Department of Physics
UNIVERSITY OF STRATHCLYDE

MSC ADVANCED PHYSICS
PH952: PROJECT

Key rate modelling and analysis for Satellite Quantum Key Distribution using BBM92 protocol

Ayush Goyal
Registration No. 202090456

Supervisor
Dr. Daniel Oi

2021

Abstract

Satellite Quantum key distribution methods have been investigated for their dependency on the factors that influence the creation of a secret key that can used for encryption. A new model was created and validated, that allows a user to determine the optimum satellite path and the apparatus to be used in a satellite-based QKD link. It was found that diffractive losses, atmospheric losses and hardware efficiency define a fundamental trade space that drives orbit, wavelength and hardware selection (optimum orbit is one that generates the highest detection rates). Our model was created using entangled based BBM92 protocol where creation of a secret key by using two simultaneous beams in the dual downlink configuration to analyse their losses for a 500 km Sun-synchronous orbit and validated by comparison to the experiments performed with the Micius satellite.

We prepare a model for the dependency of the key rate that can be generated on the relative orbital parameters of a quantum satellite. and verifying our model with taking into consideration all other parameters which are checked by incorporating them in the SPG4 algorithm for comparison with the actual motion of the Micius satellite. Our model can easily be extended to improve other characteristics of the QKD experiment for generating an optimal practical key.

Acknowledgements

I owe a great debt of gratitude to my supervisor Dr. Daniel Oi for giving me the chance to work with him. This report could not have been completed without his continuous support, guidance and patience. I have learned a great deal as he was always there offering guidance and thoughtful training. I would also like to thank him for putting up with my endless questions and am confident he will move the research forward and be succesful.

Contents

List of Figures

Chapter 1

Introduction

1.1 General Issue

While sharing sensitive data over a network, the security of the data is essential, and to accomplish that, a set of rules are imposed on the information and communications (encryption) thus creating a sharable cryptographic key to encrypt and decrypt data. While classical keys have been used till now for cryptography purposes, its use is limited as an eavesdropper can get hold of the key, which paves way for production of quantum cryptograpic keys which do not exist in physical state until they are measured and no-cloning theorem prevents from the duplication of quantum bits. This unconditional security has motivated the development of real-world systems but distance limits these real-world terrestrial systems due to losses in optical fibres. Thus, a transition to free-space QKD takes place which is also limited in distance if done terrestrially, eventuallsy paving way for free-space systems including satellites (Satellite QKD) as the next evolutionary step to extend the range of practical QKD, as the losses concerned in considerably less due to most of the transmission in space. This gives rise to a need of a validated model that accurately characterizes the orbital dynamics and the space-based optical path to produce a practical secure key that can be used for cyptography purposes.

1.2 Problem Statement

There is a need to develop the relationship of the essential factors that influence QKD secret key rates in a space-based link. The optical path needs to be characterized and the effects of the atmospheric and hardware

losses taken into account. The significance of each factor is necessary to identify the parameters that can be changed for optimization of a design setup for a satellited based QKD experiment. We create our model on the dependence of the key rate on the relative orbital parameters of the satellite.

1.3 Research Objectives/Questions/Hypotheses

The main investigations include:

- What factors influence the QKD key rate?
- What is the significance of these factors and how they depend on the orbit of the satellite?
- How do atmosphere losses affect the key rate?
- How does the protocol used influence the QKD security and key rate?
- Is violatation of Bell inequality a sufficient condition for the protocol?
- How do hardware losses, i.e. detector efficiencies, dark counts, etc., influence the key rate?
- After obtaining the QBER and raw key rate, how can you calculate secret key length and is it a secure communication?

1.4 Research Focus

This research focuses on the factors that influence satellite QKD detection rates and then develop a model to check their significance for obtaining a secure key in a dual downlink configuration. The model gives a brief understanding about the dependency of the optical path on the orbital dynamics of the satellite with respect to the optical ground stations that receive the quantum bits. Moreover, it focusses on the admospheric and harware losses that create the Quantum bit error rate which directly affects the secret key length obtained. Therfore, our model predicts an optimal orbit that ensures the greatest amount of raw key material is exchanged at both the ground stations and the optimal hardware components that then result in the best outcome for the secret key length. It is noteworthy that we focus on the BBM92 protocol in this research for production of secure keys.

1.5 Methodology

This report first identifies and presents the factors that influence satellite QKD and then according to their significance, these are incorporated into our model. Also, our model evolves from a simple model with realization of the factors responsible to a realistic model that can be used for practical generation of a secure key. Finally, our model is compared with the experimental realization of the Micius satellite and validated for the key generated. The model first develops the positions of the satellite and the ground stations and focuses on the optical path of the qubits according to their relative positions. Then it takes the free space diffraction losses and atmospheric effects into consideration and calculates QBER and key rate, by including detector efficiencies and dark count rate. Lastly, we compare the model using SGP4 algorithm to get the trajectory of the Micius satellite and take Earth parameters into account for a more realistic model to validate the factors that we have incorporated in our model. Finally, we compare our model results with the experimental results and validate our model for the creation of secret key length that can be used for cryptography.

1.6 Assumptions/Limitations

Here we focus on all the assumptions made in this report. The main assumptions that we undertook are equivalent detector efficiencies, atmospheric reciprocity up to 100 km and that the influencial factors do not change with time. We model the satellite QKD system for a 500 km low-earth orbit(LEO) sun-synchronous satellite as a satellite offers a better way for quantum key distribution but if the orbit of the satellite is too big, there are very large losses due to diffraction. Moreover, we assume a constant orbit for the satellite therby not taking phase change into account. Additionally, we produce the secret key length using the asymptotic secret key rate and do not find the true secret key length. Moreover, although we mention weather effects in our model, we do not take the weather effects into account in our calculations and realize that they can cause excessive attenuation of the optical beam. We assumed the properties for atmospheric attenuation are represented by point to point optical path and thus does not change for uplink or downlink configuration. We also assume negligible pointing errors therby line of sight approximation for the ground station telescopes.

Chapter 2

Background

2.1 Quantum key Distribution

2.1.1 Overview

Quantum key distribution refers to the special form of key generation and transmission where the laws of quantum physics are used to produce a secure key. Here photons with particular properties (like polarization) are transmitted to the receiver carrying quantum information that can be only decoded when the measurement is made. Then, a unique key is produced from the measured results which can be used to encrypt the data being shared on a public channel. Moreover, according to no-cloning theorem, it is improbable for an eavesdropper to gain enough information about the secure key without interfering with the results of the quantum communication. Using quantum communication, we transmit photons that have specific properties(polarization here) to create a unique share key such that the security of key is strong enough to create encrypted information which can be exchanged over an open channel.

2.1.2 Quantum Computations

Quantum particles for computations are represented as qubits(polarization vector here) represented as(in Dirac notation)

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

where α and β are the associated components for $|0\rangle$ and $|1\rangle$ and their squares give their respective probabilities such that $|\alpha|^2 + |\beta|^2 = 1$. These respective states are assigned a digital value for the transfer of information.

For our model, we select 2 orthogonal bases and thus choose either H/V basis(horizontal-vertical basis) or D/A basis (diagonal-antidiagonal basis) and thus their relation can be defined as

$$|D\rangle = \frac{1}{\sqrt{2}}|H\rangle + \frac{1}{\sqrt{2}}|V\rangle$$

$$|D\rangle = \frac{1}{\sqrt{2}}|H\rangle - \frac{1}{\sqrt{2}}|V\rangle$$

(We already know and can verify that the two vectors in each bases are perpendicular to each other) Therfore, we can assign digital value to each measurement and we assign 0 to $|H\rangle$ and $|D\rangle$, and 1 to $|V\rangle$ and $|A\rangle$. Now only the bits where Alice's (sender's) and Bob's (receiver's) bases are same can be stored to produce a secure key and the rest bits can be discarded. This gives rise to the traditional BB84 protocol. Since we are familiar with another interesting quantum phenomenon, i.e. quantum entanglement, we can use entanglement procedure on this method itself to obtain BBM92 protocol (also called entanglement based- BB84 protocol).

2.1.3 BBM92 protocol

1. The satellite produces polarization-entangled photon pairs in the $|\psi^-\rangle$ state.

2. The produced pairs are split up and one photon for each pair is sent to Alice and the other photon to Bob.

3. Now, Alice and Bob measure each photon in one of the two non-orthogonal complementary bases, i.e. H/V basis (horizontal = $0°$, vertical = $90°$) or D/A basis (diagonal = $+45°$, anti-diagonal = $-45°$)

4. After the measurement, Alice and Bob communicate publically over a classical channel about the basis they used for each received photon.

5. All the bits for which the basis used by both of them is same is saved and other bits are discarded, to form a secret key (their result will be exactly anti-correlated as the photons were entangled).

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |+-\rangle)$$

6. Now 10% of their measurements is used to estimate the quantum bit error rate (QBER) and the rest is used to generate a final secure key.

7. Now the CHSH inequality is tested for the particular key length and the violation indicates the presence of entanglement.

Security of BBM92 protocol

This area of interest is of particular interest as it tells us the amount of information an eavesdropper can get from our protocol and if we can securely use the secret key formed or abandon the protocol. In case of one-way protocols, researchers showedin their paper that Eve's maximal information is given by[**erven2007free**]:

$$I_{max}(A,E) = \frac{2}{ln2}e + O(e^2) \approx \frac{2}{ln2}e$$

where $I_{max}(A,E)$ is the maximum Shannon information between Alice and Eve, and e is the error rate. and Alice's and Bob's mutual information is given by:

$$I(A,B) = 1 + e\log_2(e) + (1-e)\log_2(1-e)$$

This gives us the error threshold to be the intersection of the two curves as $e \sim 14.6\%$.

Moreover, as there is entanglement involved, the violation of CHSH inequality for an imperfect quantum channel has to be studied as

$$S_{max}(e) = (1-2e)2\sqrt{2}$$

Since we know that the total secret key rate is given by

$$R = R_{sif}R_{SP}$$

where R_{sif} is the sifted key rate achieved by the experiment and R_{SP} is the Shor-Preskill bound $R_{SP} = 1 - \kappa H_2(e) - H_2(e)$ which arises from optimal error correction and privacy amplification with $H_2(e) := -e\log_2 e - (1-e)\log_2(1-e)$ being the Shannon entropy. For this value less than 50%, we obtain the threshold $e \leq 11\%$.

These two thresholds tell us if the particular generated key is secure or not.

2.2 Developments in Quantum key Distribution

The concept of quantum key distribution was born in the late 1960s when it was mentioned in "Conjugate Coding" by Stephen Wiesner and came

to fruition by one of the first quantum cryptography experiments done in 1989 [**bennett1992dawn**] where they achieved to exchange a key whose crossover frequency was 20% when weak 64516 light pulses were sent to finally create a secure key of 403-bit string over 30 cm. Four years later,[**bennett1992experimental**] the procedure was improved by the University of Geneva producing 828 bits secure key where the optical path length was 1 m using optical fiber using LEDs, proceeded by researchers in Geneva and Nyon over 23 km fiber in 1995. There were many more QKD developments over optical fibers with implementation of different protocols like BB84, B92, BBM92 etc in experimental setups and increasing the range of transmission,like in 2007, Los Alamos achieving a distance of 184.6 km with BB84 protocol at mean photon number 0.5 resulting in 13350 sifted keys with 5.3% QBER, Canara Island of La Palma transmitting entangled qubits over 144 km using Ekert protocol, and University of Cambridge achieving 1.02 Mbit/s high rate for 20 km getting $7.9x10^6$ bits with decoy BB84[**dixon2008gigahertz**]. The latest of this technology include the use of sending-or-not-sending twin field protocol to achieve 506 km distance for QKD in 2020.

It was realized pretty early that optical fibers have a limitation since bends causes birefringence leading to disturbed polarization in optical fibers, which gave rise for free-space QKD experiments, first of which done in 1992 over a $\sim 475m$ optical length with average 2% bit error rate using B92 protocol[**buttler1992point**], succeded by researchers in Clifornia in 1998 with BER of $\sim$ 1.5% for 950 m optical length and $\sim$ 0.7% for 240 m optical length[**buttler1998practical**]. Thus, reasearchers conducted free space QKD experiments and achieved realistic transmision for the first time in 1999 for 0.5 km which was eventually increased to 7 km [**hughes2000quantum**], therby paving way for achieving 12.8 bit/s with 35 dB attenuation over a distance of 144 km using BB84 protocol in 2007[**schmitt2007experimental**], and 143 km distance for entangled BBM92 protocol getting an average rate of 450 counts per second in 2020[**ecker2021strategies**].

Now, the logical evolution being spaced based transmission, experimental satellite quantum communications was investigated in 2015[**vallone2015experimental**] where they suggested violated of Bell inequalities for QKD at average QBER of 4.6% and link duration of 85 s. Moreover, different CubeSats were launched for implementing QKD experiments like SpooQy - 1 satellite[**perumangatt2021realizing**] used for demonstration of operation of an entangled photon pair source with 13.6 kbits secret key achieved for a single pass. Additionally the first independent satellite for QKD operations was launched by China in 2016. This low Earth orbit satellite called Micius with an orbit time of 94 minutes acts as a relay to distribute secure keys between multiple distance loca-

tions. It has multiple transmitters and recievers and can be used to incorporate BB84 protocol, like 100 kB secure key achieved between Xinglong and Graz, as well as entanglement based BBM92 protocol, when finite-key secret key rate of 0.12 bits per second achieved in 2019 between Delingha and Nanshan.[**yin2020entanglement**] Thus focussing on these experiments, lots of models were also developed for optimum parameters to be maintained for obtaining a secure key for cryptography purposes.

With limitations of satellite QKD for its dependence of weather conditions, an alternate method for QKD experiments has been the deloyment of high altitude technologies for increasing the range of the experiments as well as reducing losses. In 2017, researchers at Waterloo generated secure key length of upto 868 kb with $3-5\%$ error rate using a tranmitter mounted on an aeroplane with bb84 decoy-state protocol. Aso, an analysis was done in 2021 for stratospheric HAPs flying at 20 km showing promise in the field. [**pugh2017airborne**]

2.3 Modelling Satellite Dynamics

2.3.1 Overview

Our model first needs to describe the satellite dynamics, on which depends our optical path which actually gives us the secret key produced. Initially, we create a model for a spherical Earth and a circular satellite orbit and understand that the optical path of the qubits depend on the relative positions of the satellite and ground stations and not on the actual positions. Eventually, we develop the satellite dynamics using Standard General Perturbations 4 (SGP4) algorithm which defines the orbital characteristics in the Earth centered inertial coordinate frame, which can then be used to get a realistic quantum key rate.

2.3.2 SGP4

This is the algorithm that uses a position and velocity and properties of Earth to define the orbital characteristics of a satellite(Here, Micius satellite). We put in characteristics like TLE(Two-Line Element) which also incorporates perturbations in the model.[**denton2016key**]

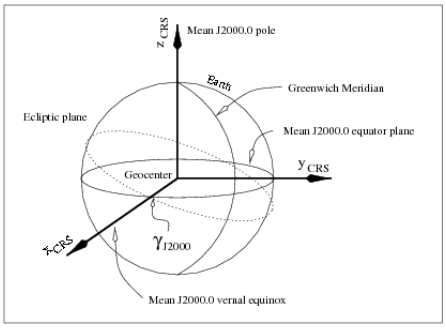

Figure 2.1: EARTH CENTERED INERTIAL FRAME OF REFERENCE

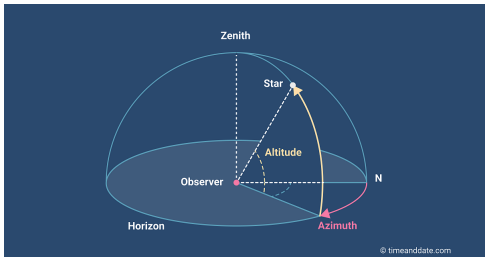

Figure 2.2: HORIZON COORDINATE SYSTEM

2.3.3 Frames of Reference

The frame of reference is an inertial Earth centered frame which is based on the plane of the equator and the pole. This frame of reference is analysed with the frame centered in the horizon coordinate system topologically, i.e. with respect to elevation angles for the ground stations. The satellite position vector is first taken into consideration by our Earth centered frame and then is correlated with the horizon corrdinate system to determine the relevant range for the optical link. The ground stations' positions are specified in the Earth centered frame and then becomes the center for our horizon coordinate system.

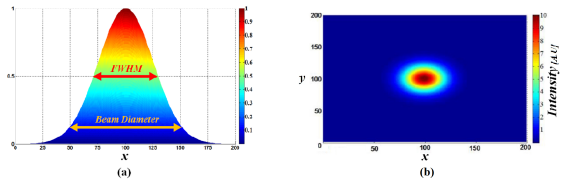

Figure 2.3: GAUSSIAN BEAM

2.4 Satellite Optical Downlinks

2.4.1 Overview

Here we describe the basic feature of an optical link between a satellite and ground stations. The optical path is the path taken by the quantum photons which behave as gaussian beams, i.e. a beam of light diffracts which is the major cause for loss of power as the beam spreads out a lot as it reaches the ground stations from a distance of 500 km. Also, the light beam makes contact with the particles in the Earth's atmosphere causing scattering which also causes loss in our channel (thus dependence of optical wavelngth used). Also, in our model, we take into the downlink path only and not uplink path, as the satellite creates entangled photons which are sent to the ground stations on the Earth.

2.4.2 Gaussian Beams

In QKD experiments, Gaussian beams can be used to transport qubits from the satellite to the ground station. These beams have a major concentration of energy in the middle of the beam and moves radially out therby decreasing the energy exponentially by the relation of the square of the radial distance.

2.4.3 Atmospheric Effects

The atmosphere directly affects the optical beam of qubits and there are losses due to all sizes of particles in the atmosphere. While the atmosphere does not affect the polarization of the beam, attenuation and scattering of the beam creates attenuation of the quantum signal and thus has to be taken into account while calculated quantum bit error rate. Moreover, the weather can create significant attenuation in the quantum signal. The level of attenuation depends on the atmospheric conditions in the optical path as

it reaches the ground stations and also on the thickness of the atmosphere, i.e. there is more attenuation at horizon compared to the zenith position of the satellite.

2.5 Relevant Research

2.5.1 Models and Experiments

QKD experiemnts using entangled based qubits or polarized qubits were demostrated throughout the years which gives promise to the emerging encyption methods using quantum physics. Bourgoin was one of the first researchers to look into this aspect and perfomed a QKD with a pick up truck and a satellite at 600 km altitude to produce key rate of 40bps with QBER of 6.5% to 8%. Then pointing, tracking and acquisition of qubit was studied using hot-air balloon (key rate 48 bps), cubesats and bigger satellites like Socrates and Oicets. Thus they overcame the range limit of ground based links as the total loss per km was effectively less, and no change in polarization. A relevant experiment can be SpooQy- 1 cubesat in 2021 which was able to produce and detect high quality entangled photons producing practical reults for entanglement based QKD(13.6 kb of secret keys for single pass, 40 dB loss).

2.5.2 Micius satellite

The launch of Micius satellite led to the major implifications of theory and experiments for QKD experiments as it is the first major quantum satellite launched in 2016 solely for quantum experiments. It is a LEO sun-synchronous satellite with a time period of about 90 minutes, that has the capacity to generate qubits at different wavelengths $(780nm, 810nm, 850nm, 1550nm)$ and transmit through two Cassegrain telescopes of apertures 300 mm and 180 mm. One of first experiments was done between Delingha, Lijiang and Nanshan ground stations where they had 1200, 1800 and 1200 mm aperture receiving telescopes respectively in 2017[**yin2017satellite**]. Entanglement based QKD was performed and average two photon count of 1.1 Hz achieved with a signal-to noise ratio of $\sim 8:1$. A similar experiment was done in 2019 between Delingha and Nanshan and secure key rate of 0.43 bits per second achieved in the asymptotic limit and finite key rate of of 0.12 bits per second produced taking failure probability thus giving them a 372-bit secret key. Also, there were many QKD experiements using BB84 protocol that resulted in final key lengths ranging from 400 kb to 833 kb. [**liao2018satellite**]

2.6 Experimental Hardware Setup

Here we discuss the influence of the hardware components on the qubits. Initially, our qubits when generated go through the losses of the transmission setup and optical losses in the telescopes that radiate the laser beam. These losses are usually minute and thus can be deemed insignificant that they can be neglected, but when the beam is received at the ground stations, the detector efficiency is the prime cause of loss and thus taken into account. Additionally, the detector carries a dark count rate where it registered counts without any incident light. This can cause error in our data and thus incorporated in our model. Also, there are losses due to detector time response with respect to the time frame of the light beam but can be ignored due to negligible effects.
Adding to this, the quantum key length depends on the probability of Alice's and Bob's measurement to be relevant and thus the probability depends on the quantum protocol procedure used(Here, entanglement based BBM92 protocol). Here, this figure describes the experimental setup of the transmitter and the receiver through where the wubits are produced and detected and thus, it picturizes the components according to which losses occur affecting our quantum key rate.

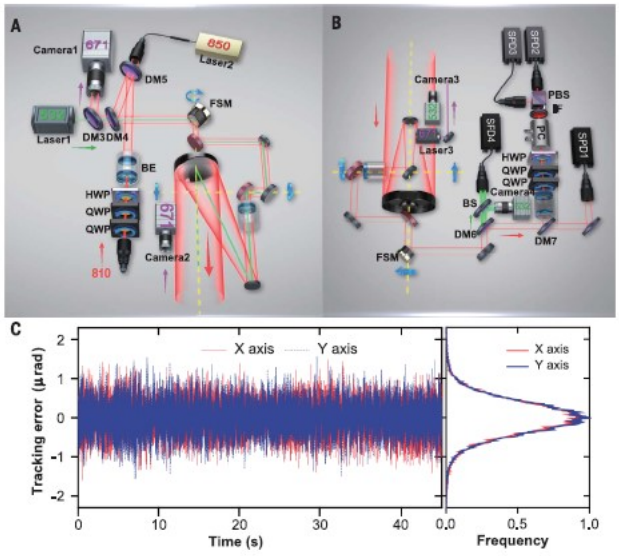

Fig. 2. The transmitters, receivers, and APT performance. (**A**) The entangled-photon beam (810 nm) is combined and co-aligned with a pulsed infrared laser (850 nm) for synchronization and a green laser (532 nm) for tracking by three DMs and sent out from an 8× telescope. For polarization compensation, two motorized QWPs and a HWP are remotely controlled. A fast steering mirror (FSM) and a two-axis turntable are used for closed-loop fine and coarse tracking, based on the 671-nm beacon laser images captured by cameras 1 and 2. BE, beam expander. (**B**) Schematic of the receiver at Delingha. The cooperating APT and polarization compensation systems are the same as those on the satellite. The tracking and synchronization lasers are separate from the signal photon and detected by single-photon detectors (SPDs). For polarization analysis along bases that are randomly switching quickly, two QWPs, a HWP, a Pockels cell (PC), and a PBS are used. BS, beam splitter; IF, interference filter. (**C**) The APT system starts tracking after the satellite reaches a 5° elevation angle. The left panel is a 50-s trace of the real-time image readout from the camera. Fine-tracking accuracy of ~0.41 μrad is achieved for both the *x* and *y* axes.

Figure 2.4: BBM92 EXPERIMENTAL SETUP WITH MICIUS EXPERIMENT[**yin2017satellite**]

Chapter 3

Methodology

3.1 Qubit Optical Path

As we are aware that the mean optical path of the quantum beam is essential to determine the quantum key, we find the range of the beam from the ground stations in our Earth centered frame.

We define the cartesian coordinates of the ground stations and the satellite and find the range by simply using

$$Range = \sqrt{(x_{ogs} - x_{sat})^2 + (y_{ogs} - y_{sat})^2 + (z_{ogs} - z_{sat})^2}$$

Now we need to incorporate the relevant range in our model which is the range where the satellite and ground station can make contact with each other and send photons. This is dependent on the elevation angle in our horizon coordinate system and thus we find the relationship between the two frames of reference. Here we plot the relevant range of the optical beam with respect to the elevation angle for both our ground stations. It is noteworthy that here the relevant range refers to the range when the satellite is in contact with both the ground stations. The relevant range and concerned time are dependent on the visibility of the satellite from the OGS and thus we find the relation between range and elevation angle which is given by:

$$R = \sqrt{R_E \sin\alpha^2 + (R_E + h)^2 - R_E^2} - R_E \sin\alpha$$

Thus,

$$R_{max} = \sqrt{R_E \sin{\alpha_{min}}^2 + (R_E + h)^2 - R_E^2} - R_E \sin\alpha_{min}$$

where α is the elevation angle for the OGS

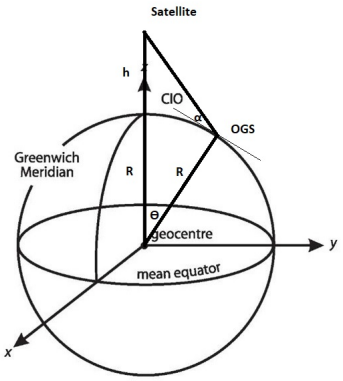

Figure 3.1: OUR MODEL INCLUDING ANGLE OF ELEVATION α AND LONGITUDE θ

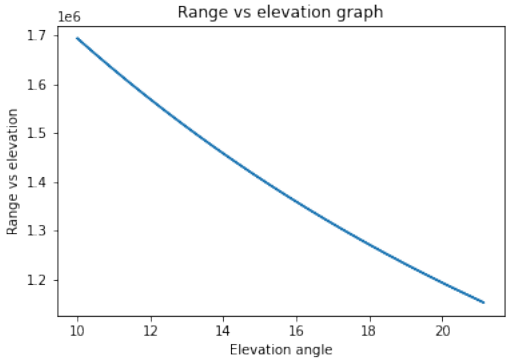

Figure 3.2: RANGE V/S ELEVATION GRAPH FOR A SINGLE OGS

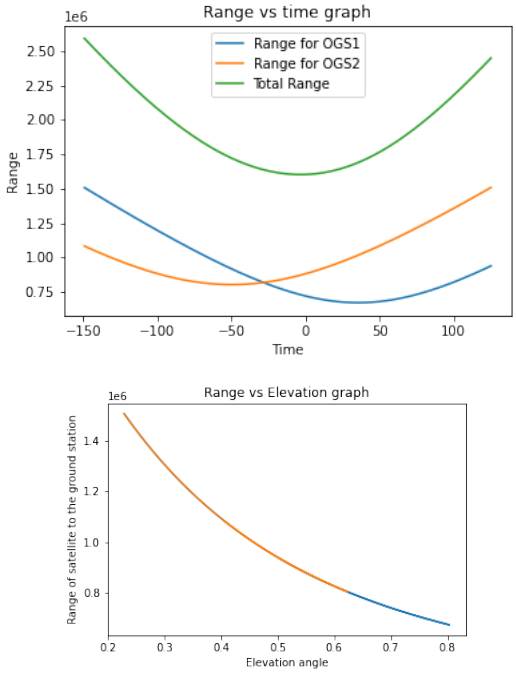

Figure 3.3: a)RANGE V/S TIME GRAPH FOR DUAL DOWNLINK CONFIGURATION FOR 2 OGSs(equidistant to the 2 OGSs and angle of intersection at 60 degree) b) RANGE V/S ELEVATION GRAPH FOR THE SAME CONFIGURATION

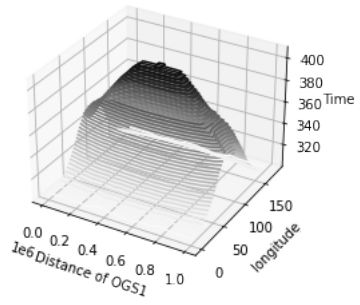

Figure 3.4: 3D PLOT OF TOTAL VISIBILITY TIME WITH RESPECT TO POSITION OF OGSs

These graphs also trace the trajectory of the motion of the satellite and gives the relevant time in which the satellite keeps in contact with the ground stations. Here, we understand that our key length is directly proportional to the amount of time the satellite keeps in contact with the two stations and thus, the motion of the satellite needs to be studied. Therfore, we make a 3d plot of the relevant time with repect to the position and direction of the great circle line joining the two ground stations.

(Note: Since we are concerned with only the optical path, we assumed a satellite at height 500 km orbiting in y-z plane and we change the positions of the OGSs)

3.2 Free space Diffraction - Dual Downlink

Now, we describe the diffraction losses and account for that in our model. As we discussed that the beam acts as a gaussian beam and thus depends on the aperture of the transmitter to determine the initial diffraction of the light beam and then depends on the range to know the spread of the beam. Thus the loss is dependent on the area of the receiver and the shadow of transmitter on Earth. Also according to Fraunhofer diffraction, we know that the angle of spread is dependent on the wavelength of light used. Considering a Gaussian beam, the beam spreads according to its surface area and is spread over an area an area of $\pi(L\theta)^2/4$. Thus, the geometric loss is dependent on the range and the apertures of the transmitter and reciever as:

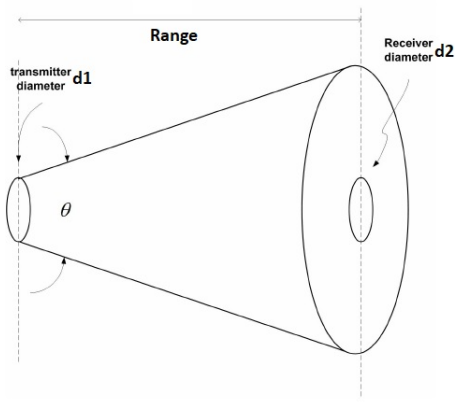

Figure 3.5: GEOMETRIC CONE FOR TRANSMITTER AND RECIEVER

$$\textbf{Geometric loss} = \frac{d_2^2}{[d_1 + (L\theta)]^2} \implies Loss \approx -20\log_{10}\frac{d2}{L\theta}[dB]$$

where d_2 is the receiver aperture and d_1 is the transmitter apperture, L is the range and θ is the diffraction airy disc angle given by $\theta = 2 * (1.22\lambda/d_1)$ given by Fraunhofer diffraction for circular aperture.[**sidhu2021key**] Here, we model the satellite moving at an angle of 60° angle from satellite motion and the movement of the satellite is from the middle of the great circle joining the two OGSs.

3.3 Atmospheric Profile and Effects

The atmospheric profile determines all the atmosphere losses in the optical beam which dependent on the wavelength of light used, the aerosol concentration, humidity concentration and turbulence effects for which we take values from other papers and create a general model. The atmosphere attenuation to the optical beam depends on the wavelength of light used and the particles it interacts with. We can formulate some basic equations for the different types of light behaviour as: Beer's law equation:atmospheric attenuation

$$\tau = exp(-\beta L)$$

where L is the range, β is the total attenuation, $\beta = \beta_{abs}\beta_{scat}$(absorption and scattering attenuation)

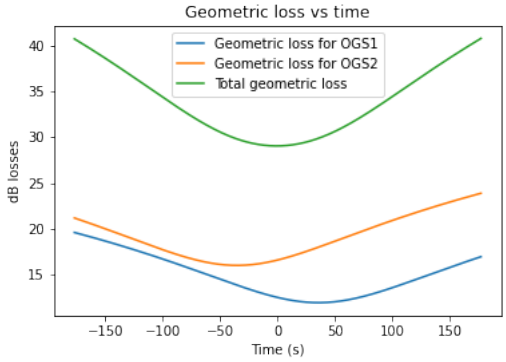

Figure 3.6: TOTAL DUAL DOWNLINK GEOMETRIC LOSS V/S TIME GRAPH

Rayleigh Scattering:

$$\alpha_m = \frac{8\pi^3(n^2-1)^2}{3N^2\lambda^4}$$

,

$$\beta_m = \alpha_m N_m$$

and

$$\beta_{abs} = \alpha_{abs} N_{abs}[\frac{1}{km}]$$

where α_{abs} is the effective cross section and N_{abs} is the concentration of the particles

We take roughly 1 dB scattering loss in our model.

Mie Scattering:

$$\beta_a = (\frac{3.91}{V})(\frac{0.55\mu}{\lambda})^i$$

where V is the visibility, i is the size distribution of scattering particles defined as
$i = 1.6$ for $V > 50km$(our case), $i = 1.3$ for $6km < V \leq 50km$, $i = 0.585V^{1/3}$ for $V < 6km$

Thus, we have roughly 1.6 dB scattering loss due to Mie scattering in our model. We can note that the visibility is dependent on the cloud cover, rain and snow losses. Thus it can drastically affect our model.

Neglecting the absorption attenuation, $\beta_{scat} = \beta_a$, the atmospheric attenuation in dB given by

$$\tau = 4.3429\beta_a L[dB]$$

For turbulence, a lot of models have been developed, one of which is the Hufnagel-Valley model given by:

$$C_n^2(h) = 0.00594(v/27)^2(10^{-5}h)^{10}exp(-\frac{h}{1000})+2.7x10^{-16}exp(-\frac{h}{1500})+A_0exp(-\frac{h}{100})$$

where h is the altitude, v is the wind speed at high altitude, A_0 is the turbulence strength at the ground level, $A_0 = 1.7x10^{-14}m^{-2/3}$ Turbulence has three main effects: scintillation, wander and beam spreading.

We would also like to mention the effects of Doppler shift for the two wavelengths used for our entangled photons. Thus the doppler shift can be calculated as:

$$\nu_a = \nu_e * \frac{(1 - \frac{v}{c}\cos\theta_{c,v})}{(1 - \frac{u}{c}\cos\theta_{c,u})}\sqrt{\frac{(1 - (\frac{u}{c})^2)}{(1 - (\frac{v}{c})^2)}}$$

We approximate these values for our entangled based model using $810nm$ light and find the doppler shift to be about $\sim 18.56GHz$ and we assume that the optical bandpass filters in our detectors can accomodate the Doppler shift therefore we infer that it would not impact the optical path.

3.4 Influence of Hardware Losses

Our model also take into account the detector efficiencies and dark count rate which directly increases our quantum bit error rate but the influence is less compared to other effects. From our study, we infer that the most optimum detectors used have blabla efficiencies and blabla dark counts which we incorporated in our model. We compensated for their effects in our model and as time progresses, we hope to see technological advances that can make these losses negligible. Another intersting hardware losses are pointing loses where there is a diffeence of angle in the line of sight transmission, but these losses are usually less than 1 dB and thus can be neglected.

For detector efficiency of 53% (value from Micius experiment), we get a loss of 2.75 dB. With APT system efficiency of 50%, we have a loss of 3 dB.

3.5 Complete Optical Link

Since we get an additional 8.35 dB more noise on both downlinks, we calculate the total attenuation for our optical link. The total attenuation of our optical link can be given by the sum of the all the losses and thus represented with respect to time as:

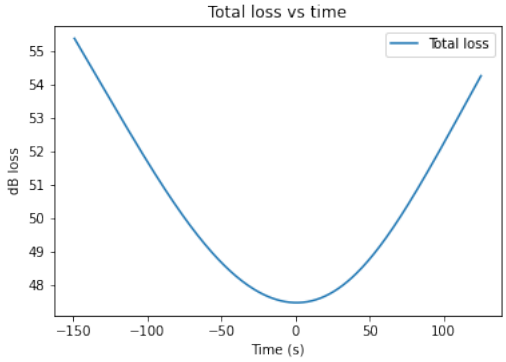

Figure 3.7: TOTAL DUAL DOWNLINK LOSS V/S TIME GRAPH

Now, we take entangled pair production to be $5.9x10^6$ and plot the sifted key rate with respect to time as:

3.5.1 Sifted QKD Key rate

This is the raw QKD key rate which is obtained through the experiment procedure.

Also, since there is 50% probabitility of chossing the same basis, we multiply the recieved bits to get the real sifted key rate.

Thus, the average sifted key for our SPG4 algorithm is 1.055 Hz, which is comparable to 1.1 Hz that was achieved in the entanglement experiment between Delingha and Nanshan in 2019. The difference of sifted key rate is because of the difference in the errors in the practical experiment which also considers the assumptions we took into our model.

Using the same principle for the sifted keys we calculated for our model, we get the same 3d plot with half the values.

3.5.2 Quantum bit error rate

The Quantum bit error rate is defined as the ratio of wrong bits recieved to the total number of bits recieved and is thus expressed as[**gisin2002quantum**]:

$$QBER = \frac{R_{error}}{R_{sift} + R_{error}} \approx \frac{R_{error}}{R_{sift}}$$

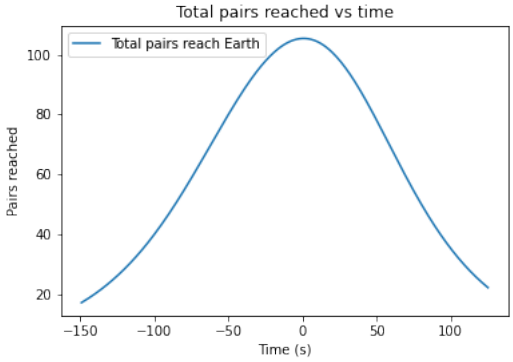

Figure 3.8: SIFTED KEY RATE V/S TIME GRAPH

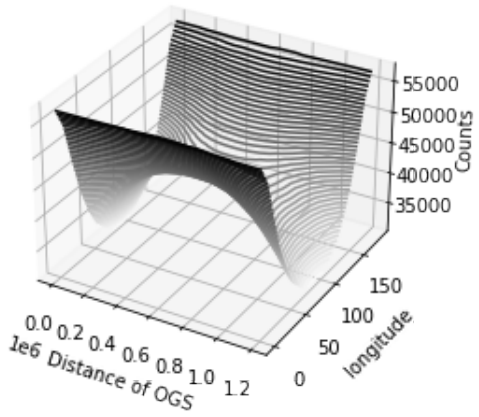

Figure 3.9: 3D PLOT OF COUNTS WITH RELATIVE ORBITAL PARAMETERS

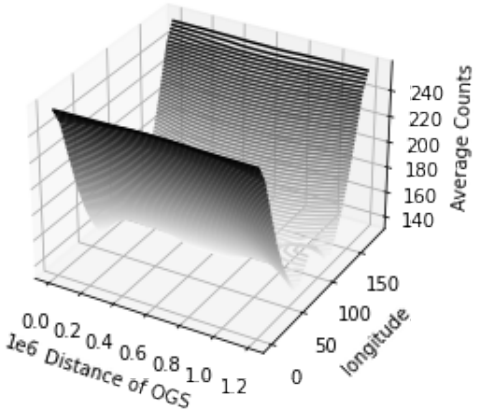

Figure 3.10: 3D PLOT OF AVERAGE KEY RATE WITH RELATIVE ORBITAL PARAMETERS

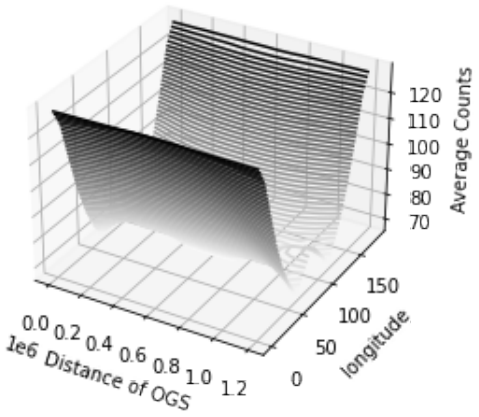

Figure 3.11: 3D PLOT OF SIFTED KEY RATE WITH RELATIVE ORBITAL PARAMETERS

and the sifted rate is calculated as:

$$R_{sift} = \frac{1}{2} q f_{rep} \mu t_{link} \eta$$

where q is the phase -coding setup factor, f_{rep} is the pulse rate, μ is the mean number of photons per pulse, t_{link} is the photon ariving probability and η is the detector efficiency. and the error rate is given by the sum of the optical errors,dark count errors, and errors due to imperfect photon sources. Thus,

$$QBER = QBER_{opt} + QBER_{det} + QBER_{acc}$$

where $QBER_{opt} = \frac{1-Visibility}{2}$, $QBER_{det} = \frac{p_{dark} n}{t_{link} \eta 2q\mu}$, and $QBER_{acc} = \frac{p_{acc}}{2q\mu}$ where p_{acc} is the probabiltiy of finding a second pair within the time window.

We see that QBER is the property of the hardware only. It depends on the detector characteristics which include its efficiency, dark count, etc.

As our model is based on the experimental observations of Juan Yin et al., therefore we take similar detector properties. Assuming four SPDs with detector efficiency better than 53% and dark count as 100 counts per second. The coincident time gate for coincident events to be 2.5 ns. Thus, the QBER is also the same for the paper and is equal to 4.5%.

3.6 Validation with SPG4 algorithm

We apply the SPG4 algorithm for the Micius Satellite and ground stations Nanshan and Delingha and plot the graph of the motion of the satellite across the Earth.

Now, we find the times for the visibilities from the two stations Delingha and Nanshan, and the time the satellite communicates with the ground stations. We also find the optical path distance for the ground stations and the satellite and then incorporate our model losses to find the key rates according to this algorithm.

These graphs give us the information for a realistic motion of the satellite which verifies our model parameters and can be directly compared to the experimental realizations for validation of our model, for the values of the losses and the sifted key rate achieved. This can further be studied by incorporating QBER to find the secure secret key length that can be used for cryptography purposes.

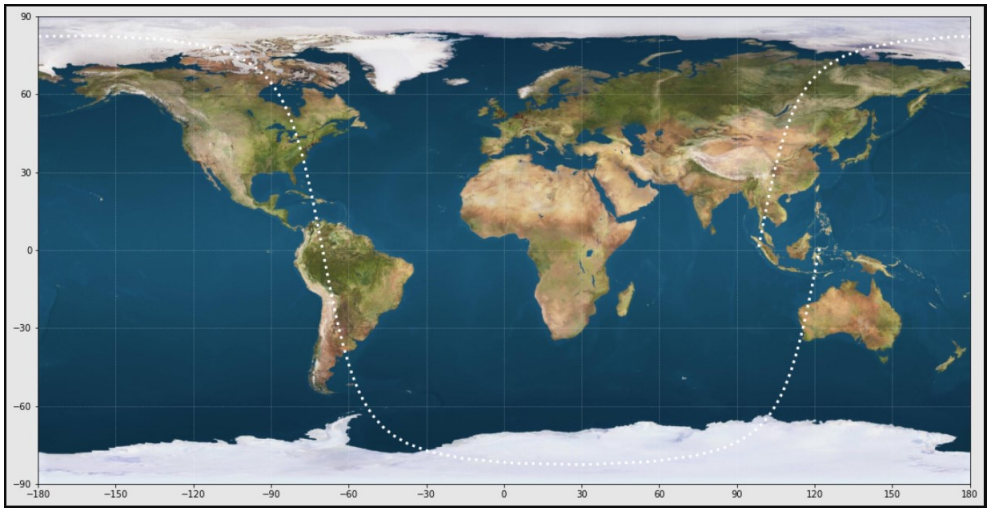

Figure 3.12: MICIUS SATELLITE MOTION ACROSS THE EARTH

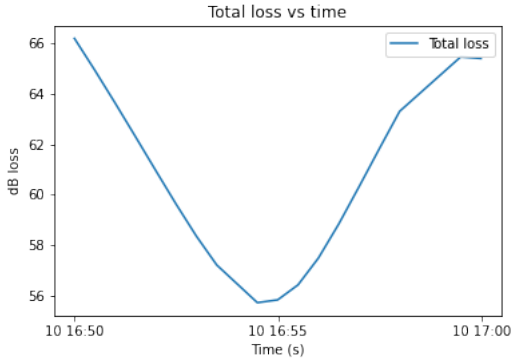

Figure 3.13: TOTAL LOSS VS TIME GRAPH USING SPG4

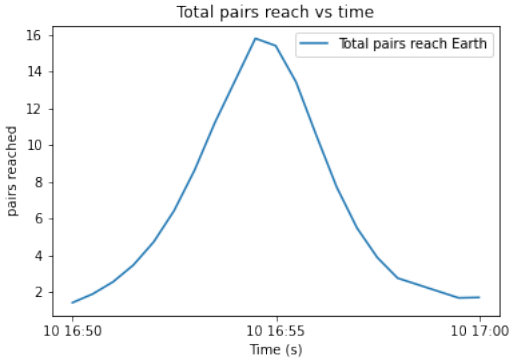

Figure 3.14: SIFTED BITS VS TIME GRAPH USING SPG4

Chapter 4

Analysis and Results

4.1 Overview

After creating our model incorporating the optical path for the photons and the associated losses, we find a secret key rate which can then be used to form a secret key length that is used for cryptography. Here we find the secret key length and compare it with other similar experiments that were performed to validate our model.

Moreover, our model plots a 3d plot for dependence of the sifted key rate on the orbital parameters and we get that the optimal results are achieved at low longitudes, i.e. the motion of the satellite in which the satellite passes over the stations, and maximum time spent in communication is in cases where the satellite passes at a 90 degree angle to the great circle joining the optical ground stations.

4.2 Secure Secret Key Rate

After obtaining the sifted key rate from our model or experiments, we use the asymptotic secret key rate equation for applying error estimation and privacy amplification to obtain the secure secret key rate. This key rate is finite key rate which is dependent on the impormation contained in a variation, i.e. Shannon entropy. Thus we find the Shor Preskill Rate taking $\kappa = 1.19$ in

$$R_{SP} = 1 - \kappa H_2(e) - H_2(e)$$

where

$$H_2(e) := -e \log_2 e - (1 - e) \log_2 (1 - e)$$

is the Shannon entropy, and e is the error rate. For $e = 4.5\%$, we find this rate as $R_{SP} = 0.598$.

Putting these values for our example in our model, we find secure key rate to be $R = 0.598 * 28.96 = 17.3 bits/s$ and finite key rate to be $R_F = 4.3 bits/s$ Thus, for our model with SPG4 algorithm, we find the secure key rate to be $R = 0.598 * 1.055 = 0.63 bits/s$ and finite key rate to be $R_F = 0.15 bits/s$ which is comparable to experimental realizations of 0.12 bits/s.

4.3 Finite Secret Key Length

A finite key should be such that the key strings with Alice and Bob are identical and should be uniformly distributed. Now, this allows the key to have failure probabilities and by using approach of the uncertainty relation for smooth entropies, the Z-basis secret key length l_z is given by[**yin2020entanglement**]

$$l_z = n_z - n_z H[E_x + \sqrt{\frac{(n_z+1)\log\left(\frac{1}{\epsilon_{sec}}\right)}{2n_x(n_x+n_z)}}] - f_e n_z H(E_z) - n_2\Delta - \log\frac{2}{\epsilon_{cot}\epsilon_{sec}^2}$$

SImilarly, the X-basis secret key length can be found and total finite key key length is

$$L = l_z + l_x$$

This finite secret key is very important as this is the key that is directly used for encryption purposes and is secure from all networks and thus can be applied to the message that needs to be encoded. The researchers obtained a 372-bit secret key in their experiment.

4.4 Investigative Questions Answered

- We found that the factors that influence the Quantum key distribution key rate to be the range of the communication with the reliance of the orbital parameters in Satellite QKD. This enables the the dependence on the optical path of the qubits produced and the losses therefore for the optical beam. Also, we observe the influence of the internal factors of the transmitter and reciever for production and measurement of the qubits. Moreover, our whole procedure is dependent on the configuration we used and the protocol that is implemented.
- We concluded that these factors directly influence the QKD sifted key rate that we obtain which depends on the optical path of the quantum information which is indeed dependent on the orbital paramaters

of the satellite relative to the ground stations as the geometric and atmospheric losses are dependent on the orbit.

- In our model, we took into consideration the atmospheric losses and the prominent effects took into our model include scattering, dispersion and turbulence effects. Moreover, this connection is highly dependent on the weather parameters which have incorporated in our model but have not implemented for comparison of the key rates with experimental realizations.

- Here, we used BBM92 protocol, also known as the entanglement based BB84 quantum protocol. We have selected this protocol since it is better than BB84 protocol in the sense that it is trusted node free which makes it more secure as the entangled bits can be produced anywhere. Also, we perform a dual downlink configuration which has much less errors compared to an uplink configuration thus making this protocol better than Twin-field QKD protocol as it avoids the spreading of the beam at an early stage reducing losses.

- In our report we have mentioned that the secure key is dependent on the sifted key rate as well as the Shor-Preskill bound, thus Bell inequality is a sufficient condition for obtaining a secure sifted QKD key rate. After obtaining the sifted key rate, we apply error correction and privacy amplification to obtain the secure secret key. Thus we can conclude that Bell inequality is sufficient for individual atacks but a secure key must also be protected from coherent attacks, which needs to be taken into consideration.

- We see that QBER directly depends on the detector efficiencies and dark counts which affect the sifted QKD key rate that we calculate and thus we take these into account. We can see that optimizing our detector can drastically influence the security of the secure quantum key length produced for encryption purposes.

- The secure key length produced if positive can then be used for practical encryption purposes.

Chapter 5

Conclusion

We created a model for satellite quantum key distribution using BBM92 protocol in dual-downlink configuration and analysed the secret key length produced using asymptotic secret key rate formula. Here we modeled the dependence of key rate on the orbital characteristics and comparing the results to the real-life experiments for validation of our model. In addition to that, a model with SPG4 algorithm was also prepared to validate the losses into account. This feature validates our model in much more detail and makes our model very accurate for the distance and angle of intersection of satellite motion relative to the positions of the two optical ground stations. We can conclude that our model is pretty accurate in determining the sifted key rate that can be achieved for different orbital characteristics of the satellite relative to the positions of the optical ground stations.

We infer from our model that even though the maximum visibility time is for a configuration in which the satellite between the stations at an equal distance, the optimal secure key rate obtained is for configurations where the satellite passes over the stations which is a counterintuitive result. Thus, we need to select the orbital parameters to optimize the visibility time and the secret key rate to achieve best secret key length and our model can give a good insight into the same. We observe the difference in the values is because of the difference in range values between our model and the experimental results. Our model with SPG4 algorithm affirms our understanding of the system with the production of very similar secure key rate as the experimental observations.

Our model explicitly defines the relative orbital parameters for optimal secure key rates that can be achieved for cryptography purposes. Therfore, our model provides a good insight into the optimum relative motion of the

satellite with respect to ground stations to achieve best secret key rates.

Our model can be further improved in detail by computing other losses like pointing errors and other losses to accurately determine all the losses in the optical path of the qubits. Moreover, the shape of the Earth's perturbations can help us in determining the exact values for our orbits.