Provability of Security and Efficiency of Quantum Key Distribution (QKD) Algorithms

Master's Thesis Submitted
in Partial Fulfilment of the Requirements
for the Degree of

MASTER OF TECHNOLOGY

in
Computer Science

by

Vinayak Bhogan
(Roll No. CS1708)

to the

DEPARTMENT OF COMPUTER SCIENCE
INDIAN STATISTICAL INSTITUTE
KOLKATA - 700108, INDIA

Jun 2019

CERTIFICATE

This is to certify that the work contained in this report entitled **"Provability of Security and Efficiency of Quantum Key Distribution (QKD) Algorithms"** submitted by **Vinayak Bhogan** (**Roll No: CS1708**) to Department of Computer Science, Indian Statistical Institute Kolkata towards the requirement of the course dissertation has been carried out by him/her under my supervision.

Prof. Subhamoy Maitra
Professor (Higher Academic Grade)
Applied Statistics Unit
Indian Statistical Institute

ABSTRACT

With recent developments in quantum communications, much of the focus has been put on development of different Quantum Key Distribution(QKD) protocols that can successfully generate a symmetric key over insecure quantum channel.

In this thesis, I have discussed in-depth security proof of a well known secure protocol named as BB84 protocol. This simple version of proof was first proposed by Shor and Preskill[1], in year 2000. It involves two step derivation of BB84 protocol from a 'Lo-Chau' protocol, which has already been proven secure. I shall provide proof of exponentially lower bounds on mutual information shared between sender/receiver and an adversary, therfore proving its security.

Along with it, I have also introduced another varient of Lo-Chau protocol which is more efficient in terms of shared resources, i.e. it uses almost 50% lesser quantum states exchanged over channel. I shall also prove it to be secure using the same technique used for BB84.

Acknowledgements

I thank Prof. Subhamoy Maitra for his guidance regarding the security proof presented for BB84 protocol. His suggestions about ongoing research has been of lot of help to understand the right approach to be taken for security proof. The inputs provided by prof. Maitra has been crucial to build the intuition for new protocol, for which I am grateful.

PREFACE

Major part of this thesis involves details of the security proof for BB84 protocol. While first chapter gets into basics of CSS codes, chapters 2 and 3 describe the overall transformation of protocols from Lo-Chau to BB84. The 5_{th} chapter deals with final bounds over qunatum information in Lo-Chau protocol.

Last chapter introduces to GHZ state and its alternate representation which is of lot of use to detect evesdropping. I have introduced a new, efficient 'GHZ' protocol in this chapter, along with it's working and proof of security.

Contents

Chapter 1

CSS codes

1.1 Introduction

CSS represents optimal family of quantum error correcting codes designed to correct both bit flip as well as phase flip errors that occurr qubits while transmission.

1.2 Construction

For constructing a CSS code, we must have 2 linear codes at our hands satisfying following properties :

- C_1 must be an $[n, k_1]$ and C_2 must be an $[n, k_2]$ linear code for $k_2 < k_1$
- $C_2 \subseteq C_1$
- If C_1 and $C_2^{\perp}$ both can correct upto t errors, then the resulting CSS code will be an $[n, k_1 - k_2]$ code that can correct upto t quantum errors (can correct t bit flip and t phase flip errors arbitrarily)

1.3 Encoding

1. Let $N = 2^{k_1 - k_2}$. The space spanned by all possible encodings will have dimention N. Select codewords $x_0, \ldots, x_{2^N - 1} \in C_1$, such that

$$x_i + x_j \notin C_2$$

for $i \neq j$ (there always exists such vector since $k_1 - k2 > 0$ implies $C_1 \neq C_2$)

2. If we denote classical states in $k_1 - k_2$ qubits with numbers $0, 1, \ldots, N-1$ in binary as x_j, then j^{th} state is encoded as,

$$|j\rangle \longmapsto |x_j + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x_j + y\rangle$$

1.4 Decoding

While correcting errors using CSS codes, we shall make use of Hadamard gates and few properties of C_1, C_2 *and* $C_2^{\perp}$. So before going into actual steps for decoding CSS codes, we shall delve into proving few propositions about Hadamard gates as well as $C_2^{\perp}$.

1.4.1 Facts used in decoding CSS codes

Mathematically, the Hadamard gate (H) transformations are defined as,

$$H(|0\rangle) = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Proposition 1. *Let $|x\rangle$ be any binary representation of n qubit states formed of states $|0\rangle$ and $|1\rangle$. Then ,*

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in {F_2}^n} (-1)^{y \cdot x} |y\rangle$$

Where F_2^n is vector space of n dimension

Proof. We shall prove this by induction over n.
Base case ($n = 1$) :
This case is pretty straight forward as,

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{y \in F_2 = \{0,1\}} (-1)^{y \cdot 0} |y\rangle$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{y \in F_2 = \{0,1\}} (-1)^{y \cdot 1} |y\rangle$$

Inductive Hypothesis : Suppose the proposition holds for all the the values up to $n = k$
Inductive step : Let $n = k+1$, and $|x\rangle = |x_k\rangle \otimes |x'\rangle$, where $|x'\rangle$ is last qubit.

$$\begin{aligned}
H^{\otimes(k+1)}|x\rangle &= (H^{\otimes k} \otimes H)(|x_k\rangle \otimes |x'\rangle) \\
&= H^{\otimes k}|x_k\rangle \otimes H|x'\rangle \\
&= \left(\frac{1}{\sqrt{2^k}} \sum_{y \in {F_2}^k = \{0,1\}^k} (-1)^{y \cdot x_k} |y\rangle \right) \left(\frac{1}{\sqrt{2}} \sum_{w \in F_2 = \{0,1\}} (-1)^{w \cdot x'} |w\rangle \right) \\
&= \frac{1}{\sqrt{2^{k+1}}} \sum_{y \in {F_2}^k = \{0,1\}^k} \Big((-1)^{y \cdot x_k + 0 \cdot x'} |y\rangle|0\rangle + (-1)^{y \cdot x_k + 1 \cdot x'} |y\rangle|1\rangle \Big) \\
&= \frac{1}{\sqrt{2^{k+1}}} \sum_{y \in {F_2}^{k+1} = \{0,1\}^{k+1}} (-1)^{y \cdot x} |y\rangle
\end{aligned}$$

QED. □

Proposition 2. *If $z \in C_2^{\perp}$, then $\sum_{y \in C_2} (-1)^{y \cdot z} = |C_2|$*

Proof. By definition,

$$C_2^{\perp} = \{u | u \cdot v = 0 \; for \; \forall v \in C_2\}$$

So, for any $z \in C_2^{\perp}$

$$\begin{aligned}
\sum_{y \in C_2} (-1)^{y \cdot z} &= \sum_{y \in C_2} (-1)^0 = \sum_{y \in C_2} 1 \\
&= |C_2|
\end{aligned}$$

□

Proposition 3. *If $z \notin C_2^{\perp}$, then $\sum_{y \in C_2} (-1)^{y \cdot z} = 0$*

Proof. We begin the proof by defining a function f_z as follows

$$\begin{aligned}
f_z : C_2 &\to \{0, 1\} \\
f_z(y) &= (z \cdot y) \; mod \; 2
\end{aligned}$$

Where

$z \in F_2^n$ but $z \notin C_2^{\perp}$
$y \in C_2$
$z \cdot y \rightarrow$ Dot product of vectors z and y

We already know that the linear code C_2 is subspace of F_2^n, therefore it is a **group under binary vector addition**. Same can be said for set $\{0, 1\}$, as a group with identity 0.
It could be easily seen that,

$$\begin{aligned} f_z(0) &= z \cdot 0 = 0 \\ f_z(y_1 + y_2) &= z \cdot (y_1 + y_2) \; mod \; 2 \\ &= z \cdot y_1 \; mod \; 2 + z \cdot y_2 \; mod \; 2 \\ &= f_z(y_1) + f_z(y_2) \end{aligned}$$

This indicates f_z is a **homomorphism**, with some kernel $K = \{u | u \in C_2 \; and \; f_z(u) = 0\}$. K is non empty as $0 \in C_2$ and $f_z(0) = 0$ therefore, $0 \in K$.
By first homomorphism theorem,

$$C_2 \setminus K \approx \{0, 1\}$$

This implies there are exactly 2 distinct cosets $K \; and \; K'$ partitioning C_2 into equal parts of size $|K|$, such that,

$$f_z(K) = 0 \tag{a}$$
$$f_z(K') = 1 \tag{b}$$

From a and b,

$$\sum_{y \in C_2} (-1)^{y \cdot z} = 0$$

as required. □

1.4.2 Decoding steps

Assume the transmitted state is

$$|x + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} |x + y\rangle$$

And let the received state be,

$$|x' + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y + e_1\rangle$$

Where
$e_1 \rightarrow$ Binary error vector representing bit flips
$e_2 \rightarrow$ Binary error vector representing phase flips

1. First we make use of codes C_1 to correct e_1. Using parity check matrix H_1 for C_1, we first detect the syndrome and correct the bit flip errors. The resultant state after correction would be,

$$|x' + C_2\rangle \xrightarrow{C_1 \, correct} \frac{1}{\sqrt{|C_2|}} \sum_{y \in C_2} (-1)^{(x+y)\cdot e_2} |x + y\rangle$$

2. To detect and correct e_2, we first apply Hadamard transform on above state. By using proposition 1, we get,

$$|x' + C_2\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n |C_2|}} \sum_{y \in C_2} \sum_{w \in {F_2}^n} (-1)^{(x+y)\cdot e_2} \cdot (-1)^{(x+y)\cdot w} |w\rangle$$

$$|x' + C_2\rangle = \frac{1}{\sqrt{2^n |C_2|}} \sum_{w \in {F_2}^n} \sum_{y \in C_2} (-1)^{(x+y)\cdot (w+e_2)} |w\rangle$$

Substitute $w' = w + e_2$. As w spans over all the vectors in space ${F_2}^n$ and e_2 is just a random constant vector, w' also takes up every vector in ${F_2}^n$.

$$|x' + C_2\rangle = \frac{1}{\sqrt{2^n |C_2|}} \sum_{w' \in {F_2}^n} \sum_{y \in C_2} (-1)^{(x+y)\cdot (w')} |w' + e_2\rangle$$

This substitution indicates how phase errors are being converted into bit errors.

3. Now lets rewrite above expression in two parts of outer sum over F_2^n

$$|x' + C_2\rangle = \frac{(-1)^{x\cdot w'}}{\sqrt{2^n|C_2|}} \left(\sum_{\boldsymbol{w' \in C_2^\perp}} \sum_{y\in C_2} (-1)^{y\cdot w'} |w' + e_2\rangle + \sum_{\boldsymbol{w' \notin C_2^\perp}} \sum_{y\in C_2} (-1)^{y\cdot w'} |w' + e_2\rangle \right)$$

Using propositions 2 and 3, we arrive at expression

$$|x' + C_2\rangle = \frac{(-1)^{x\cdot w'}}{\sqrt{2^n|C_2|}} \left(\sum_{\boldsymbol{w' \in C_2^\perp}} |C_2| \cdot |w' + e_2\rangle + 0 \right)$$
$$|x' + C_2\rangle = \frac{1}{\sqrt{2^n/|C_2|}} \sum_{\boldsymbol{w' \in C_2^\perp}} (-1)^{x\cdot w'} |w' + e_2\rangle$$

4. Using parity check matrix $H_2^\perp$ of $C_2^\perp$, we correct e_2.

$$|x' + C_2\rangle \xrightarrow{C_2^\perp correct} \frac{1}{\sqrt{2^n/|C_2|}} \sum_{w'\in C_2^\perp} (-1)^{x\cdot w'} |w'\rangle$$

5. Finally, to recover original state, we apply Hadamard transform again

$$|x' + C_2\rangle \xrightarrow{H^{\otimes n}} \frac{1}{\sqrt{2^n/|C_2|}} \left(\frac{1}{\sqrt{2^n}} \sum_{v\in F_2^n} \sum_{w'\in C_2^\perp} (-1)^{x\cdot w'} (-1)^{v\cdot w'} |v\rangle \right)$$
$$|x' + C_2\rangle = \frac{\sqrt{|C_2|}}{2^n} \left(\sum_{v\in F_2^n} \sum_{w'\in C_2^\perp} (-1)^{(x+v)\cdot w'} |v\rangle \right)$$

Substituting $v' = x + v$,

$$|x' + C_2\rangle = \frac{\sqrt{|C_2|}}{2^n} \left(\sum_{v'\in F_2^n} \sum_{w'\in C_2^\perp} (-1)^{v'\cdot w'} |x + v'\rangle \right)$$

$$|x' + C_2\rangle = \frac{\sqrt{|C_2|}}{2^n} \left(\sum_{v' \in C_2} \sum_{w' \in C_2^\perp} (-1)^{v' \cdot w'} |x + v'\rangle \right) + \frac{\sqrt{|C_2|}}{2^n} \left(\sum_{v' \notin C_2} \sum_{w' \in C_2^\perp} (-1)^{v' \cdot w'} |x + v'\rangle \right)$$

Using proposition 2 and 3,

$$|x' + C_2\rangle = \frac{\sqrt{|C_2|}}{2^n} \left(\sum_{v' \in C_2} |C_2^\perp| |x + v'\rangle + 0 \right)$$

Substituting $|C_2^\perp| = \dfrac{|F_2^n|}{|C_2|} = \dfrac{2^n}{|C_2|}$

$$|x' + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{v' \in C_2} |x + v'\rangle$$

Just like the original state transmitted.

Chapter 2

Lo and Chau protocol to CSS

2.1 Modified Lo and Chau protocol

2.1.1 Introduction - Lo and Chau(LC) protocol

Lo and Chau (LC) protocol [2] aims to share a secret key through sharing entangled qubit pairs between sender (Alice) and receiver(Bob), while providing exponential security against evesdropper (Eve) or channel errors (Collectively refered as transmission errors). We shall prove how LC protocol acheives this security with help of random parity checks in later chapter.

The slightly modified version of LC protocol is as follows

2.1.2 Protocol 1 : Modified Protocol

1 Alice creates $2n$ EPR pairs in Bell state $(\Phi^+)^{\otimes 2n}$. Each pair of qubits, has Bell state $\Phi^+ = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. So there are total $4n$ qubits in total, forming $2n$ entangled pairs.

2 Alice randomly selects a binary string b of size $2n$, and performs Hadamard transform on second part of pair for which b is 1. That is, if j^{th} bit of b is 1, then Hadamard transform is applied on second qubit of j^{th} EPR pair. So the effective j^{th} pair's state would be,

$$\Phi_j^+ = (I \otimes H)\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{|0\rangle|+\rangle+|1\rangle|-\rangle}{\sqrt{2}}$$

3 Alice sends second half/second qubit of each EPR pair to Bob

4 Bob receives the qubits and announes it publically through classical channel. After this, Both Alice and Bob holds $2n$ qubits each.

5 Alice selects n of the $2n$ qubits she has, as check bits for Eve's intereference. Here Alice simply selects the qubits for checking, but performs no measurement as Bob still has few qubits transformed by Hadamard gate (as done in step [2]).

6 Alice publically annouces the string b, along with positions of check bits.

7 Bob then performs Hadamard transform on qubits where b is 1.

8 Alice and Bob measure their halves of the n check EPR pairs in $|0\rangle$, $|1\rangle$ basis and share the results. This is done to identify if Eve's presence. Alice and bob share their measurements over classical channel, and if too many of those measurements disagree (Indication of Eve's presence), they abandon the protocol.

9 Once possibility of Eve's presence is ruled out, its time to correct quantum channel/transmission errors. To do this, Alice and Bob make the measurements on code (non-check) qubits of σ_z (To correct bit flip errors) and σ_x(To correct phase flip errors). This is so called **Entanglment Purification**. Alice and Bob share their results, and transform their states to achieve nearly perfect m EPR pairs

10 Alice and Bob finally measure remaining m EPR pairs in $|0\rangle$, $|1\rangle$ basis to obtain a shared secret key.

2.2 Useful definitions and propositions

The modified LC protocol shares n imperfect EPR pairs, each in Φ^+ state, and arrives at m near perfect EPR pairs after entanglement purification. This process is just like traditional error correcting codes, where messages of m bit length are protected by n bit codeword.

First we define few terms

Definition 1 (Parameterised CSS code)**.**
Let F_2^n be a binary vector space on n bits. Two linear codes C_1 and C_2 (each correcting upto t bit errors) contained in F_2^n such that

$$\{0\} \subset C_1 \subset C_2 \subset F_2^n$$

Let x, z be n bit binary vectors. Then, $\boldsymbol{Q_{x,z}}$ is called parameterised CSS code, where for each vector in $v \in C_1$, the corresponding codeword is,

$$v \to \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w \cdot z} |v + w + x\rangle$$

Proposition 4. *Bit flips and phase flip error rates detected by individual qubit measurement are same as the rates detected by Bell basis measurement.*

Proof. Ideally any entangled pair shared among Alice and Bob must have a state Φ^+. However due to channel errors it may get flipped onto one of the states below :

$$\Phi^+ = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \xrightarrow{Bit\ flip} \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{2} = \Psi^+$$
$$\Phi^+ = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \xrightarrow{phase\ flip} \frac{|0\rangle|0\rangle - |1\rangle|1\rangle}{2} = \Phi^-$$
$$\Phi^+ = \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}} \xrightarrow{Bit\ \&\ phase\ flip} \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{2} = \Psi^-$$

If we take 2 qubits, say $|00\rangle$ at a time then their resultant state after a single bit flip would be,

$$|00\rangle \xrightarrow{Bit\ flip} |01\rangle \text{ or } |10\rangle \tag{a}$$

Assuming errors are truely uniformly random, a bit flip error leads to states $|\Psi^+\rangle$ and $|\Psi-\rangle$ with equal probability. So resultant state of bit flipped qubits is ensemble of both states $|\Psi^+\rangle$ and $|\Psi^-\rangle$. Let the erroneous state has density matrix D_b

$$\begin{aligned} D_b &= \frac{1}{2}\left(|\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\right) \\ &= \frac{1}{2}\left[\frac{1}{2}\left(|01\rangle + |10\rangle\right)\left(\langle 01| + \langle 10|\right) + \frac{1}{2}\left(|01\rangle - |10\rangle\right)\left(\langle 01| - \langle 10|\right)\right] \end{aligned}$$

$$= \frac{1}{4}(\ |01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10| + |01\rangle\langle 01|$$
$$- |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10| \ )$$
$$= \frac{1}{2}\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)$$

$D_b = \frac{1}{2}\left(|01\rangle\langle 01| + |10\rangle\langle 10|\right)$ indicates that D_b is exactly equal to to ensemble of states $|01\rangle$ and $|10\rangle$, with equal probability.
$\therefore$ Measurement of bit flips in terms of Ψ^- and Ψ^+, is same as measring bit flips using state $|00\rangle$

Similarly, we can show that, for phase flip errors,

$$D_p = \frac{1}{2}\left(|\Phi^-\rangle\langle\Phi^-| + |\Psi^-\rangle\langle\Psi^-|\right)$$
$$= \frac{1}{2}\left(|+-\rangle\langle +-| + |-+\rangle\langle -+|\right)$$

□

2.3 Conversion of LC protocol to CSS

In this section, we show with subtle changes, we can convert the LC protocol into a CSS code.

2.3.1 Similarities between CSS and LC protocol

1. LC protocol initially shares imperfect $(\Phi^+)^{\otimes n}$ state between Alice and bob and later arrive at near perfect $(\Phi^+)^{\otimes m}$ $(m < n)$ through entanglement purification protocol, which is nothing but CSS code Q of n qubits, protecting m qubits from channel error, where $m < n$.

2. Once Eve's interference is ruled out, entanglement purification process (Which is CSS code correction in modified LC protocol) done by both Alice and Bob by the syndrome measurements on code qubits to detect any error. Alice and Bob share their results & both applies Z or X or both transforms accordingly.
   Once all qubits are shared by Alice to Bob, each party does this by syndrome measurements σ_z and σ_x for each row in H_1 and H_2 respectively.

However when error rate is under limit, **It doesn't matter if Alice measures her syndrome before or after the transmission of qubits**. If Alice measures her share before qubit transmission, with error measurements as x & z as bit and flip error vectors respectively, . As Alice detected the errors x, y with first part of EPR pairs, the second part must have same errors x, y. So, when bob receives scond part of EPR pairs, he must correct x, y on top of general channel errors.So it is equivalent of sending bob with parameterized CSS code $Q_{x,y}$ 1.

3. Now, Along with syndrome measurements, Alice can also measure the m qubits at her end before sending the Bob's share of qubits. This doesn't affect the outcome i.e. a random key k on both sides, because error rate is in permissible limit and thus correctable by CSS code and particles shared with Bob are/were entangled in Φ^+ state. Once Alice measures her share, all Bob has to do receive, correct and then measure his share which will be perfectly in sync with Alice.

   Combining it with second step, this is same as Alice Encoding a random key K of size m, using a parameterized CSS code $Q_{x,y}$ as,

$$K \rightarrow \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w \cdot z} |K + w + x\rangle$$

2.3.2 Protocol 2 : CSS code

In this section, we integrate the changes discussed in similarities from LC protocol and convert it into CSS protocol. Detailed steps of CSS protocol equivalent to LC protocol are as follows :

1. Alice creates n check qubits, a random key of K of size m and random key b of size $2n$.

2. Alice also chooses two random n bit strings x, y, as parameters for CSS code $Q_{x,y}$.

3. Alice encodes key $|K\rangle$ using $Q_{x,y}$ as

$$|K\rangle \rightarrow \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w \cdot z} |K + w + x\rangle$$

4. Alice chooses n out of $2n$ and puts check bits in these position and code bits in rest

5. Alice applies Hadamard transform to the qubits having position where b is 1. The resultant state is sent to Bob.

6. Alice announces b, positions of check bits, and x, y so Bob can figure out $Q_{x,y}$

7. Bob performs Hadamard transform on qubits where b is 1.

8. Bob checks if too many qubits are in error, aborts the protocol if so.

9. Bob uses $Q_{x,y}$ and decodes the key K

Chapter 3

CSS protocol to BB84

3.1 Propositions

Proposition 5. *Through **CSS protocol**, Alice effectively shares the mixed state*

$$M = \frac{1}{|C_2|} \sum_{w \in C_2} |k' + w + x\rangle\langle k' + w + x|$$

with bob when averaging over phase error z.

Proof. In CSS protocol, Alice's shares n qubits to bpb, collectively in state,

$$|N\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{w \in C_2} (-1)^{w \cdot z} |k + w + x\rangle$$

encoding m bit key k, using subspace C_2. The density matrix representation of the state would be,

$$\begin{aligned} D_N &= |N\rangle\langle N| \\ &= \left(\frac{1}{\sqrt{|C_2|}} \sum_{w_1 \in C_2} (-1)^{w_1 \cdot z} |k + w_1 + x\rangle \right) \cdot \left(\frac{1}{\sqrt{|C_2|}} \sum_{w_2 \in C_2} (-1)^{w_2 \cdot z} \langle k + w_2 + x| \right) \\ &= \frac{1}{|C_2|} \sum_{w_1, w_2 \in C_2} (-1)^{(w_1 + w_2) \cdot z} |k + w_1 + x\rangle\langle k + w_2 + x| \end{aligned}$$

Averaging over all the z, we get,

$$D_N = \frac{1}{2^n |C_2|} \sum_{z \in F_2^n} \sum_{w_1, w_2 \in C_2} (-1)^{(w_1 + w_2) \cdot z} |k + w_1 + x\rangle\langle k + w_2 + x|$$

$$= \frac{1}{2^n|C_2|} \sum_{\substack{w_1,w_2 \in C_2 \\ w_1 \neq w_2}} (-1)^{(w_1+w_2)\cdot z} |k+w_1+x\rangle\langle k+w_2+x| + \sum_{\substack{w_1,w_2 \in C_2 \\ w_1 = w_2}} (-1)^{(w_1+w_2)\cdot z} |k+w_1+x\rangle\langle k+w_2+x|$$

Now, the function $(-1)^{(w_1+w_2)\cdot z}$ is gives balanced output,i.e. -1 for half the input and 1 for rest, $\forall z \in F_2^n$, whenever $w_1 \neq w_2$ or $w_1 + w_2 \neq 0$. This means all the terms in summation $\sum_{\substack{w_1,w_2 \in C_2 \\ w_1 \neq w_2}} (\cdots)$ will be zero.
So we are left with,

$$\begin{aligned} D_N &= \frac{1}{2^n|C_2|} \sum_{\substack{w_1,w_2 \in C_2 \\ w_1 = w_2}} (-1)^{(w_1+w_2)\cdot z} |k+w_1+x\rangle\langle k+w_2+x| \\ &= \frac{1}{2^n|C_2|} \sum_{z \in F_2^n} \sum_{w \in C_2} (-1)^{(w+w)\cdot z} |k+w+x\rangle\langle k+w+x| \\ &= \frac{1}{|C_2|} \sum_{w \in C_2} |k+w+x\rangle\langle k+w+x| \end{aligned}$$

□

3.2 Similarities between CSS and BB84

1. Under CSS protocol, Alice exchanges vectors x, z with Bob to correct the entanglement on both sides. However, **key is solely dependent on entangled qubit values so Bob can work just fine with having information only about $\boldsymbol{x}$**, and Alice can completely discard phase error z. With ignoring z value, Alice effectively shares mixture of states $|k+x+w\rangle$ (as described in proposition 5)

2. In BB84 protocol, Alice first sends qubits to Bob, which he measures in random basis (either in $|0\rangle, |1\rangle$ or $|+\rangle, |-\rangle$ basis). Both Alice and Bob discards the qubits which were measured in different basis. Among whats left, after check bit evaluation,let Alice has string of qubits v while Bob has same copies of qubits with some channel error, $v + e$.

3. Alice can choose any random valid codeword $u \in C_1$, and send $u + v$. All bob has to do is add his state to this new state received from Alice, so Bob has $(u + v) + v + e = u + e$ state, which Bob can always correct to u. This random codeword $u + C_2$ will can serve as new key.

4. In CSS protocol, Alice shares $|k + w + x\rangle$ and share x with Bob over classical channel so Bob can retrive key k. Similary in BB84 protocol, Alice shares key u with additional information v, which even Bob has with some error. So Alice shares $|u + v + C_2\rangle$, which bob then makes $u+e+C_2$ and corrects it to $|u+C_2\rangle$. Which tells us these two protocols are equivalent.

3.3 BB84 (Modified)

1. Alice creates $(4 + \delta)n$ random bits.

2. Alice chooses a random $(4+\delta)n$ bit string b. For each bit, she creates a state in the $|0\rangle$, $|1\rangle$ (if corresponding bit of b is 0) or the $|+\rangle$, $|-\rangle$ basis (if the bit of b 1).

3. Alice sends the resulting qubits to Bob.

4. Bob receives the $(4 + \delta)n$ qubits, measuring each in either $|0\rangle$, $|1\rangle$ or $|+\rangle$, $|-\rangle$ basis at random.

5. Alice announces b

6. Bob discards any results where he measured a different basis than Alice prepared. With high probabiltiy, there are at least $2n$ bits left (if not, abort the protocol). Alice decides randomly on a set of $2n$ bits to use for the protocol, and chooses at random n of these to be check bits.

7. Alice and Bob announce the values of their check bits. If too few of these values agree, they abort the protocol.

8. Alice announces $u+v$, where v is the string consisiting of the remaining non-check bits, and u is a random codeword in C_1

9. Bob subtracts $u+v$ from his code qubits, $v+\epsilon$, and corrects the result, $u + \epsilon$ to codeword in C_1

10. Alice and Bob use the coset of $u + C_2$ as the key.

Chapter 4

Security Analysis

4.1 Introduction

So far we have proved equivalance of Modified Lo-Chau protocol and BB84 protocol using CSS code as link between them. In this chapter, we shall focus on proving security of Modified Lo-Chau protocol against evesdroppers. The proof shall focus on quantum information theory and Eve's mutual information gain of secret key throughout the protocol.

4.2 Quantum Information : Definitions and General Propositions

4.2.1 Quantum Entropy

To understand the information gained over exchange of qubits, let us analyze the following scenario between two peers, Alice and Bob :

- Alice samples $X \in \Sigma \subseteq \{0,1\}^n$, where $X = x$ with some probability $p(x)$
- Alice sends state with density matrix $\sigma_X \in \mathbb{C}^{d \times d}$
- Bob picks POVM's (positive operator valued measure) $\{E_y\}_{y \in \Gamma}$, where $\Gamma \subseteq \{0,1\}^n$

- Bob measures σ_X, and receives output $Y \in \Gamma$, where $Y = y$ given $X = x$ with probability $tr(E_y\sigma_x)(= p_{y|x})$.
- Bob tries to identify X from Y

From Bob's perspective, he gets different states σ_x with probability $p(x)$, and he has to distinguish between different σ_x's. So overall, mixed state seen by Bob is,

$$\begin{cases} \sigma_{x_1} & \text{with prob. } p(x_1) \\ \sigma_{x_2} & \text{with prob. } p(x_2) \\ & \vdots \end{cases}$$
$$\equiv \sum_{x\in\Sigma} p(x)\sigma_x = \rho_B$$

And from Alice's point of view, its simply ensemble of pure states as follows :

$$\begin{cases} |x_1\rangle & \text{with prob. } p(x_1) \\ |x_2\rangle & \text{with prob. } p(x_2) \\ & \vdots \end{cases}$$
$$\equiv \sum_{x\in\Sigma} p(x)|x\rangle\langle x| = \rho_A$$

The joint state ρ of Alice and Bob is then simply tensor product of states; given as,

$$\rho_{AB} = \sum_{x\in\Sigma} p(x)|x\rangle\langle x| \otimes \sigma_x \tag{4.1}$$

It's easy to verify that $\rho_A = tr_B(\rho_{AB})$ and $\rho_B = tr_A(\rho_{AB})$. But how to measure the information contained in ρ ?

To answer this, we shall introduce the notion of **Quantum Entropy**, i.e. quantum counterpart of classical Shannon's entropy.

Definition 2 (Von Neumann Entropy)**.**
Given a mixed state with density matrix $\rho \in \mathbb{C}^{d\times d}$ *with eigenvalues* $\alpha_1, \alpha_2, \cdots, \alpha_d$*, with corresponding eigenvectors* $|u_1\rangle, \cdots, |u_d\rangle$*, then Von Neumann Entropy is defined as*

$$S(\rho) = \sum_{i=1}^{d} \alpha_i \log \frac{1}{\alpha_i}$$

As $\rho \log(1/\rho) = \sum_{i=1}^{d} \alpha_i \log(\frac{1}{\alpha_i})|u_i\rangle\langle u_i|$*, then we have the alternate form of entropy as,*

$$S(\rho) = tr(\rho \log(1/\rho))$$

4.2.2 Accessible information

First we need a measure of mutual entropy shared across two parties, which is given by Quantum mutual information [3]

Definition 3 (Quantum Mutual Information)**.**
If ρ *is joint state between two quantum systems* A *and* B *then the Quantum Mutual Information as,*

$$I(\rho_A; \rho_B) = S(\rho_A) + S(\rho_B) - S(\rho)$$

Also, as the quantum information extraction is solely dependant on Bob's measurement; let us define the 'Accessible Information' that Bob can extract from state.

Definition 4 (Accessible Information)**.**
Accessible information is the maximum possible mutual information obtained by best possible measurement,

$$I_{Acc}(\{p_x, \sigma_x\}) = \sup_{over\ all\ E_y} I(X;Y)$$

Now we move onto proving one of the important theorems known as Holevo's bound.

4.2.3 Holevo's Bound

Theorem 6 (Holevo's Bound)**.** *Let X be a classical random variable $\{p_x = Prob(X = x)\}$ and $\{p_x, \sigma_x\}$ a mixture of quantum states. Let Y represent measurement results on state $\rho_B = \sum_{x\in\Sigma} p_x\sigma_x$ in the basis $\{E_y\}$. Then,*

$$I(X,Y) \leq \chi(\{p_x,\sigma_x\}),\ \textit{and so}\ I_{acc}(p_x,\sigma_x) \leq \chi(p_x,\sigma_x)$$

where $\chi(p_x,\sigma_x) = S(\rho_B) - \sum_{x\in\Sigma} p_x S(\sigma_x)$

Proof.
As discussed earlier in equation 4.1, we have a joint state for Alice and Bob as given as,

$$\rho_{AB} = \sum_{x\in\Sigma} p(x)|x\rangle\langle x| \otimes \sigma_x$$

We will consider a larger state represented by Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, by adding ancilla bit used by Bob to store measurement result as follows

$$\rho_{AB} = \sum_{x\in\Sigma} p(x)|x\rangle\langle x| \otimes \sigma_x \otimes |0\rangle\langle 0| \tag{a}$$

Also we can define the measurement by Bob as unitary operator

$$U_{ABC} = I_A \otimes U_{BC}$$

where,

$$U_{BC}|\phi\rangle_B \otimes |a\rangle_C = \sum_y P_y|\phi\rangle_B \otimes |a \oplus y\rangle_C$$

So, when bob measures the state ρ_{ABC}

$$\rho'_{ABC} = U_{ABC}\rho_{ABC}U^\dagger_{ABC} = \sum_{x,y,y'} p_x|x\rangle\langle x| \otimes P_y\sigma_x P_{y'} \otimes |y\rangle\langle y'|$$

The states ρ_{ABC} and ρ'_{ABC} have the same eigenvalues, as latter is just unitary transformation of the prior. Thus their quantum entropies must be same.

$$S(\rho_{ABC}) = S(\rho'_{ABC})$$

The partial density matrices of joint system of Bob with ancilla, before and after the measurement will be just as follows :

$$\rho_{BC} = tr_A(\rho_{ABC}) = \sum_x p_x\sigma_x \otimes |0\rangle\langle 0|$$

And

$$\rho'_{BC} = tr(\rho'_{ABC}) = \sum_x P_y \sigma_x P_y \otimes |y\rangle\langle y'|$$

Again both ρ_{BC} and ρ'_{BC} have same entropy, since one can be converted into another by unitary transformation $I_A \otimes U_{BC}$. Thus we get,

$$S(\rho_{BC}) = S(\rho'_{BC})$$

From the property of strong subadditivity [3],

$$\begin{aligned} S(\rho'_{ABC}) + S(\rho'_C) &\leq S(\rho'_{AC}) + S(\rho'_{BC}) \\ S(\rho'_{ABC}) - S(\rho'_{BC}) &\leq S(\rho'_{AC}) - S(\rho'_C) \end{aligned}$$

Using facts $S(\rho_{BC}) = S(\rho'_{BC})$ and $S(\rho_{ABC}) = S(\rho'_{ABC})$,

$$S(\rho_{ABC}) - S(\rho_{BC}) \leq S(\rho_{AC}) - S(\rho_C) \tag{b}$$

Now we begin calculating each of the entropies in eq(b)

(1) $S(\rho_{ABC})$

$$S(\rho_{ABC}) = S(\sum_X p_x |x\rangle\langle x| \otimes \sigma_x \otimes |0\rangle\langle 0|)$$

Let us denote the spectral decomposition of σ_x as $\sigma_x = \sum_{a_x} \lambda_{a_x} |a_x\rangle\langle a_x|$. Then,

$$\sum_x p_x |x\rangle\langle x| \otimes \sigma_x \otimes |0\rangle\langle 0| = \sum_{x,a_x} p_x \lambda_{a_x} |x\rangle\langle x| \otimes |a_x\rangle\langle a_x| \otimes |0\rangle\langle 0|$$

As this is convex combination of mutually orthogonal states, we can write

$$\begin{aligned} S(\rho_{ABC}) &= -\sum_{x,a_x} p_x \lambda_{a_x} \log(p_x \lambda_{a_x}) \\ &= -\sum_{x,a_x} p_x \lambda_{a_x} \log(\lambda_{a_x}) - \sum_x p_x \log(p_x) \\ &= -\sum_x p_x S(\sigma_x) + H(X) \end{aligned} \tag{c}$$

(2) S(ρ_{BC})
As $\rho_{BC} = \sum_x p_x \sigma_x \otimes |0\rangle\langle 0| = \rho_B \otimes |0\rangle\langle 0|$, we can ignore last pure ancilla qubit which adds nothing to entropy. Then,

$$S(\rho_{BC}) = S(\rho_B) \tag{d}$$

(3) S(ρ'_{AC})

$$\begin{aligned}\rho'_{AC} &= tr_B(\rho'_{ABC}) \\ &= tr_B(\sum_{x,y,y'} p_x |x\rangle\langle x| \otimes P_y \sigma_x P_{y'} \otimes |y\rangle\langle y'|)\end{aligned}$$

By cyclicity of trace,

$$tr_B(P_y \sigma_x P_{y'}) = tr_B(P_{y'} P_y \sigma_x) = \delta_{yy'} p_{y|x}$$

And then we have,

$$\rho'_{AC} = \sum_{x,y} p_{x,y} |x\rangle\langle x| \otimes |y\rangle\langle y|$$

The states $|x\rangle\langle x| \otimes |y\rangle\langle y'|$ are mutually orthogonal, and thus this matrix is represents joint distribution of random variables (X, Y). Then the entropy value becomes,

$$S(\rho'_{A,B}) = H(X, Y) \tag{e}$$

(4) $S(\rho_C)$

First we have,

$$\begin{aligned}\rho'_C &= tr_A(\rho'_{AC}) \\ &= tr_A\left(\sum_{x,y} p_{x,y}|x\rangle\langle x| \otimes |y\rangle\langle y|\right) \\ &= \sum_{x,y} p_{x,y}|y\rangle\langle y| \\ &= \sum_{y} p_y|y\rangle\langle y|\end{aligned}$$

So we get,

$$S(\rho'_C) = H(Y) \tag{f}$$

Substituting eq(c), eq(d), eq(e), eq(f) in eq(b),

$$H(X) + \sum_x p_x S(\sigma_x) - S(\rho) \leq H(X,Y) - H(Y)$$

Using the substitutions $I(X,Y) = H(X,Y) - H(X) - H(Y)$ and $\chi(\{p_x, \sigma_x\}) = S(\rho) - \sum_x p_x S(\sigma_x)$,

$$I(X,Y) \leq \chi(\{p_x, \sigma_x\})$$

As required. □

4.3 Bounds on Mutual Information of Eve

In this section, we shall focus on how much of of mutual information Eve can get her hands on, in a quantum protocol to generate a secret key between Alice and Bob.
Let's begin by defining a measure of closeness between any two quantum states, say ρ and σ.

Definition 5 (Fidelity)**.**
The Fidelity of states ρ and σ is defined to be

$$F(\rho, \sigma) = tr(\sqrt{\rho^{1/2}\sigma\rho^{1/2}})$$

It is an important bounded measure as $F(\rho,\sigma) = F(\sigma,\rho)$ and $0 \leq F(\rho,\sigma) \leq 1$, with $F(\rho,\sigma) = 1$ when $\rho = \sigma$. In other words, more the states are similar,

higher the value of fidelity.
In *Modified Lo-Chau protocol*. Ideally, Alice and Bob must share perfect $(\Phi^+)^{\otimes n}$, however quantum channel noise and Eve's presence would cause them to share an imperfect state ρ. Now we shall derive upper bounds on information Eve can get about ρ.

Proposition 7. *If Alice and Bob share a state having fidelity* $F(\rho, |\Phi^+\rangle\langle\Phi^+|^{\otimes n})^2 > 1 - 2^{-s}$ *with* $(\Phi^+)^{\otimes n}$*, then Eve's mutual information with the key is at most* $2^{-c} + 2^{-2s}$ *where* $c = s - \log_2(2n + s + 1/\ln 2)$.

Proof. We shall begin with basic expression of fidelity given in defintion **??** with given states, ρ and $\sigma = (|\Phi^+\rangle\langle\Phi^+|)^{\otimes n}$

$$F(\sigma, \rho) = tr(\sqrt{\sigma^{1/2}\rho\sigma^{1/2}})$$

Since σ is a pure state desnity matrix, we have $\sigma = \sigma^{1/2}$. Using this, we can write,

$$\begin{aligned} F(\sigma, \rho) &= tr(\sqrt{\sigma\rho\sigma}) \\ &= tr(\sqrt{{}^{\otimes n}|\Phi^+\rangle\langle\Phi^+|\rho|\Phi^+\rangle\langle\Phi^+|^{\otimes n}}) \\ &= tr(\sqrt{{}^{\otimes n}\langle\Phi^+|\rho|\Phi^+\rangle^{\otimes n} \cdot {}^{\otimes n}|\Phi^+\rangle\langle\Phi^+|^{\otimes n}}) \end{aligned}$$

As ${}^{\otimes n}|\Phi^+\rangle\langle\Phi^+|\rho|\Phi^+\rangle\langle\Phi^+|^{\otimes n}$ is a scalar quantity, and $tr({}^{\otimes n}|\Phi^+\rangle\langle\Phi^+|^{\otimes n}) = 1$ as diagonal entries are simply the probability distribution of pure state,

$$F(\sigma, \rho) = \sqrt{{}^{\otimes n}\langle\Phi^+|\rho|\Phi^+\rangle^{\otimes n}} \tag{a}$$

Substituting eq(a) in the assumption $F(\sigma, \rho)^2 > 1 - 2^{-s}$, we get,

$${}^{\otimes n}\langle\Phi^+|\rho|\Phi^+\rangle^{\otimes n} > 1 - 2^{-s}$$

As product of eigenvalues of ρ gives the scalar product, largest eigenvalue of ρ must be greater than $1 - 2^{-s}$.
Also we can note the fact that sum of eigenvalues is nothing but trace of the matrix. Since $tr(\rho) = 1$, all the eigenvalues must sum upto 1. So removing largest eigenvalue, rest of them will sum up to at most 2^{-s}. Thus the density matrix ρ is bounded by density matrix ρ_{max} having largest diagonal value $1 - 2^{-s}$ and rest is equally distributed among $2^{2n} - 1$ diagonal entries as

$2^{-s}/(2^{2n}-1)$. The maximum entropy is,

$$\begin{aligned}
S(\rho_{max}) &= -(1-2^{-s})\log_2(1-2^{-s}) - 2^{-s}\log_2\left(\frac{2^{-s}}{2^{2n}-1}\right) \\
&= -\log_2(1-2^{-s}) + 2^{-s}\log_2(1-2^{-s}) - 2^{-s}\log_2(2^{-s}) \\
&\quad + 2^{-s}\log_2(2^{2n}-1) \\
&= -\log_2(1-2^{-s}) + 2^{-s}\log_2(1-2^{-s}) + s2^{-s} + 2n2^{-s} \\
&\quad + 2^{-s}\log_2(1-2^{-2n}) \\
&= \frac{1}{\ln(2)}\left(2^{-s} + \frac{2^{-2s}}{2} + \cdots\right) \\
&\quad + \frac{2^{-s}}{\ln(2)}\left(2^{-s} + \frac{2^{-2s}}{2} + \cdots\right) + s2^{-s} + 2n2^{-s} + 2^{-s}\log_2(1-2^{-2n}) \\
&= 2^{-s}\left(2n + s + \frac{1}{\ln 2}\right) + \frac{2^{-2s}}{\ln 2}\left(2^{-s} + \frac{2^{-2s}}{2} + \cdots\right) \\
&\quad + \left(\frac{2^{-2s}}{2} + \frac{2^{-3s}}{3} + \cdots\right) \\
&= 2^{-s}\left(2n + s + \frac{1}{\ln 2}\right) + O(-2s)
\end{aligned}$$

By Holevo's bound [6], $S(\rho)$ is an upper bound on information $I(X,Y)$ available to Eve. So the we have,

$$I(X,Y) \leq 2^{-c} + 2^{O(-2s)}$$

where $c = s - \log_2(2n + s + \frac{1}{\ln 2})$ □

This essentially proves that Eve's knowledge of the key through Lo and Chau protocol (modified) reduces exponentially as the fidelity of shared entanglement increases. As we also have shown that modified Lo and Chau protocol is equivalent to BB84, it also proves security of BB84 protocol.

Chapter 5

An Efficient QKD Scheme : GHZ Protocol

5.1 Introduction

So far major entanglement based QKD protocols has efficiency around 50% as half of the entanglements are lost in measurement to check Eve's presence, and then rest half of the entanglements are used to create shared key.
In this chapter, we shall present **GHZ protocol** that can achieve **0**% entanglement loss in quantum key distribution, thereby achieving 100% utilization of shared entanglement.

5.2 Definitions and Propositions

We shall begin by defining *Greenberger–Horne–Zeilinger (GHZ state)* that shall be used in establishing entanglements between Alice and Bob.

Definition 6 (Generalized GHZ state)**.**
A generalized GHZ state is an entangled quantum state of $N > 2$ subsystems defined as,

$$|GHZ\rangle = \frac{|0\rangle^{\otimes N} + |1\rangle^{\otimes N}}{\sqrt{2}}$$

But, we shall be more interested in GHZ state with $N = 4$. The total

possible different GHZ states for $N = 4$ are as follows :

$$G_0 = \frac{|0000\rangle + |1111\rangle}{\sqrt{2}} \qquad G_1 = \frac{|0001\rangle + |1110\rangle}{\sqrt{2}}$$
$$G_2 = \frac{|0010\rangle + |1101\rangle}{\sqrt{2}} \qquad G_3 = \frac{|0011\rangle + |1100\rangle}{\sqrt{2}}$$
$$G_4 = \frac{|0100\rangle + |1011\rangle}{\sqrt{2}} \qquad G_5 = \frac{|0101\rangle + |1010\rangle}{\sqrt{2}}$$
$$G_6 = \frac{|0110\rangle + |1001\rangle}{\sqrt{2}} \qquad G_7 = \frac{|0111\rangle + |1000\rangle}{\sqrt{2}}$$

However these GHZ states also has another representations, which are essential for developing our protocol. We shall express the representation for state G_0.

Proposition 8. *For the state* $G_0 = \frac{|0000\rangle+|1111\rangle}{\sqrt{2}}$*, we have*

$$G_0 = \frac{|\Phi^+\Phi^+\rangle + |\Phi^-\Phi^-\rangle}{\sqrt{2}}$$

Where Φ^+ *and* Φ^- *represent the Bell states.*

Proof.
We begin with statement,

$$G_0 = \frac{|\Phi^+\Phi^+\rangle + |\Phi^-\Phi^-\rangle}{\sqrt{2}} \tag{a}$$

We also got,

$$\Phi^+ = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \& \qquad \Phi^- = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{b}$$

Substituting eq(b) into eq(a), we get

$$G_0 = \frac{\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|00\rangle+|11\rangle}{\sqrt{2}}\right) + \left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)\cdot\left(\frac{|00\rangle-|11\rangle}{\sqrt{2}}\right)}{\sqrt{2}}$$
$$= \frac{1}{2\sqrt{2}}\left(|00\rangle|00\rangle + |00\rangle|11\rangle + |11\rangle|00\rangle + |11\rangle|11\rangle\right)$$

$$
\begin{aligned}
&\quad +|00\rangle|00\rangle - |00\rangle|11\rangle - |11\rangle|00\rangle + |11\rangle|11\rangle) \\
&= \frac{2\left(|00\rangle|00\rangle + |11\rangle|11\rangle\right)}{2\sqrt{2}} \\
&= \frac{|0000\rangle + |1111\rangle}{\sqrt{2}}
\end{aligned}
$$

As required. □

Moreover, this entanglement is valid with any kind of pairing of qubits. i.e. if $G_0 = \frac{|0_1 0_2 0_3 0_4\rangle + |1_1 1_2 1_3 1_4\rangle}{\sqrt{2}}$, then following is true as well :

$$
\begin{aligned}
G_0 &= \frac{|\Phi^+_{12}\rangle|\Phi^+_{34}\rangle + |\Phi^-_{12}\rangle|\Phi^-_{34}\rangle}{\sqrt{2}} = \frac{|\Phi^+_{13}\rangle|\Phi^+_{24}\rangle + |\Phi^-_{13}\rangle|\Phi^-_{24}\rangle}{\sqrt{2}} \\
&= \frac{|\Phi^+_{14}\rangle|\Phi^+_{23}\rangle + |\Phi^-_{14}\rangle|\Phi^-_{23}\rangle}{\sqrt{2}} \qquad \text{and so on ...}
\end{aligned}
$$

Where $\Phi^+_{ij} = \frac{|0_i 0_j\rangle + |1_i 1_j\rangle}{\sqrt{2}}$ and $\Phi^-_{ij} = \frac{|0_i 0_j\rangle - |1_i 1_j\rangle}{\sqrt{2}}$.

5.3 GHZ protocol

Now we introduce a new QKD protocol that utilizes all the qubits shared between Alice and Bob.

1. Alice creates n copies of $G_0 = \frac{|0000\rangle + |1111\rangle}{\sqrt{2}}$ state.
2. Alice selects a random n bit string b, and performs a Hadamard transform on 4^{th} qubit of i^{th} G_0 state, whenever i^{th} bit of b is 1.
3. Alice then sends first qubit of i^{th} state to Bob.
4. Once Bob receives all the n qubits, it annouces the fact on public channel.
5. Alice then performs Hadamrd transform again on 4^{th} qubit, and performs Bell basis measurement on 3^{rd} and 4^{th} qubit.
6. Under ideal conditions, these Bell measurements by Alice must return either Φ^+ or Φ^-. If too many of measurements results in Ψ^+ or Ψ^-, Alice aborts the protocol.

7. Alice and Bob make the measurements on code qubits of σ_z for each row in $r \in H_1$ and σ_x for each row $r \in H_2$. Alice and Bob share the results so as to obtain m nearly perfect EPR pairs.

8. Alice and Bob measure the EPR pairs in the $|0\rangle$, $|1\rangle$ basis to obtain a secret key.

5.4 How GHZ protocol works?

5.4.1 Detection of Eve's measurement

Consider the protocol executed between Alice and Bob using single G_0 state. If corresponding bit of b is 1, then Hadamard transform gets applied on fourth qubit. So the resultant state before Alice shares first qubit is,

$$\begin{aligned} G_0' &= (I \otimes I \otimes I \otimes H)G_0 \\ &= \frac{|000\rangle \frac{|0\rangle+|1\rangle}{\sqrt{2}}}{\sqrt{2}} + \frac{|111\rangle \frac{|0\rangle-|1\rangle}{\sqrt{2}}}{\sqrt{2}} \\ &= \frac{|0000\rangle + |0001\rangle + |1110\rangle - |1111\rangle}{2} \end{aligned}$$

As per the protocol, we then transfer first qubit to Bob. However, if Eve intervenes and measures the first qubit before it reaches Bob, the state G_0' collapses onto one of the superimposed state. For example, say it collapsed on state $|0000\rangle$ due to Eve's measurement. Now when Bob annouces he has received the first qubit, Alice will again apply Hadamard transform on 4^{th} qubit. So the resultant state will now be,

$$\begin{aligned} (I \otimes I \otimes I \otimes H)|0000\rangle &= \frac{|0000\rangle + |0001\rangle}{\sqrt{2}} \\ &= |00\rangle(|00\rangle + |01\rangle) \\ &= |00\rangle \left(\frac{|\Phi^+\rangle + |\Phi^-\rangle}{\sqrt{2}} + \frac{|\Psi^+\rangle + |\Psi^-\rangle}{\sqrt{2}} \right) \end{aligned}$$

Now when Alice performs Bell basis measurement on third and forth qubit, result will be Ψ^+ or Ψ^- with the probability of 0.5. Same results can be derived for other possible collapsed states $|0001\rangle, |1110\rangle$ and $|1111\rangle$ as well.

As Alice performs measurements for rest of the states, it is evident that rate of occurrence of states $|\Psi^+\rangle$ and $|\Psi^-\rangle$ indicates presence of Eve in channel.
There is still the probability of Eve transforming or replacing the qubits shared, however it can be radially verified by encoding mutually known public codewords using present key by one party while other party decodes varifies it

5.4.2 Generation of EPR pair in GHZ protocol

As soon as we rule out the possibility of Eve's measurement, Alice can simply do Bell basis measurement on 3^{rd} and 4^{th} and first two qubits shall share maximally entangled state $|\Phi^+$ (refer 8).

5.5 Security of GHZ protocol

In this section, we shall prove the security of GHZ protocol by converting it to Modified Lo-Chau protocol. Similarities between GHZ and Lo-Chau protocol :

1. Initially Alice shares first qubit of n G_0 states with Bob, like Lo-Chau protocol
2. By the time Alice finishes her measurements on third and forth qubits, Alice and Bob shares n imperfect Φ^+ states, exactly like Lo-Chau protocol.
3. From here onwards, the GHZ protocol works exactly like Lo-Chau protocol till the key is generated. Thus all the security bounds that exists on Lo-Chau protocol, are just the same for GHZ protocol.

5.6 Advantages over Lo-Chau Protocol

- To generate a Key of size m, only n qubits are shared in GHZ protocol, whereas Lo-Chau protocol requires $2n$ entanglements to be shared between Alice and Bob.

- Since Alice detects the Eve's measurement by solely local state measurements, errors introduced by state decoherence and experimental setup can be greatly reduced.

Bibliography

[1] Peter W. Shor, John Preskill. *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*.
AT&T Labs Research, Florham Park, NJ 07932, USA.
Lauritsen Laboratory of High Energy Physics, California Institute of Technology, Pasadena, CA 91125, USA.

[2] Hoi-Kwong Lo and Hoi-Kwong Lo. *Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances.*
Annalen der Physik, 322(10):891–921, 1905.

[3] Michael A. Nielsen & Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

[4] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin and W. K. Wootters. *Mixed state entanglement and quantum error correction*. Phys. Rev. A 54, 3824-3851 (1996), arXive e-print quant-ph/9604024

[5] A. R. Calderbank and P. Shor *Good quantum error correcting codes exists*. Phys. Rev. A 54, 1098-1105 (1996), arXive e-print quant-ph/9512032