An approach to global Quantum Communication using satellite quantum key distribution

Nimrat Kaur

A dissertation submitted for the partial fulfillment of

BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali

June 2020

Certificate of Examination

This is to certify that the dissertation titled ”An approach to global Quantum Communication using satellite quantum key distribution” submitted by Ms. Nimrat Kaur (Reg. No. MS15054) for the partial fulfilment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Sandeep Goyal Dr. Kavita Dorai Dr. Arvind

(Supervisor)

Dated: June 8, 2020

Declaration

The work in this dissertation has been carried out by me under the guidance of Dr. Arvind at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgement of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Nimrat Kaur

(Candidate)

Dated: June 8, 2020

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Dr. Arvind

(Supervisor)

Acknowledgements

It is my pleasant duty to thank a large number of people and institutions, for the various forms of support, encouragement, and help that they have provided during the time spent on this thesis.

First and foremost, I'd like to thank Dr. Arvind for providing me with the opportunity to work under his able guidance and for his continuous support over the past year. Besides my advisor, I'd like to thank rest of my thesis committee: Dr. Kavita Dorai and Dr. Sandeep Goyal who, via the means of evaluation, kept pushing me forward. I'd specially like to thank Jaskaran Singh and Soumyakanti Bose for the meaningful discussions that have been a significant part of this thesis. Along with them, I'd also like to thank Rajendra Singh Bhati, Kirtpreet Singh, Jorawar Singh, and the other members of Quantum Computation and Quantum Information(QCQI) group who have been a constant guidance and support during the previous year.

I'd like to extend my gratitude to my parents for being a constant pillar of love and strength, who have been there whenever I needed them the most. I'd like to thank my siblings who have been a source of positivity and happiness during my struggles.

A special thanks to Harpreet Kaur and Preeti Mann, who have taught me numerous things that I'll remember for my whole life. I'd also like to thank Bhavya, Tyagi, Suri, and many others for making my life at IISER a memorable journey.

And finally, I'd also like to extend my thanks and appreciation to IISER Mohali and DST for enabling me to pursue my passion for the sciences.

Nimrat Kaur

Contents

Declaration v

Acknowledgements vii

Abstract xi

1 Introduction 1

2 Background 3

2.1 Protocols . . . 3

2.2 Channels . . . 4

3 Satellite quantum key distribution 7

3.1 Space to ground QKD . . . 7

3.1.1 Satellite to ground decoy state QKD . . . 8

3.1.2 Key generation among involved parties . . . 10

3.1.3 Shortcomings . . . 11

4 A comprehensive study of satellite QKD 13

4.1 Important points . . . 13

5 Proposed method for satellite quantum key distribution 17

5.1 Entanglement based quantum key distribution . . . 17

5.2 Measurement device independent (MDI) QKD . . . 18

5.3 The proposal . . . 19

6 Conclusions and Future work 25

List of Figures

3.1 Motion of satellite when it passes over the ground station 9

3.2 Variation of different quantities with time a) Distance b) Sifted key rate c) Quantum bit error rate 9

3.3 Secret key generation between two parties 10

4.1 A sketch of uplink protocol 14

4.2 A sketch of downlink protocol 14

5.1 Basic outsketch of bell state measurement in MDI-QKD 19

5.2 Overview of the proposed method 20

Abstract

Quantum key distribution (QKD) is the result of the need of a more secure communication channel as compared to a classical channel. It is a quantum alternative to classical cryptography, and is inherently secure and ideally unhackable. It became widely popular in the quantum world after the protocol given in the 1984 paper by Charles Bennett and Gilles Brassard(BB84 protocol), followed by a series of different protocols designed by scientists from all around the globe.

While the security of QKD is unmatched, but the distance over which QKD can be achieved is very small as compared to classical communication. It is because the photons used for QKD are diminished very easily due to atmospheric turbulence over large distances. The quantum signals can't be amplified noiselessly like classical signals owing to the quantum no-cloning theorem, which posed a difficulty to the applicability of QKD over large distances.

To overcome the short range problem of QKD, satellite QKD was suggested, as the actual atmospheric distance that the the photons would then have to travel would be equal to earth's atmosphere, which is easily achievable. So satellite quantum key distribution becomes the only viable method to actually achieve a global quantum communication.

Chapter 1

Introduction

Quantum cryptography is the science of using quantum mechanics to perform cryptographic tasks. It uses intrinsic properties of quantum particles to develop unbreakable cryptosystems. Security of cryptosystems is attributed to secret keys, which consist of randomly chosen large string of bits. The best known example of quantum cryptography is Quantum key distribution (QKD) - an information-theoretically secure solution to the key exchange problem.

Quantum key distribution is a secure communication method to produce a shared random secret key between two parties. It lets users to know if there is an eavesdropper, owing to the fact that measurements disturb quantum states, making the interception of data by any third party detectable. It has an information-theoretic security, which is its practical advantage over public key distribution that relies on computational difficulty of some mathematical functions for security.

The process of quantum key distribution includes raw key exchange where legitimate users exchange quantum states along a quantum channel to share information to generate a key. Key sifting comes after raw key exchange where the two parties reconcile their basis to determine which qubits can be used for key generation. The last part is key distillation in which the parties conduct error correction, privacy amplification and authentication to finally obtain a usable key of a considerable size.

There are a lot of protocols that have been devised over time to perform quantum key distribution, but the ones which are used more often are a few, such as BB84 [NC11],

E91 [NC11], and decoy state protocols [LMC05]. Security of BB84 protocol has been proved a number of times [SP00]. But today, by making use of decoy state protocols, scientists have managed to achieve secure quantum key distribution even if there are no perfect source of photons or measurement devices, which otherwise would have lead to unsecure quantum communication.

On ground, quantum key distribution is limited to a few hundred kilometer due to inability of photons to travel to long distances without diminishing, and owing to the fact that it is impossible to amplify quantum signals [WZ09]. So, to achieve a global quantum network, there is a need for longer quantum key distribution links. To achieve quantum key distribution on such a scale, satellite to ground links become important.

We try to work on this aspect of quantum key distribution, as we try to find a protocol that will allow us to obtain a reasonable length of quantum key between stations separated by thousands of km on earth, within a short time period. We work on the models that have already been employed by other countries and try to develop our own model, while overcoming the visible challenges of atmospheric attenuation, signal diminishing, and cost-effectiveness.

Chapter 2

Background

In this chapter, we talk about the background required to discuss quantum key distribution in context of quantum information.

2.1 Protocols

Quantum key distribution makes use of individual quanta of light in quantum superposition state as information carriers. The security of QKD comes from the aspect of quantum mechanics that measuring a quantum signal would disturb its original state and the signal would collapse to an irreversible state. So the presence of a third party is detectable and thus makes the quantum communication more secure than classical communication where there is no way to find about the presence of eavesdroppers.

There are two types of protocols that have been proposed for quantum key distribution:

1. **Prepare and measure protocols:** Measurement is an integral part of the quantum key distribution protocols. These protocols include the preparation of quantum signals by one of the involved parties. The remaining involved party then measure these signals to finally obtain a shared secret key among themselves. An example of such a protocol is BB84 protocol given by Bennett and Brassard in 1984 [BB20].

2. **Entanglement based protocols:** In these type of protocols, an entangled pair of

photons is prepared by one of the involved parties, or by a third party. One photon of the pair stays with the first involved party and the other one goes to the second party. E91 protocol is an entanglement based protocol that was given by Arthur Ekert in 1991 [Eke91].

QKD can also be divided as discrete variable QKD and continuous variable QKD. We have worked with discrete variable QKD as a part of this thesis.

Discrete variable BB84 protocol is one of the most used protocol for generating quantum keys. However there are still many loopholes that can be exploited because of inavailability of ideal single photos sources and detectors. Eavesdroppers can take this opportunity to intercept important information without getting detected.
To overcome this problem, scientists have developed decoy-state protocols which can improve the security of quantum communication. By using different decoy states, we can find out if a third party is trying to intercept some information by exploiting the loopholes of the system.

2.2 Channels

There are different channels that can be used for generating keys for quantum communication. Here we'll classify them as traditional channels and recent channels.

- **Traditional channels:**
  - Optical fibres are the most commonly used channel for travelling of signals. However, for quantum signals, such as photons, optical fibres are not preferred for long distance QKD. Since the quantum signals cannot be amplified noiselessly owing to the quantum no-cloning theorem, there is high channel loss in this channel of information transfer and thus very low coverage area.
  - Another commonly used channel for signal transfer is terrestrial free space. However, this channel also faces same challenges as that of optical fibres in

case of quantum signals, and thus is not a preferred channel because of high channel loss and low coverage area.

Quantum key distribution through these channels is limited to a few hundred kilometre because of high noise and inability of amplification of quantum signals. In theory, quantum repeaters can help increase the range of QKD by combining entanglement swapping, entanglement purification, and quantum memory, but in practice, it is far from real. With the current technology, quantum repeaters cannot be used to increase the range of QKD.

- **Recent channels:** A very recent channel for QKD is a link between space and ground. Since the only atmosphere that the signal would have to pass through when going from earth to space or vice-versa is limited to the atmospheric thickness of earth, such a channel is actually very suitable to perform QKD over large distance. Such a channel leads to less channel loss and more coverage area.

We can make the best use of space to ground links with the help of satellites. Satellite to ground links have actually made it possible to achieve quantum key distribution on very large distances [LCL+17]. Thus global quantum communication is achievable through links involving space and satellites rather than ground channels such as optical fibres.

Chapter 3

Satellite quantum key distribution

In this chapter, we'll talk about satellite quantum key distribution in detail. In particular, we'll go through the achievements that scientists have managed to achieve by sending a quantum satellite in space, and how this has changed the way how we look at the global quantum communication.

3.1 Space to ground QKD

Ever since the introduction of quantum key distribution in place of public key distribution for a more secure communication, a lot of advancement has been made in the field of quantum communication. In the past couple of years, the range of QKD has increased from only a few cm to hundreds of km. However, this still doesn't fulfil the requirement for a global quantum communication. While the channels such as optical fibres and terrestrial free space allow QKD up to some hundreds of km, QKD on a global scale can only be achieved through links involving space, as the atmospheric turbulence would decrease by a great amount in such a link as compared to any ground links.

China is the first country that has successfully managed to achieve great results, by launching its quantum satellite Micius. Equipped with three payloads, the following have been achieved by the Chinese satellite:

- Satellite to ground decoy state QKD

- Satellite to ground entanglement distribution
- Ground to satellite quantum teleportation [RXY+17]

3.1.1 Satellite to ground decoy state QKD

Micius is a low earth orbit satellite, that orbits the earth at an altitude of around 500 km in a sun-synchronous orbit. It goes over the particular locations on particular time every day, its orbit set in such a way that it passes over the locations of interest during night time. By facilitating this, the background noise during the process of quantum key distribution decreases greatly as there is no stray light to disturb the process.

This satellite has employed decoy state BB84 protocol, and uses weak coherent pulses to avert PNS attacks. In the absence of decoy state method, eavesdroppers take advantage of the fact that most of the single photon sources available are not ideal and end up sending multiple photons instead of single photons. Thus they can launch photon number splitting (PNS) attacks, and can intercept the information without getting detected. Micius uses 3-intensity decoy state protocol, with its decoy states being a high intensity pulse, a moderate intensity pulse, and a zero-intensity (vacuum) pulse [LCL+17].

Signal and decoy pulses are generated by various combination of eight laser sources that are there in the satellite payload, and are then later encoded by using a BB84 encoding module. These encoded signals are then sent to earth, and are decoded by BB84 decoding modules employed on the ground stations.

The satellite passes over the ground station where it wants to send the signal at night time to avoid the background noise. The satellite gets locked to the ground station when the elevation angle of satellite to ground is $\sim 15^{\circ}$, on both ascent and descent. It is only between these angles that the satellite can send the information good enough to be used to generate a key. The satellite stays locked to the ground station for a time period of about 5 minutes only as it is unable to send more useful signals due to larger distance and more atmospheric thickness.

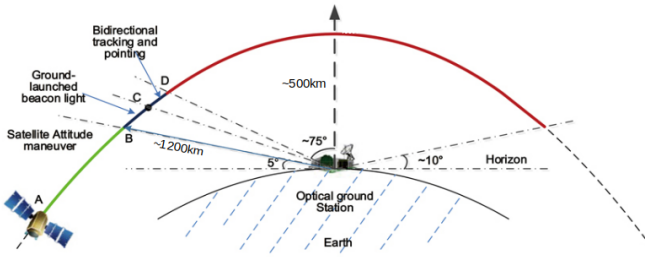

Figure 3.1: Motion of satellite when it passes over the ground station

A key is generated after privacy amplification and key sifting. These processes are done through classical channels, and the speed of these classical channels for uplink is $\sim$ 1 Mbps, and for downlink, it is $\sim$ 4 Mbps. Only after these processes of privacy amplification and key sifting, a shared usable key is generated between the satellite and the ground station. The key that is generated leads to the link speed of $\sim$ 12 kbps at $\sim$ 500 km, and $\sim$ 1 kbps at $\sim$ 1200 km, both calculated for a downlink channel.

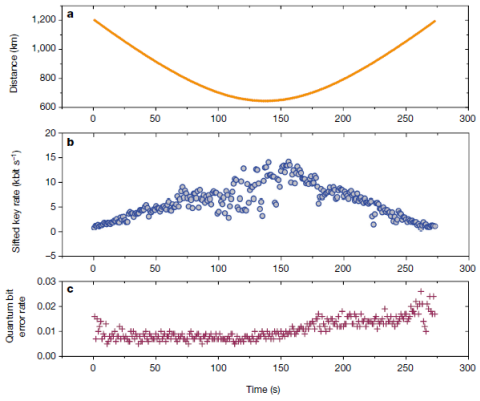

Figure 3.2: Variation of different quantities with time a) Distance b) Sifted key rate c) Quantum bit error rate

If we were to compare the key rate obtained by this space to ground link with an hypothetical optical fibre link of the same length, the key rate for the former is 20 orders of magnitude higher than the latter. It only shows the importance of such links while devising a global quantum communication network, and quantum internet.

3.1.2 Key generation among involved parties

Once the satellite has performed a successful key generation (key k_1) with one of the involved parties, it then flies over to the ground station of the second party. The advantage of being in a sun-synchronous orbit is that the satellite orbits the earth in such a way that it reaches the second ground station during night time again, which reduces the noise parameter. The same procedure is followed again, and the satellite generates a shared key with the second ground station (key k_2).

Once the satellite has generated two separate keys with two ground stations, it then announces the result of an EXCLUSIVE OR operation on the keys to one of the ground station. Since each ground station is aware of its own secret key, then the ground station which has received the results from the satellite can easily decode the key of the other ground station by performing a bitwise addition of the announced result and its own key. In this way, the two ground stations finally manage to achieve a single secret shared key, without actually having to announce any of the key publicly. Thus the chances of an eavesdropper intercepting the secret key would be decreased significantly.
The satellite announces

$$k_1 \oplus k_2$$

Let's say the second ground station receives the announced results, then it performs the

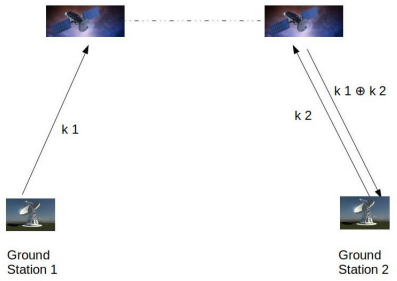

Figure 3.3: Secret key generation between two parties

operation

$$k_1 \oplus k_2 \oplus k_2 = k_1$$

Now, since both the ground stations have access to k_1, they can use key k_1 as their secret key for encoding the information.

3.1.3 Shortcomings

Even though the results that this satellite Micius has achieved are worth celebrating, there are still some shortcomings that have a room for improvement.

- A major shortcoming of this satellite is that it spends very little time in the range of each ground station. In return, this reduces the key generation rate.
- Because of the orbit being a low earth orbit (LEO), the coverage area of this satellite is very small, which again leads to small key generation rate.
- Farther the two parties are located, the more time it will take the satellite to cover the two parties, and the key generation rate will decrease as a consequence.
- Another unavoidable problem that this method faces is that there is a need to trust the satellite. If the eavesdropper gains access to the satellite, which is a key part of this satellite to ground quantum key distribution, the whole system will collapse. The keys as well as the information that is encoded will fall in the hands of the eavesdropper without any opportunity of detecting the eavesdropper.

While the last problem is something that is unavoidable with the current technology, we have made efforts to improve the first three shortcomings as a part of this thesis work.

Chapter 4

A comprehensive study of satellite QKD

In this chapter, we have explained about all the important points that will help in devising a more efficient satellite to ground quantum key distribution. After understanding these points properly, we'll be able to suggest a more efficient satellite to ground quantum key distribution method.

4.1 Important points

Before we try to devise a method to overcome the existing problems in satellite quantum key distribution achieved by Chinese quantum satellite Micius, we have listed here the most important points that need to be understood properly to devise a more efficient method [LCL+17].

- For an effective long distance space to ground link, we need to ensure a high signal to noise ratio (SNR). To achieve a high SNR, we can either increase the signal value, or decrease the noise value. But the signal that we require for a secure communication needs to be comprised of single photons. Since ideal single photon sources are not available, we have to use weak coherent pulses of particular intensity such that they correspond to single photons. However, if we try to increase the signal value indefinitely, the signal will no longer satisfy the condition of single photon intensity, and thus the link would no longer be secure. So, to increase SNR, we need to work on decreasing the noise factor as much as we can.

- The most significant way to decrease the noise of a space to ground link is to use a downlink protocol. That means the link should be from the satellite to ground and not from ground to the satellite, which would be called an uplink. In an uplink, the

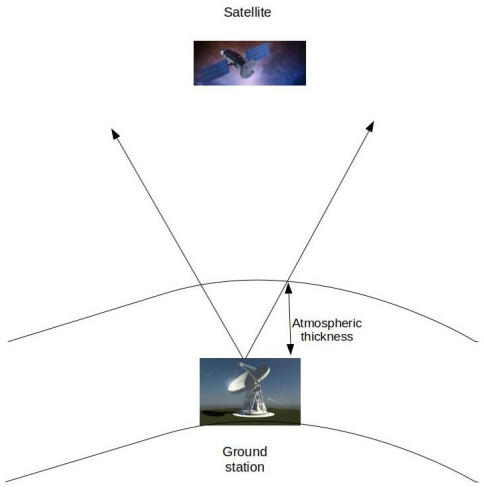

Figure 4.1: A sketch of uplink protocol

signal passes through the atmospheric thickness at the very starting of its path, and thus the beam diffraction and beam wandering is very high even if the atmospheric thickness is not more than 15 km. Thus by the time the signal reaches the satellite, it is barely usable for key generation, and thus the key rate is very small.
However, in case of a downlink protocol, the signal is sent from the space to the

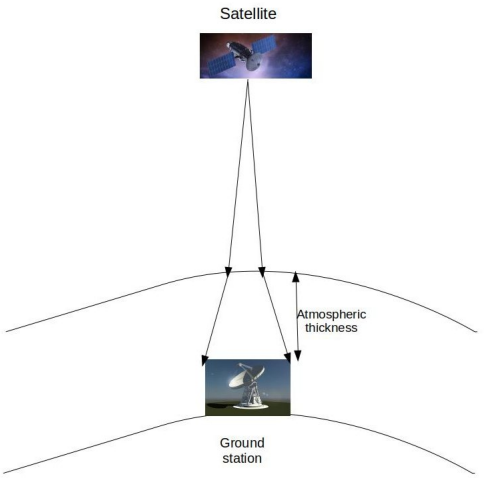

Figure 4.2: A sketch of downlink protocol

ground, and by the time it enters the earth's atmosphere, it has already covered most of its path, and the beam wandering and beam diffraction only occurs at the end of the signal path. Most of the signal travels without or little noise as it passes through vacuum, and the noise factor for a downlink protocol is far lesser than that of the uplink protocol. Ultimately, most of the signal is usable and the key rate is much more when compared to an uplink protocol.

- As the signal is sent from the satellite and reaches the ground station, light from other sources, such as sun, interferes with the signal, and it becomes increasingly difficult to identify the original signal. The noise factor in the signal increases sharply and thus such a signal cannot be used for key generation purpose. However, to overcome this difficulty, spectral and temporal filtering of the signal is very important. If we know the original frequency of the weak coherent pulses that are used as the signal, we can perform temporal filtering on the incoming signal to separate the signal of the desired frequency and to remove the undesired frequencies. Similarly, we also know the original wavelength of the weak coherent pulses, and thus we can make use of spectral filtering to filter out the background noise that is of different wavelength than the signal. Only the original signal with that particular wavelength would pass through the filter.

  Thus by performing spectral and temporal filtering of the incoming signal, we can reduce the noise factor by a great degree.

- As the weak coherent laser pulses leave the satellite and travel towards the ground station, there is beam diffraction as the path that needs to be covered is very large. By the time the signal reaches the ground, it spreads over a large distance and provides less information that can be used for key generation, thus decreasing the key rate. So we need to decrease the beam diffraction as much as possible. To decrease the beam diffraction, we can try to decrease the aperture size of the satellite telescope that sends the signal towards the ground station. This will lead to overall smaller diffraction. To capture most of the signal that arrives on earth after beam diffraction, a higher aperture telescope would lead to better results, as not much information would not be lost even after beam diffraction.

- The relative motion of the fast moving satellite and ground station needs to be taken into account, as this causes beam wandering. If it is not considered, most of the information would be lost due to beam wandering. Beam wandering mostly occurs at the origin of the signal, and even a little bit of disorientation at the starting would lead to very poor results in terms of the key generation. But if we properly consider the motion of satellite with respect to the ground, we can decrease the extent of beam wandering, and increase the key generation rate.

- To establish a stable link to send the information from the satellite to ground, the precision with which the satellite points towards the ground station should be very high. A high-bandwidth and high-precision pointing and tracking system would help us in decreasing the noise factor in the signal to noise ratio, where the tracking system helps us track the signal that is being sent from the satellite to ground. As long as we are able to design a model for which loss due to the pointing and tracking error is lesser than the atmospheric loss, the model should be considered successful in this aspect.

Chapter 5

Proposed method for satellite quantum key distribution

In this chapter, we will propose a method for successful satellite to ground quantum key distribution. We will take reference from Chinese satellite Micius and how it managed to perform QKD using entangled photons, and we will try to incorporate our own method to make improvements to the existing method and increase the range of quantum key distribution.

5.1 Entanglement based quantum key distribution

As Jian-Wei Pan et al. discuss in their paper [YCL+17b], the basic concept of entanglement based QKD is that one photon from a pair of entangled pair of photons is distributed to the two parties among which we need to distribute the quantum key. It could be either that one of the parties prepare an entangled pair of photons and send one photon to the other party. Or it could be that a third party prepares an entangled pair of photons and distribute one to each party. In the latter case, there is no need to worry about trusting the third party. Even if the third party was the eavesdropper, he/she would not be able to gain any information about the secret key. It is because, secret key generation in this case depends on the fact that the involved parties only need to announce their bases in which they made the measurements and not the results. So no matter who prepares the entangled pair of photons, the two parties only need to reconcile their bases and need to

use information corresponding to the same measurement bases. Since no information can be intercepted from the measurement bases, the method is secure.

According to the previous research, entanglement based QKD is more robust against atmospheric attenuation and can tolerate higher channel loss as compared to coherent-state QKD. We'll be able to get better results if we use entanglement based QKD for satellite quantum key distribution. Even though the distance is limited to a few hundred km for channels like optical fibres and terrestrial free space, but this is not the case for space to ground links where the effective atmospheric thickness is not more than 15 km. So we have tried to make use of entanglement based satellite to ground key distribution to overcome the problems faced by decoy state BB84 protocol used by Micius to perform large scale QKD.

5.2 Measurement device independent (MDI) QKD

As the name suggests, measurement device independent quantum key distribution is the method which lets us perform secure QKD even with not so perfect detectors or measurement devices. Eavesdroppers have often launched detector side channel attacks by taking advantage of the imperfections of the single photon sources and detectors. However, by making use of measurement device independent QKD, we can remove the threat originating due to imperfect measurement devices.

MDI QKD [LCQ12] makes use of Bell state measurements (BSM) to project the incoming photons in an entangled state. Let's say that there are two parties, and each party has an entangled pair of photons. For MDI-QKD, both the parties would send one photon from their entangled pair to a third party. Now this third party could be an eavesdropper herself, it does not affect the security of the system. This third party would perform bell state measurements on the incoming photons, and would announce the bases of the measurements. Because of the bell state measurements, the incoming photons are projected into one of the four Bell states. Because of this, the remaining photon of the entangled

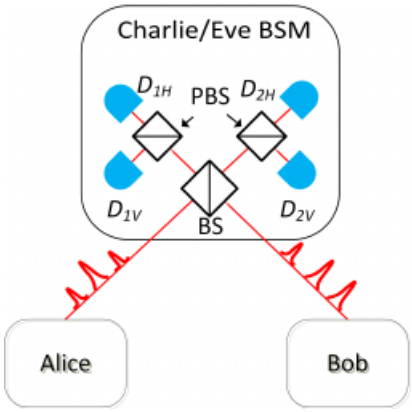

Figure 5.1: Basic outsketch of bell state measurement in MDI-QKD

photon pair of each party also collapses to the corresponding bell state. So in this way, because of entanglement swapping, the remaining photons of both parties get entangled amongst themselves. By using the announced bases by the third party as their measurement bases, both the parties would be able to generate a shared random secret key.

5.3 The proposal

What we plan to do is to combine entanglement based QKD with the MDI-QKD, and try to understand how this works out for satellite quantum key distribution. According to the points discussed in the last chapter, we will keep in mind the following things before making the proposal:

- The orbit of the satellite should be a sun synchronous orbit, and the satellite should be put into orbit in such a way that it will pass over the required locations at night time to avoid background noise caused by day light.
- It is best to propose a protocol that makes use of downlinks rather than uplinks to reduce noise and increase key rate.

Keeping in mind these points, we have prepared an outline for the entanglement based satellite quantum key distribution involving MDI-QKD.

We propose a two satellite-three ground station system, where the satellites are equipped with entangled photons source. There are three ground stations, and two out of three are

the ones among which we need to generate a secret key. The third one is the middle ground station, which is included to increase the range of the satellite quantum key distribution. We can keep adding more satellites and ground stations to increase the range of quantum key distribution, however that would lead to more expensive operations.

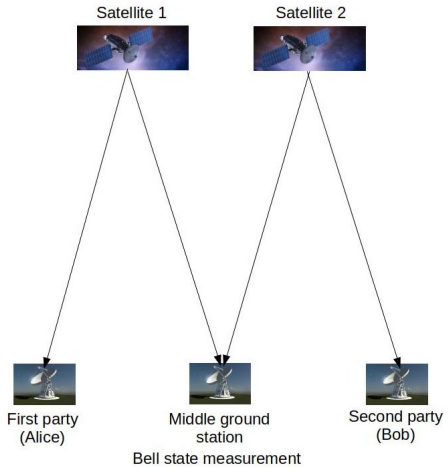

Figure 5.2: Overview of the proposed method

Both the satellites would prepare entangled pair of photons and send one pair to one of the involved parties, and the other to the middle ground station. The middle ground station would then perform the bell state measurements on the incoming photons and announce the results. When the middle ground station performs bell state measurements to project the incoming photons to a bell state, the remaining photons of each entangled pair also collapse to the corresponding bell state. By doing so, the photons that were sent to the main parties now become entangled amongst themselves, a process known as entanglement swapping. By performing measurements on them in the bases announced by the middle ground station, both parties can then generate a random secret key among themselves.

Now we'll try to explain all the important points that will help us in explaining this method in detail:
Scientists around the globe have already made very compact entangled photon sources,

and some of them have passed all the tests and are approved to be sent into space. So we might not need a special quantum satellite for this purpose, as it is technologically possible to mount these entangled photon sources on normal satellites that are already orbiting the earth, which will reduce the cost as compared to preparing a completely new quantum satellite equipped with entangled photon sources. What we need to make sure is that the source of these entangled photons is robust against various conditions in space such as temperature and vibrations. We'll have to make use of two telescopes in each satellite, as the satellite needs to send signals in two directions. Bidirectional entanglement distribution has already been proved where there are two downlinks that send entangled photons to two location on earth separated by 1200 km [YCL$^+$17a]. Telescopes with small aperture would be able to reduce the beam diffraction and thus increase the efficiency of the satellite to ground links. Previously, satellite telescopes with apertures of 300 mm and 180 mm have been used, which can be reduced further in future. Ground stations also need to be equipped with telescopes to receive the signal coming from the satellites, and thus should have large diameters to capture most of the signal.

When the entangled photon source prepares two entangled photons, it sends these photons through single mode fibres (SMFs) to transmitters, and then these photons are transmitted to the ground stations with the telescopes. One photon is sent to the first ground station (say Alice), and the second to the middle ground station. At the same time, second satellite has also prepared two entangled photons and sent them to the second party (say Bob) and the middle ground station. There are two assumptions that we make here:

1. We need to assume that we have access to at least some quantum memory, so that Alice and Bob can store their photons for some time when the middle ground station is performing the measurements.

2. The second assumption is that the satellites are trusted. In theory, we assume that the entangled state that the satellite prepares is a pure state, so there is no need to worry. However, practically we need to ensure the reliability of the satellite.

Let's assume that these satellites prepare the bell states of the form $|\Psi\rangle_{12} = (|H\rangle_1|V\rangle_2 \pm |V\rangle_1|H\rangle_2)/\sqrt{2}$, where $|H\rangle$ and $|V\rangle$ represent horizontal and vertical polarization states,

respectively. If the satellite is a low earth orbit satellite, each photon travels a distance of about 600 to 1000 km before reaching the ground station, and various factors account to channel loss. These factors include beam diffraction, optical loss, pointing error, and atmospheric attenuation, however not limited to these.

To increase the link efficiency, we need to equip our satellite and ground stations with high bandwidth and high precision APT systems, that is acquiring, pointing, and tracking systems. Another factor that we need to keep in check is the optical efficiency of the telescopes that we use. Micius has achieved an optical efficiency of 45 to 55% for its telescopes. The link efficiency and the key generation rate would increase further if we are able to increase this efficiency.

Relative motion of satellite and ground stations induces some shifts in the photons reaching the ground station, so we need to work on that to restore the polarization of photons. According to our proposed method, we need to work on the photons reaching the middle ground station first by making use of different wave plates. Some sort of time stamp, to indicate the time when the photons left the satellites helps to identify the photon pairs. In a previous work, it has been proved that even after traveling for such long distance, almost 2000 km when the link length of two downlinks is added, the photons still retain their entanglement. Calculating the loss due to all the factors such as beam diffraction, optical loss, stray light, pointing error, absorption, and atmospheric turbulence, overall channel loss comes out to be around 29 dB at 530 km and around 44 dB at 1600 km for two downlinks. Since our method incorporates four downlinks at the same time, our channel loss would not be more than 100 dB even after travelling 3200 km in total. If we compare it to the other channel losses, such as optical fibres(channel loss 0.16 dB/km), it turns out to be more than five time lesser than them.

When the middle ground station performs bell state measurements (BSMs), the incoming photons from both the satellites get projected into one of the following four states:

$$|\Psi^{\pm}\rangle = (|H\rangle|V\rangle \pm |V\rangle|H\rangle)/\sqrt{2}$$

$$|\Phi^{\pm}\rangle = (|H\rangle|H\rangle \pm |V\rangle|V\rangle)/\sqrt{2}$$

Although, the original setup could only identify the first two states, but that was enough to prove the security of the MDI-QKD. Now when the incoming photons collapse to one

of these states, the corresponding photons that are with Alice and Bob would also collapse to the corresponding Bell states. By doing so, the photons of Alice and Bob get entangled among themselves because of entanglement swapping. Once the measurements are performed, the middle ground station would announce the measurement results as well as the instances when it received these results. So Alice and Bob only need to keep the photons corresponding to these instances, and measure them according to the bases announced by the middle ground station. Because their photons are entangled, they'll be able to find out about the results of the other party, and thus a secret key can be generated after the required error-correction as well as post-processing.

Chapter 6

Conclusions and Future work

Even though we have made use of two satellites and three ground station for our proposal, we've done so to increase the range of the communication in a small time. We could have used just one satellite for this purpose, but that would have required quantum memory, and the time for which we need the quantum memory would be directly proportional to the distance we need to cover for the communication. Since it is not possible with the current technology, we can only incorporate two satellites in this method.
However, we can not keep on adding satellites and ground stations to increase the range, as doing so will also increase the total link length, channel loss, and thus ultimately decrease the key rate. So with this method, we can double the range of what has already been achieved, even though the speed would be a little less, but it would still be feasible.

In future, we can go deep into this method, to try to find the key rate and fidelity by running simulations and thus we can check the practicality of this method. We believe that this method would work very well if we were to use it in Indian context. The distance from the extreme north to extreme south of India is around 3300 km and that from extreme east to extreme west is around 3000 km. We can try to simulate this method in Indian context and try to find the location where we can set the middle ground station so that it can serve all of India.

Bibliography

[BB20] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[LCL+17] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, and et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, Aug 2017.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.

[RXY+17] Ji-Gang Ren, Ping Xu, Hai-Lin Yong, Liang Zhang, Sheng-Kai Liao, Juan Yin, Wei-Yue Liu, Wen-Qi Cai, Meng Yang, Li Li, and et al. Ground-to-satellite quantum teleportation. *Nature*, 549(7670):70–73, Aug 2017.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[WZ09] William K Wootters and Wojciech H Zurek. The no-cloning theorem. *Physics Today*, 62(2):76–77, 2009.

[YCL+17a] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Guang-Bing Li, Qi-Ming Lu, Yun-Hong Gong, Yu Xu, Shuang-Lin Li, Feng-Zhi Li, Ya-Yun Yin, Zi-Qing Jiang, Ming Li, Jian-Jun Jia, Ge Ren, Dong He, Yi-Lin Zhou, Xiao-Xiang Zhang, Na Wang, Xiang Chang, Zhen-Cai Zhu, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[YCL+17b] Juan Yin, Yuan Cao, Yu-Huai Li, Ji-Gang Ren, Sheng-Kai Liao, Liang Zhang, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, Ming Li, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Rong Shu, Cheng-Zhi Peng, Jian-Yu Wang, and Jian-Wei Pan. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119:200501, Nov 2017.