [RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [RU08] T. Richardson and R. Urbanke. *Modern Coding Theory*. Cambridge University Press, 2008.
- [Sha49] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.
- [Sho94] P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
- [Zha18] Yusheng Zhao. Development of Quantum Key Distribution and Attacks against It. *J. Phys.: Conf. Ser.*, 1087:042028, September 2018.