MŰEGYETEM 1782

Budapest University of Technology and Economics
Faculty of Electrical Engineering and Informatics
Department of Networked Systems and Services

Ákos Korsós

Analyzation of first generation quantum key distribution protocol on Earth-satellite channel

SUPERVISORS

László Bacsárdi, PhD., Sándor Imre, DSc., Zsolt Kis, Phd.

BUDAPEST, 2016

Tartalomjegyzék

Összefoglaló

A TDK dolgozat célja, hogy szimuláció segítségével vizsgálja a Föld-műhold közti kvantum kommunikációt és egy globális, műholdas kvantum kulcsosztó hálózatot javasoljon.

A kvantumszámítógépek fejlődése a jelenleg használt információtechnológia több területére hatással van. A digitális kommunikáció során az információk titkosítása és a titkosításhoz használt kulcsok megosztása olyan kriptográfiai algoritmusokkal történnek, melyek biztonsága a komplexitásukból ered, vagyis a jelenlegi technológiával csillagászati ideig tartana feltörni a titkosítást. Ez a biztonság a kvantumszámítógép megjelenésével azonban már nem lesz elegendő, a jelenlegi kriptográfiai rendszerek (például az RSA és az azon alapuló SSH és SSL/TLS) bizonyos kvantumalgoritmusokkal (például Shor-algoritmus) rövid időn belül feltörhetőek.

Ezért a lehető leghamarabb célszerű olyan kriptográfiai rendszereket alkalmazni, melyek ellenállnak a kvantummechanikai alapú feltörésnek . Egy lehetséges megoldás az optikai kábelen történő kvantum kulcsosztás, amellyel azonban a fizikai korlátok miatt, az egymástól legfeljebb körülbelül 100km-re található felek között lehetséges a kulcsosztás. Ha ezt a távolságot tovább akarjuk növelni, akkor egy lehetséges megoldás a műholdakon alapuló és szabadtéri csatornán történő kvantum kulcsosztás, mely használatával globálisan lehetségessé válna két tetszőleges pont között az információelméleti biztonságot nyújtó kvantum kulcsosztás.

Dolgozatomban ennek a globális, kvantum alapú kulcsosztó műholdas hálózatnak a szimulációjával vizsgálom a Föld és a műhold közti kvantum kommunikáció tulajdonságait, az eredményeket kiértékelem és javaslatot teszek egyes, a foton polarizációs állapotának mérését torzító hatások korrigálására is.

Abstract

The purpose of this TDK paper is to analyze the Earth-satellite quantum communication using a simulation and to propose a global, satellite based quantum key distribution network.

The development of quantum computers effects several fields of the current information technology. In digital communication the data encryption and the distribution of keys used for the encryption rely on computationally secure cryptosystems, which means that cracking the encryption with current technology would take astronomical time. With the arrival of quantum computers, this security will not be enough, the current cryptosystems (e.g. RSA and the relying SSH or SSL/TLS) will be breakable in short time with existing quantum algorithms (e.g. Shor's algorithm).

For this reason, it is expedient to develop and apply cryptosystems as soon as possible, that can withstand quantum mechanical code breaking. One possible solution is the quantum key distribution using optical fiber cables, but because of the physical limitations, this can only be used for nodes with up to 100km between them. If we want to increase this distance, then a possible solution would be a satellite-based, free-space quantum key distribution, which could provide global, information-theoretically secure key distribution between two arbitrary nodes on Earth.

In this work, I analyze the properties of the Earth-satellite quantum communication by simulating a global, satellite based quantum key distribution network, evaluate the results and propose solutions to correct some of the effects that distort the polarization measurement of the photons.

1 Introduction

Humans have been writing in code since the invention of writing, and the everlasting competition between codemakers and codebreakers has always fascinated me.

Codemakers have developed ciphers like the Caesar cipher, Vigenère cipher and the Enigma. These codes were believed to be unbreakable until codebreakers eventually found and exploited the weaknesses. Cryptography and cryptanalysis have always had a huge impact on history [1].

Currently we live in an era, where public key cryptosystems like RSA can guarantee computationally secure communication. Yet, the quantum computers are evolving and Shor's quantum algorithm will be able to crack RSA in just a few seconds. This would make RSA based protocols like SSH and SSL/TLS useless. Thus we need new methods for key distribution that can withstand attacks from quantum computers. Quantum key distribution may be a solution that can take cryptography to the next level.

Today's wireless communication conveniently allows us to be connected anywhere, but it is much more susceptible to eavesdropping than communication through optical fibers. Due to the openness of the wireless communication channel, there is a more urgent need to enhance its security. Using one-time pad encryption would provide an information theoretically secure communication, however it requires truly random and long keys, also the key distribution for each message is very cumbersome and impractical.

Using quantum key distribution (QKD), which is probably the most advanced practical branch of quantum communication, two communicating parties can establish a secret cryptographic key. Since the security is based on the fundamental properties of quantum mechanics, in principle information-theoretic security can be achieved. The secret key, established with QKD can be used to encrypt further classical communication to provide information-theoretically secure encryption and a mobile QKD network could deliver an unparalleled level of security to wireless users. In the future, even the one-time pad could be used in conjunction with QKD protocols.

Although commercial applications of QKD technology are already available, currently direct QKD links on the ground cannot reach distances beyond a few hundred kilometers due to optical losses [2]. With quantum repeaters long-distance QKD networks may be feasible, but such devices are not ready for operational integration yet [3].

Alternatively satellites could be used as relays to provide a global free-space QKD network. An orbiting satellite could act as an untrusted node, connecting two ground stations and facilitating key distribution without knowing the key, or as a trusted node by exchanging individual keys with each ground station and broadcasting the combination of the keys. Then the two ground stations can extract the key of the other station from the broadcasted combination, giving both stations a shared key. This way no other party than the satellite can intercept the shared key. By requiring only one link at a time the trusted node satellite has a simpler design and allows key distribution between two parties located anywhere on Earth, with a suitable orbit.

2 Short Overview of Orbital Mechanics and Quantum Computing

2.1 Basic Orbital Mechanics Concepts

2.1.1 Orbital elements

The parameters required to uniquely identify a specific orbit are called orbital elements. Many ways exist to describe the same elliptic orbit, but in this paper the six Keplerian elements are used [4].

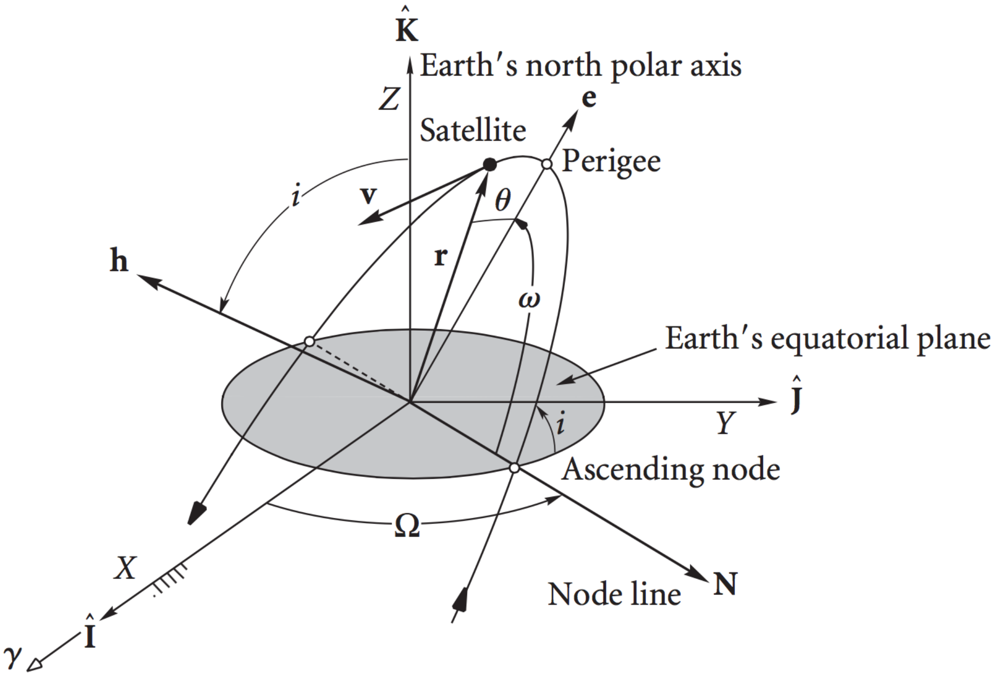

Figure 1: The orbital elements that describe an elliptic orbit in three dimensions [4]

These consists of two elements that define the shape and size of the orbit in the plane:

- **Eccentricity**: shape of the ellipse, describing how much the orbit deviates from a perfect circle. The value of 0 is a circular orbit and values between 0 and 1 form an elliptical orbit.
- a **Semi-major axis**: the sum of the periapsis and apoapsis distances divided by two. In case of circular orbits it is the distance between the centers of the bodies. *(the semi-major axis can be replaced by the angular momentum)*

To locate a point on the orbit rquires a third element:

- θ **True anomaly**: an angular parameter that defines the position of a body along an elliptic orbit *(frequently replaced by the mean anomaly)*

Describing the orientation of an orbit in three dimensions requires three additional elements:

- i **Inclination**: vertical tilt of the ellipse with respect to the reference plane, measured at the ascending node (where the orbit passes upward through the reference plane)
- **Right ascension (RA) of the ascending node**: horizontally orients the ascending node of the ellipse with respect to the reference frame's vernal point (the reference direction)
- **Argument of perigee**: defines the orientation of the ellipse in the orbital plane, as an angle measured from the ascending node to the periapsis

In this work, I have used the plane of the equator as the reference plane and the direction defined by the prime meridian as the reference direction (thus the vernal point is where the prime meridian passes the equatorial plane.

During the simulations the inclination, the RA of the ascending node and the argument of the perigee are all 0, therefore the orbital plane is equivalent to the Earth's equatorial plane and the perigee is located on the plane defined by the prime meridian. These simplify the simulations in such a way, that the elliptic orbit can be identified by only describing the eccentricity and the semi-major axis.

If we examine the elliptical orbit, we can write up several equations that can be used later.

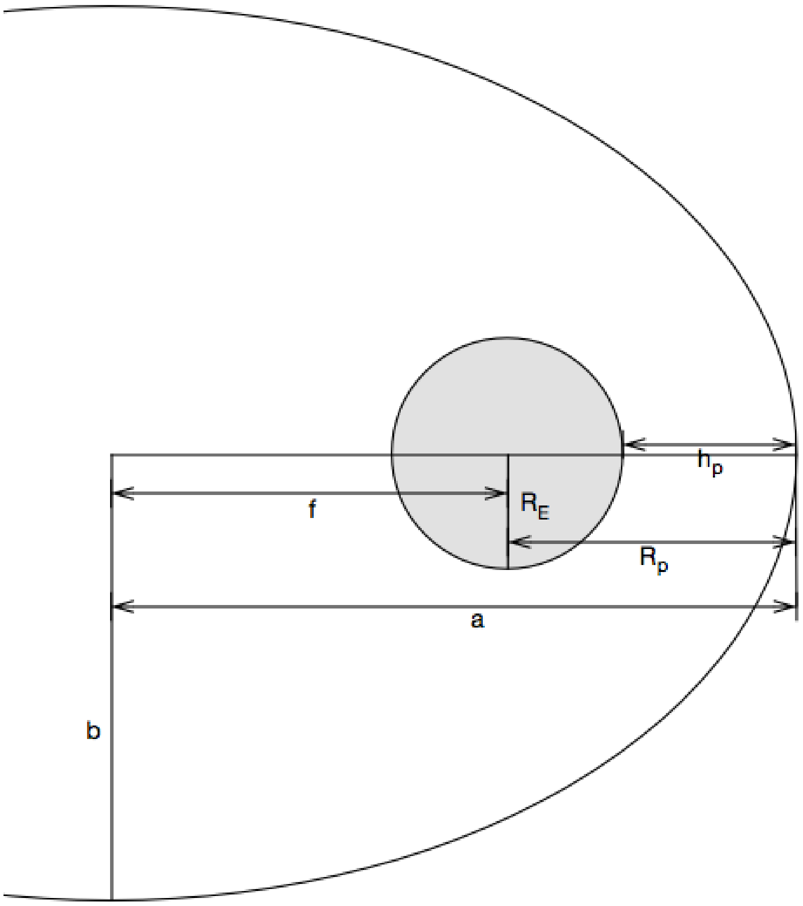

Figure 2: An elliptic orbit around the Earth, where a is the semi-major axis, b is the semi-minor axis, f is the focus distance, R_E is the radius of the Earth, R_p is the perigee distance and h_p is the altitude of the satellite at the perigee.

The perigee distance is equal to the radius of the Earth and the altitude of the orbiting satellite when it is closest to the Earth (at perigee) because the center of the Earth is located in the focus of the elliptic orbit:

$$R_p = R_E + h_p$$

The perigee distance can also be described using the eccentricity and the semi major axis:

$$R_p = (1- \quad)a \qquad a = \frac{R_p}{(1- \quad)}$$

The semi-major axis is the sum of the focus distance, the radius of the Earth and the altitude of the satellite at the perigee:

$$a = h_p + R_E + f \qquad f = a - h_p - R_E$$

Also, the focus distance can be expressed using the semi-major axis and the semi-minor axis:

$$f^2 = a^2 - b^2 \;\rightarrow\; b = \sqrt{a^2 - f^2}$$

Using these equations we are able to calculate all the necessary parameters *(focus distance, semi-major axis, semi-minor axis)* of an elliptic orbit just by describing the eccentricity of the orbit and the altitude of the satellite at the perigee.

2.1.2 Orbiting body

When the orbital elements are known, we can calculate the attributes of the orbiting bodies. The orbital speed of a body travelling along an elliptic orbit can be calculated from the Vis-viva equation as:

$$(1) \qquad v = \sqrt{\mu\left(\frac{2}{r} - \frac{1}{a}\right)} \;,$$

where is the standard gravitational parameter, r is the distance between the orbiting bodies and a is the length of the semi-major axis.

The orbital period can also be computed as:

$$(2) \qquad T = 2\pi\sqrt{\frac{a^3}{\mu}} \;.$$

Assuming a Cartesian coordinate system where the origo is the center of the elliptic orbit, the *x* axis is along the major axis and the *y* axis is along the minor axis, the coordinates of a body travelling along the elliptic orbit can be calculated from the trigonometric parametric formula of the ellipse:

$$(3) \qquad \begin{aligned} x(\Theta) &= a \cdot cos(\Theta) \\ y(\Theta) &= b \cdot sin(\Theta) \end{aligned}$$

where θ is the true anomaly, the angle between the current position of the orbiting body and the direction of the periapsis. In our case the direction of the periapsis is equivalent to the *x* axis.

Also, if one of the coordinates is known, the equation of an ellipse can be used to calculate the other coordinate:

$$(4) \qquad \left(\frac{x - x_0}{a}\right)^2 + \left(\frac{y - y_0}{b}\right)^2 = 1 \;,$$

where x_0 and y_0 are the coordinates of the ellipse's center.

2.1.3 Basic Quantum Concepts

The basic unit of information in classical computing and digital communication is a binary digit (bit). A bit can have only one of two values, most commonly represented as either 0 or 1.

The **quantum bit (qubit)** is the quantum analogue of the classical bit in quantum computing and has a few similarities to a classical bit. However, while a classical bit has to be in one state or another, a quantum bit is described by a wave function (or probability amplitudes) which describes a two state quantum mechanical superposition. Therefore a qubit exists in both 0 and 1 states simultaneously in the absence of an observer.

A qubit in an arbitrary state can be measured and once an observer has measured the qubit, the wave function collapses and one of the states emerges according to the probability described by the wave function. The two states in which a qubit may be measured are called as basis states and are conventionally written as $|0\rangle$ and $|1\rangle$ *("ket 0" and "ket 1")*, represented by the Dirac (or "bra-ket") notation [5].

An arbitrary state, written as $|\varphi\rangle$ can be described as a weighted combination of the computational basis vectors, where the complex numbers a and b are called the probability amplitudes:

$$|\varphi\rangle = a|0\rangle + b|1\rangle = a\begin{bmatrix} 1 \\ 0 \end{bmatrix} + b\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

When $|\varphi\rangle$ is measured, the probability of outcome $|0\rangle$ is a^2 and the probability of outcome $|1\rangle$ is b^2 . Because the total probability of all possible outcomes must be 1, a and b must fulfill the $a^2+b^2=1$ equation.

We can also geometrically represent a qubit as a sphere, called the Bloch sphere, where the points on the sphere surface are the pure states of the qubit.

Quantum communication means the distribution of different quantum states between two parties, conventionally named Alice and Bob via a quantum channel. Theoretically it makes no difference whether atoms, electrons or any other quantized particles are used in the exchange. However it is the quantum of light, the photon which is preferably used, because photon quantum states can be transmitted over longer distances without decoherence.

A **photon** is an elementary particle, the quantum of all forms of electromagnetic radiation including light. An electromagnetic wave consists of an electric and a magnetic field oscillating at right angles to each other (in free space). The wave itself propagates at a direction perpendicular to oscillations in both fields (in free space). In general, natural light is unpolarised, meaning that it's electric field is oscillating in random directions. By passing the light through a polarization filter it can be made into polarized light, meaning that it's oscillations take place in a single direction (see Fig. 3).

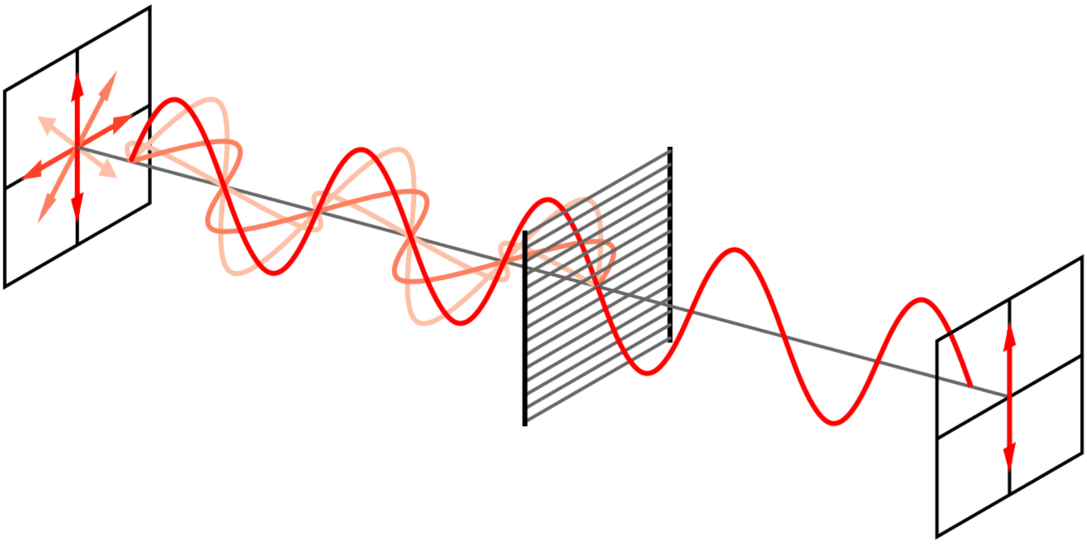

Figure 3: After unpolarised light passes a polarisation filter, its electric field is oscillating along one direction only and the results are polarised photons.

(Image courtesy: WikimediaCommons https://commons.wikimedia.org/wiki/File:Wire-grid-polarizer.svg)

Two orthogonal, such as vertical and horizontal polarisation states are called as a polarisation basis. For example, we could assign $|0\rangle$ to the horizontal (0°) polarisation state and $|1\rangle$ to the vertical (90°) state. In this case, when a photon with 45° polarisation is measured, the result would be $|0\rangle$ or $|1\rangle$ with 50-50% probability. Respectively measuring a photon with 30° polarisation would result $|1\rangle$ with 30/90 = 33% probability.

Quantum channel is any medium which allows light to propagate, thus carries quantum information. The most common channels are optical fibers and free space. Free space offers much more flexibility, allowing links between moving objects but it is also much more noisy. We can define four different communication models depending on whether we want to transmit classical/quantum information over a classical/quantum channel.

Transmitting *classical information over a classical channel* is trivial since it does not involve quantum particles and there are several classical techniques for this.

In the case of transmitting *classical information over a quantum channel*, Alice encodes the classical information in a qubit and sends the qubit to Bob, who then recovers the classical information via measurement. In the *superdense coding* technique, one can send two bits of classical information using only one qubit.

Another scenario is when we would like to send *quantum information over a classical channel*. In quantum teleportation, Alice and Bob has one particle of an entangled pair. After performing some unitary transformations, Alice measures her entangled particle and the qubit to be teleported, which results in two classical bits of information. She sends these two bits over a classical channel to Bob, who will modify his qubit in a way, that results in a qubit identical to the original qubit chosen for teleportation.

Transmitting *quantum states through a quantum channel* is basically using any quantized particle and exchanging the particle between the communicating parties. For example, when using photons, one can use lasers to send the polarized photons to the receiver, but even electrons or atoms can be exchanged and their spin property can be used for the quantum states.

Quantum Entanglement

Two particles can be generated in such a way, that they behave as if they are a single entity and measuring one particle causes the probability wave function of the other particle to collapse into an exact, predictable state. These pairs are called EPR pairs after Einstein, Podolsky and Rosen who first described this phenomenon [6].

For example, particles have a property called "spin" which could be spin-up or spin-down. If the particles of a spin singlet EPR pair are separated, and one particle is found to be spin up, measuring the other particle on the same basis will be found to be the exact opposite: spin down. It suggests that one particle of the entangled pair instantaneously "knows" what measurement has been performed on the other. Later Bell investigated the properties of entangled systems and proved, that quantum entanglements hold even when the two particles are physically separated and the phenomenon occurs regardless of the distance between the particles [7].

Einstein and others considered this behavior to be impossible, referring to it as "spooky action at a distance" because seemingly it would contradict that nothing can travel faster than light (called the EPR paradox), but later the counterintuitive predictions were verified experimentally [8].

Quantum No-Cloning

The Quantum No-Cloning Theorem was first identified by Wootters, Zurek and Dieks in 1982, and it states that it is impossible to create an identical copy of an arbitrary unknown quantum state [9]. This means that copies of quantum states cannot be used for error correction, an eavesdropper cannot create copies of intercepted qubits and quantum signal cannot be amplified along a quantum channel.

Quantum Error Correction

Transmitted quantum information has to be protected from errors which occur through noise on the channel, the presence of an eavesdropper or quantum decoherence (loss of ordering of the phase angles in quantum superposition, causing dephasing). A classical error correction method is based on redundancy, copying a bit multiple times and since the errors are mostly single-bit errors, the information can be restored from the other redundant bits.

The no-cloning theorem makes impossible to copy the qubits. Shor developed a method to create a quantum error correction code (ECC) by spreading the information of one qubit onto a highly entangled state of several qubits [10].

A typical quantum error correction in QKD systems also consists of estimating the error rate of transmission, the quantum bit error rate (QBER) and assuming that all errors are due to eavesdropping. If the actual QBER is less than a predetermined threshold value, the key is assumed to be safe, otherwise the key is discarded and a new key establishment is initiated.

Privacy Amplification method is a necessary step in all practical QKD protocols. When Alice and Bob establishes a key, a malicious eavesdropper may gain some information about the key. Privacy amplification counteracts this by compressing the established key using universal hash functions by an appropriate factor. The compression factor is determined by the previously estimated QBER, assuming that all transmission errors were caused by eavesdropping.

There are two main categories of QKD, each exploits a different property of quantum mechanics. Prepare and measure(P&M) protocols are based on the Heisenberg uncertainty principle and the no-cloning theorem, while entanglement-based (E-B) protocols exploit the quantum entanglement phenomenon.

These two categories can be further divided into two subcategories, discrete variable (DV) QKD and continuous variable (CV) QKD.

2.2 First generation: Discrete Variable QKD

Discrete Variable QKD (DV QKD) exploits the particle nature of light. The information is encoded at single photon level and single photon detectors are used to measure the quantum states. DV protocols were the first to be invented and they still remain the most widely implemented protocols.

The first DV QKD protocol was proposed in 1984 by Bennett and Brassard therefore it is called BB84 and it is based on Heisenberg's Uncertainty principle [11]. The basic idea is that if Alice and Bob are two communicating parties, Alice can transmit a random secret key to Bob by encoding the bits of the secret key in the polarization of individual photons and sending this series of photons to Bob. Since the measurement of the photons is not possible without disturbing their states, any attempt would reveal the presence of the eavesdropper. Also the non-cloning theorem guarantees that the eavesdropper cannot replicate a particle of unknown state.

There are several other DV QKD protocols based on Heisenberg's uncertainty principle which are essentially variants of the BB84 idea.

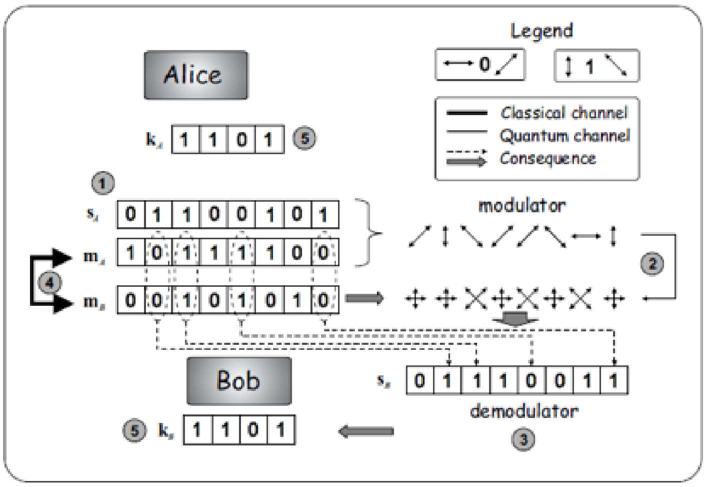

Figure 4: An overview of the BB84 QKD protocol. Source [5]

In the first step of the BB84 scheme, Alice creates a random bit and then randomly selects one of her two bases, rectilinear(+) or diagonal (×) to transmit it in. She then prepares a photon polarization state depending both on the bit value and basis according to a predefined rule. Alice then transmits a single photon in the specified state to Bob, using a quantum channel. This process is then repeated from the random bit stage, with Alice recording the state, basis and time of each photon sent.

Basis	0	1
+	↑	→
×	↗	↘

Table 1: Alice's rule for preparing the photon polarization state.

As Bob does not know the basis, he selects a random basis and measures the received photon in it. He does this for every received photon, recording the time, measurement basis used and the result. After Bob has measured all the photons, he communicates with Alice over a public classical channel. Alice broadcasts the basis the photons were sent in and Bob broadcasts the basis each was measured in. They both discard the bits and photon measurements where Bob used different basis, which is half on average. The remaining half of the bits is then used as a shared key.

To check the presence of an eavesdropper, they compare a certain subset of their remaining bit strings. If a third party has eavesdropped on the photons and has gained any information about the photon polarizations, then this would introduce errors in

Bob's measurements. If the bits differ they drop the shared key and try again, as the security of the key cannot be guaranteed.

After publishing the BB84 protocol, Bennett realized that it is not necessary to use two orthogonal basis for encoding and decoding, instead a single non-orthogonal basis can be used without affecting the security of the protocol [12]. Thus it operates with only two states instead of four. This method was published in 1992 and is known as the B92 protocol.

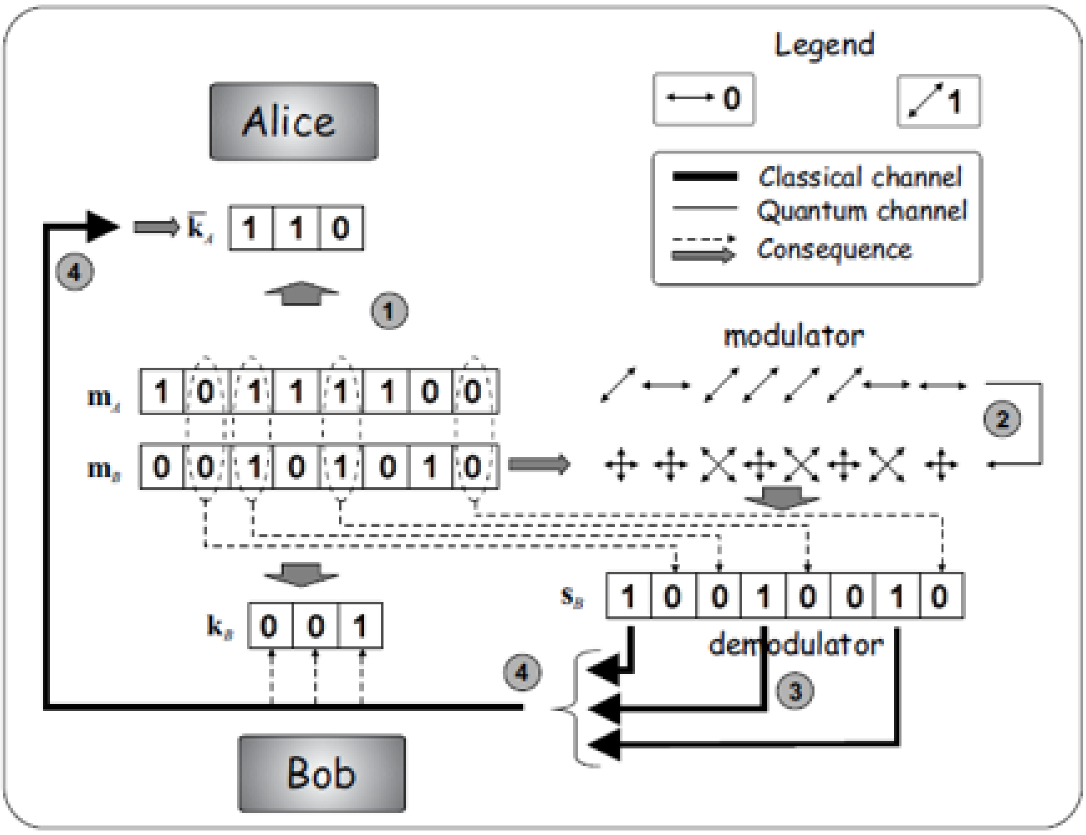

Figure 5: An overview of the B92 QKD protocol. Source [5]

The steps of the B92 are similar to the BB84 protocol, Alice selects a random bit string. However this time the basis used to encode each bit is not random, but determined by the bit value. If the bit value is 0 she uses rectilinear basis, otherwise diagonal bases. Bob still randomly selects the basis used to measure each received photon but if he chooses the wrong basis, his measurement result may be wrong with 0.5 probability. He can simply tell Alice whether or not he measured the received photon correctly.

Bit	Basis	Photon polarization
0	+	→
1	×	↗

Table 2: The rule for choosing the basis and preparing the photon.

In 1991, Ekert proposed a new scheme that uses entangled pairs of photons, known as the E91 protocol [13]. The entangled pairs can be created by Alice, Bob or even by a trusted third party. The photons are distributed so that Alice and Bob receives one photon from each pair. This is definitely a more secure method than using polarised photons, because entangled states make it hard for an eavesdropper to gain information about the key.

In the E91 protocol, Alice and Bob both independently and randomly choose from three different basis. If they choose the same basis, their measurement results will be anti-correlated, meaning when Bob's result is 0, Alice's result will be 1 and vica versa. If they don't use the same basis for the measurements, the results are random. After the measurements, Alice and Bob both publicly announce which bases the particles were measured in and discard the random measurements. Because there is a 33% chance that they used the same basis for a given measurement, on average 33% of the bits remain that can be used as the shared key.

There are several other DV QKD protocols, both entanglement and polarised photon based, most notably the COW (2004), KMB09 (2009), S09 (2009) and S13 (2013) protocols [14].

2.3 Second generation: Continuous Variable QKD

DV coding requires single photon sources and photon-counting measurement techniques for which there are currently no reliable and cheap solutions for practical use. An alternative method, which exploits the wave nature of light was conceived in the early 2000's. Two continuous variable (CV) QKD protocols were proposed in 2002 by F. Grosshans [15] and Ch. Silberhorn [16].

In CV QKD, information is encoded onto the amplitude and phase quadratures of weak pulses of light and the receiver measures the quadratures of the received laser beam using homodyne detection methods. So it does not rely on truly single photon sources or photon counters.

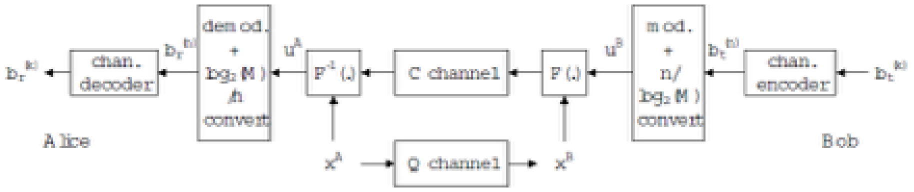

Figure 6: Overview of a generic CV QKD protocol.

During a generic CV QKD protocol, Alice generates two separate coherent light pulses. One weak signal and a strong local oscillator (LO) for synchronization. The signal is then modulated using amplitude and phase modulators, following a centered Gaussian distribution in both quadratures. Using multiplexing, the signal and the LO are transmitted to Bob without any cross-talk. Bob then measures the received signals using a homodyne detector.

After the quantum transmission, a classical communication is also required. Alice and Bob compare a random sample of the distribution and determine the noise level. Finally, Alice and Bob applies error-correction algorithms and privacy amplification to extract the secret key.

CV QKD was proven to be information-theoretically secure in 2009, therefore guarantees similar security to DV QKD. But outweighs it in terms of performance, cost and power consumption, making it much more compatible with telecommunication technologies [17].

3 State-of-art of the free-space QKD

The transformation of the secure communication market is imminent in the near future. The currently used standard public key encryption methods will not be resistant to attacks by quantum computers and since 2015 the National Security Agency (NSA) of the United States advises vendors to be prepared for a transition to cryptography that can withstand quantum computers [18].

As part of the transition, a global QKD network is required to provide secure key distribution between two communicating parties, located anywhere on Earth. Since fiber-based QKD solutions are already available for Metropolitan Area Network (MAN), it seems reasonable to connect the different MANs using geosynchronous satellites to provide a wide area network (WAN) [19]. The feasibility analysis of such method was successfully concluded in 2012 and the validity of the analysis was verified in 2013 and 2014 in Erlangen. Even the possibility of using satellites as quantum repeaters to extend the distance of entangled pair distribution has been studied with promising results [20].

Despite the rapid advancements, free-space quantum communication still raises several questions.

A free-space quantum communication requires direct line of sight between the transmitter and the receiver. Therefore a satellite QKD link requires precise optical pointing mechanisms in the transmitter that continuously aims at the receiver. Recent demonstrations of QKD use moving transmitters, imitating the case of a transmitting satellite platform, however a satellite-based quantum receiver seems less complex to develop [21]. In 2015 the viability of a moving receiver was demonstrated by driving a pickup truck with a receiver approximately 650 meters from a transmitter [22]. During the demonstration the BB84 QKD protocol was implemented with a tracking algorithm to correct the incurred polarization drifts. Albeit the speed of the truck is significantly less than the orbital velocity of a low earth orbit (LEO) satellite, the feasibility of QKD from a ground station to an orbiting satellite was proved.

In 2013, a Chinese team demonstrated a quasi-single-photon transmission using a LEO satellite at 400km altitude [23]. The size of the corner retro-reflector on the satellite was 11.34 cm^2 and the orbital velocity of the satellite was approximately 7.5 km/s, which requires immensely precise pointing mechanisms and tracking algorithms. The photons were emitted in pulsed intervals, but the return time was disordered due to the changing distance of the satellite, rising new issues. In order to identify which pulse the photons belong to, they had to measure the current distance of the satellite, use it as a synchronization data and perform an offline analysis. Eventually they have achieved a signal-noise ratio that seems good enough to set up an unconditionally secure QKD link between satellite and Earth.

However several transmissions proved the feasibility of quantum communication from low earth orbit satellites, within 1500 km of altitude, satellites with orbits higher than LEO are also interesting for the implementation of a global QKD network using geostationary satellites. Therefore italian researchers experimented with a single photon exchange spanning a distance of 7000 km [24]. Their results show that while it is required to upgrade the detectors, it is possible to achieve a signal to noise ratio suitable for quantum communication up to 23000 km.

A team from the University of Waterloo, Canada constructed an experimental apparatus in 2015 that implements the BB84 DV QKD protocol with minimal resource requirements, that could be practically used on a satellite in the future [25]. Laboratory experiments showed the feasibility of satellite QKD using a quantum optical uplink with reduced computational requirements at the receiver. They have also noted that the varying time of flight due to the changing distance between the satellite and ground station is still an important challenge of satellite QKD.

In August, 2016 a collaborative endeavour between the Chinese Academy of Sciences and the Austrian Academy of Sciences, called QUESS (Quantum Experiments at Space Scale) launched the world's first satellite dedicated to testing the fundamentals of quantum communication in space. The main goal of the mission is to demonstrate QKD between the satellite and two ground stations [26].

Another challenge in free-space QKD is how to match the temporal and spatial modes of photons from different users. Since the photons from two QKD users are highly indistinguishable and atmospheric turbulence acts independently on the two quantum channels, matching the arrival times and spatial modes of photons propagated through two independent free-space channels could be very difficult [27]. In 2015 a free-space reconfigurable QKD network was proposed by a team in the USA, introducing a measurement device independent (MDI) QKD that could solve this challenge and has been also successfully demonstrated over a 600 km long fiber link.

An experiment in 2015 showed that quantum interference also has to be taken into account during quantum communications [28]. Individual particles can be in more than one place at a time, which is called quantum superposition and causes interference during single photon detection which can be observed with photons, electrons and even other particles. The Italian team demonstrated the interference along satellite-ground channels and even measured that the relative motion of the satellite to the ground station modulates the interference pattern.

Using a free-space quantum channel it is inevitable that background noise will appear during the transmissions. The advantage of QC via satellites is that transmission loss is dominated by diffraction rather than absorption and scales much more better with distance. For example the transmission loss for a photon pair for a 2000 km distance in free-space is only of order 40 dB, while in a fiber link for the same distance it would be 300 dB [20]. Also a study analyzed effects of channel noise on different DV and CV QKD protocols by describing the channel noise as a single, constant parameter because it seems that in short periods of time channel noise affects all of the travelling photons in the same way [29]. If channel noise causes too high transmission loss, it could be problematic to tell whether the loss was caused by the noise or by the eavesdropping of a malicious attacker. Their results clearly show that while CV QKD protocols seem to be more resilient for some intermediate values of the channel transmittance, DV QKD protocols perform much better when channel transmittance is close to 1 (seemingly no channel noise) or the transmittance is significantly less than 1 (channel with high noise). They suggest that if high quality sources and detectors are available, but the quantum channel is noisy, DV QKD techniques have more potential.

Single-photon detection is related to various important applications, specifically the realizations of precise measurement and DV QKD protocols. Photon detection is affected by several factors and to decrease noise and unwanted dark counts, multiple solutions have been developed including low temperature detectors and superconductors [30]. A chinese team in 2016 proposed a technique to enhance the photon detection efficiency by using the cavity technique to convert the traveling photon into a standing wave and storing in the cavity.

A team mainly from the United Kingdom has analyzed the consequences of spacetime being curved on different quantum communication protocols [31]. They have shown that the photon propagation is affected by the curvature of spacetime and may change their frequency distribution in centre, shape and bandwidth. These effects occur between two communicating users that are located at different heights in the gravitational potential of the Earth, for example between a satellite and a ground station.

Also, the presence of atmospheric turbulence represents an obstacle for free-space quantum communications. In 2014, a quantum communication experiment succeeded in establishing a point-to-point free-space link at a distance of 1.6km, using discrete modulation of two or four signal states [32]. Their results show that Gaussian modulation can be realized with this system and indicates strong potential of free-space channels for CV QKD systems. They also noted, that in free-space scenarios, special consideration has to be given to atmospheric turbulence that leads to undesired excess noise in the communication. The fluctuating transmissivity of the channel increases optical losses and the background photons that are always present increase the overall quantum bit error rate (QBER) and limit the possibility of exchanging a secure key. For this reason, current demonstrations of QKD have avoided the condition of normal background by operating in dark nights or by using a very strict filtering that causes a low key rate.

However, an Italian team in 2014 introduced a method to exploit the turbulence as a resource for QKD [33]. They pointed out that the transmissivity typically has peaks lasting a few milliseconds, distributed in a low transmissivity background. They proposed an adaptive real time selection (ARTS) scheme where these peaks in transmissivity are instantaneously detected and it makes available the selection of the time intervals of high channel transmissivity, producing a viable QBER.

Secure quantum communication has been so far confirmed feasible in both fiber and free-space air. However, seawater covers more than 70% of the earth and underwater communication is vital for underwater exploration and modern communication. Recently a chinese team demonstrated that polarization quantum states can survive even after travelling through seawater which makes underwater quantum communication also feasible [34].

Discrete-variable coding requires photon-counting techniques for which there are currently no reliable and cheap methods. Therefore continuous-variable coding, as a more practical and promising alternative is extensively studied. However these systems were considered unsuitable for long-distance communication, in 2012 a french team successfully demonstrated CV QKD over 80km of optical fibre [35]. In free-space a japanese team has demonstrated quantum key distribution using four coherent states over 5 meters with pulsed diode laser and a pulsed homodyne detector [36]. There have been also studies to examine the effects of atmosphere on the laser beam propagation and to gain knowledge of the transfer characteristics of the medium [37]. The results show that the received beam diameter, shape and phase is significantly distorted while also beam intensity fluctuations are introduced over a 145 km path. Despite DV communication can currently reach longer distances is free-space, CV communication using homodyne detection instead of photon counting techniques is definitely promising for long-range free-space QKD [38].

4 Satellite-to-satellite CV QKD simulation

CV QKD has several advantages over DV QKD in practical free-space communication. Qubits are generated by single photon sources in DV QKD which appear to be really expensive yet and do not guarantee truly single photons. With a given probability, these sources may produce two or more photons that makes the QKD process vulnerable to attacks like photon number splitting. However CV QKD sources operate with weak coherent laser pulses which are more appropriate for practical use.

Also, in DV QKD the the photons are detected with photon counters which does not appear to be reliable enough. Photon counters are very sensitive to background light sources and also produce dark counts which are false county without any incident light. CV QKD implementations use homodyne detection method, sending a weak signal pulse and a strong local oscillator (LO) pulse. The homodyne detector filters the received light and detects photons only with the same frequency as the LO. This technique makes CV QKD much more resilient to background noise.

Also, CV QKD is compatible with Dense Wavelength Division Multiplexing (DWDM) which means a single optical channel can be used by multiple users that could not be achieved with DV QKD. Additionally, this makes CV QKD compatible with most standard telecommunication optical networks [35].

In CV QKD, we need both a quantum and a classical channel between Alice and Bob. For the classical channel, the satellite has to be equipped with any regular radio wave transmitter and receiver. For the quantum channel, a pulsed laser diode, amplitude and phase modulators are required to generate the photons and a homodyne detector with a phase modulator are required to measure the photon beams.

To connect Alice's and Bob's apparatus, a line of sight is required between the satellites and the devices have to be able to aim to the other satellite. Therefore precise tracking mechanisms, distance and velocity measurements are required. Since CV QKD relies on intense post-processing and calculations, super fast data processing units (FPGA cards) are also required. Furthermore, to predict the amplitude, phase and beam diameter distortion caused by background noise, an eavesdropper or atmosphere an accurate channel model has to be developed. Even the spacetime curvature affects the photon propagation which has to be taken into account when developing the channel model [31].

5 Global QKD network

Let’s assume that Alice and Bob are two communicating parties, who wish to establish a secret key with entangled pairs of photons using a global satellite network. In this case, the satellites could be used in several different ways to provide a secure quantum key distribution [22].

For example, Alice can generate the entangled pairs of photons and send one photon from each pair to Bob, using a satellite as a relay (Fig. 7). In this scenario, the satellite is an untrusted node with the sole task to forward the photon without disturbing the quantum state. During the communication, the path of the photons is very long and contains both uplink and downlink, which significantly distorts the photon polarisation.

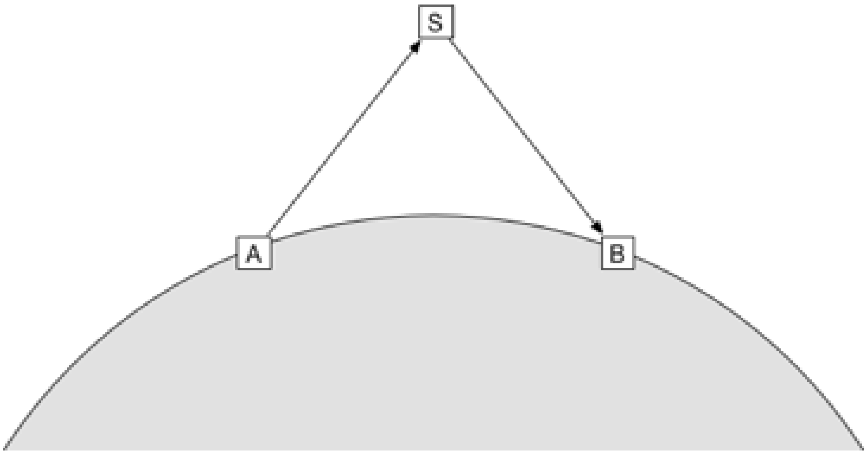

Figure 7: The *S* satellite acts as an untrusted relay and forwards the photons received from *A* ground station to *B* ground station without disturbing the quantum state.

The satellite could also be used as a trusted node, when it independently establishes individual keys with Alice and Bob (Fig. 8). Then the satellite broadcasts a combination of the two keys, from which Alice and Bob can extract each other’s key. In this case, the path of the photons is much shorter. Also, since this setup requires only one link at a time, this allows key distribution between two parties located anywhere on Earth, however, it still contains both uplink and downlink paths.

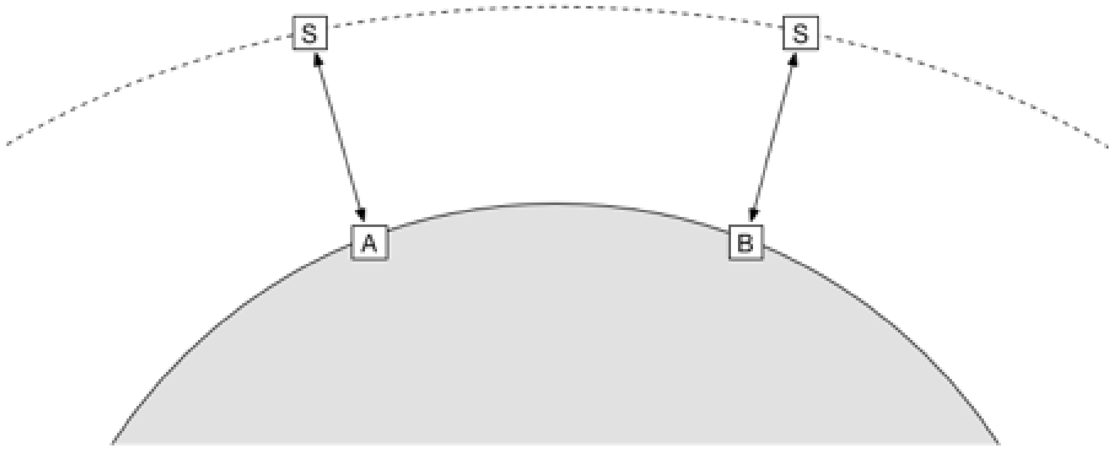

Figure 8: The S satellite acts as a trusted node and first it establishes a key with A station, then later with B station. This solution does not require simultaneous line of sight between the stations and the satellite, so a larger area can be covered, however the B station has to wait for the satellite to arrive.

The solution proposed in this paper utilizes the satellite as a trusted node. In this scenario, the satellite is used to generate entangled pairs of photons, then sends one-one photons of each pair to Alice and Bob, respectively. The range covered by the satellite can be extended by using other satellites as mirrors.

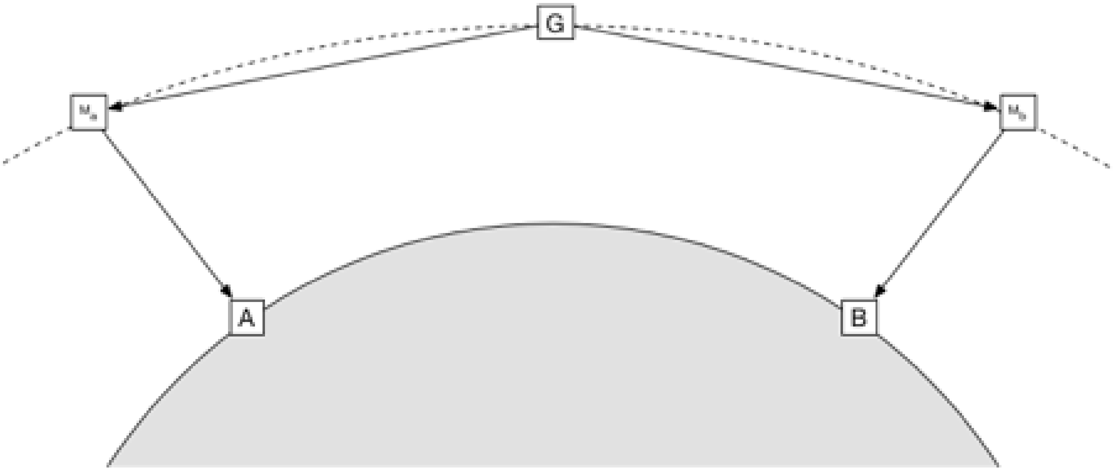

Figure 9: G satellite generates the entangled pairs and sends one photon of each pair to A and B ground stations. The range is extended with M_a and M_b mirrors. If the links between the generator and the mirrors are above the atmosphere, a significant amount of distortion can be avoided.

To simplify the calculations, I have assumed that the generator and the two mirrors are on the same orbit. And as stated before, the orbital plane is ekvivalent to the plane of the equator.

5.1 Maximum distance between satellites

To be able to simulate such a network, it is important to know the maximum distance between the generator and the mirrors. More generally, since quantum communication utilizes photon beams, two communicating satellites have to have a line-of-sight (LOS) on each other and should not be blocked by the Earth. Furthermore, the laser beam should not pass through the atmosphere because it would be greatly distorted.

Therefore we should determine a maximum distance between the communicating satellites which is not trivial since the velocities and therefore the distance between the satellites are continuously changing during their orbit.

For this reason, I have calculated the maximum distance between the two communicating satellites when they are closest to the perigee and also equal distance from the perigee. This is also the worst case scenario, when the satellites are closest to each other and also the laser beam between the two satellites is travelling closest to the atmosphere.

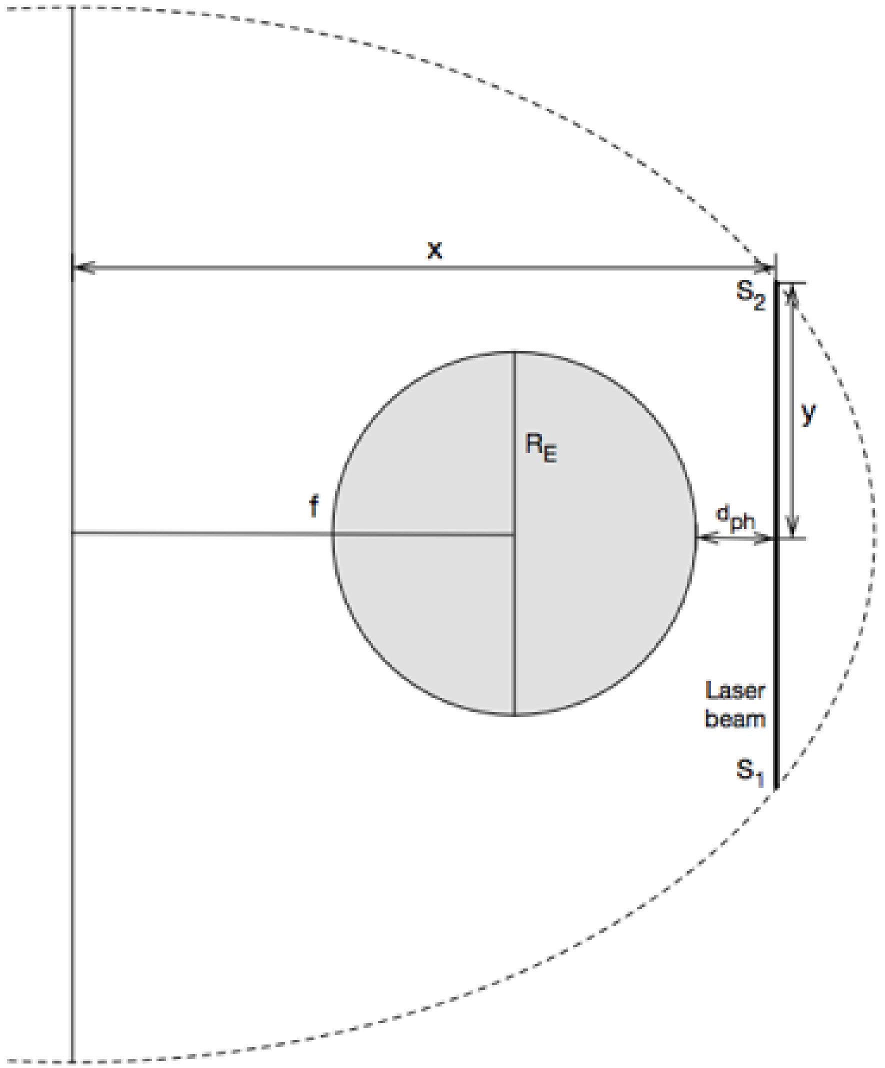

Figure 10: S_1 **and** S_2 **are two communicating satellites with a laser beam between them. They are equal distance from the perigee. The Cartesian coordinates of a satellite (x and y) can be calculated from the equation of the ellipse. The distance between the laser beam and the surface of the Earth is** d_{ph} **, the radius of the Earth is** R_E **and the focus distance is** f

Given the parameters that identify an orbit, we can calculate the maximum allowed distance between two satellites when the laser beam does not pass through the atmosphere.

Expressing the y value from the equation of the ellipse we get:

$$(5) \qquad \left(\tfrac{x}{a}\right)^2 + \left(\tfrac{y}{b}\right)^2 = 1 \rightarrow |y| = \sqrt{b^2 \cdot \left(1 - \left(\tfrac{x}{a}\right)^2\right)} \ .$$

From this equation, we can calculate the *y* coordinate when the *x* coordinate of the satellite is known.

The worst scenario, when the photons travel closest to the Earth is when the two satellites are at equal distance from the periapsis and between the Earth and the periapsis.

In this case, the x coordinate equals to the sum of the distance from the center (f), the radius of the Earth (R_E) and the allowed minimum distance between the surface of the Earth and a travelling photon (d_{ph})

$$(6) \qquad x = f + R_E + d_{ph} \quad .$$

Using the calculated x coordinate with the previous equation, the *y* coordinate can be calcualted. Then the maximum distance between the satellites when they are equally distant from the perigee is twice the *y* coordinate.

5.2 Rotation of quantum basis states

While the moving satellites generate and reflect the entangled pairs of photons, the basis states of the received qubits may be rotated in reference to what the basis states were on the generating satellite. The angular velocity of this rotation depends on the location of the ground station, the attributes of the mirror and the generator. The aim is that, we want to be able to calculate the received qubit's angle of rotation knowing the attributes of the ground station and the satellites.

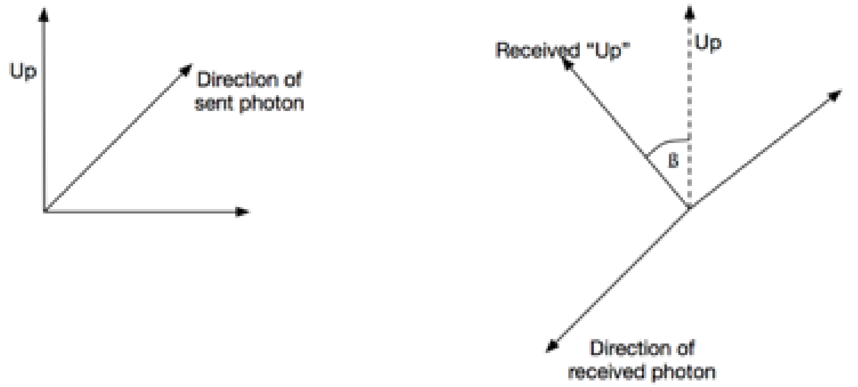

Figure 11: The left figure shows the basis states when they are generated. G chose the "up" base which points to the North, sends the photon to the mirror and the third base is the cross product of these two. The right figure shows the received photon from the perspective of the ground station. The received "up" vector has been rotated during the reflection and the angle of the rotation

depends on the velocity of the generator and the mirror and the position of the ground station as well. We have to calculate the angle in order to correct the rotated "up" vector.

I have used a Cartesian coordinate system during these calculations with the center of Earth as the origo. I have also assumed that the equatorial plane is the orbital plane and the vernal point is where the prime meridian passes the orbital plane.

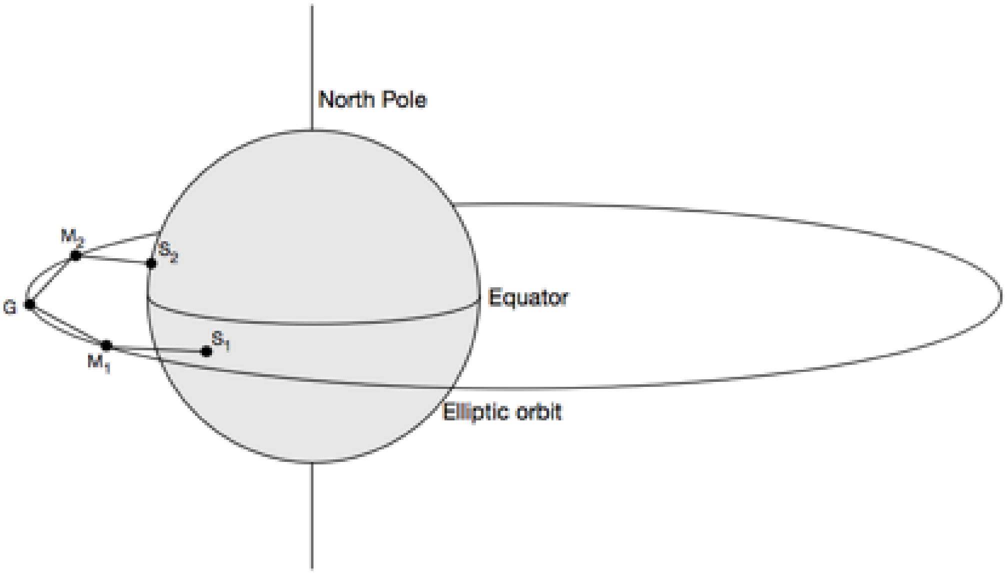

Figure 12: G is the generator satellite, M_1 and M_2 are the mirror satellites, S_1 and S_2 are the ground stations on the surface of Earth. The perigee is equal to the vernal point which is at the prime meridian (the 0 longitude on Earth)

First we have to calculate the normal to the surface of the mirror satellites which will be used to reflect the qubits. Since we would like to reflect the photon beam from the generator to the stations on Earth, we can calculate the normal to the surface of the mirrors from the positions of the ground stations, the generator and the mirrors. According to the law of reflection, the incident ray, the reflected ray and the normal to the surface of the mirror all lie on the same plane. Also, the angle of reflection is equal to the angle of incidence.

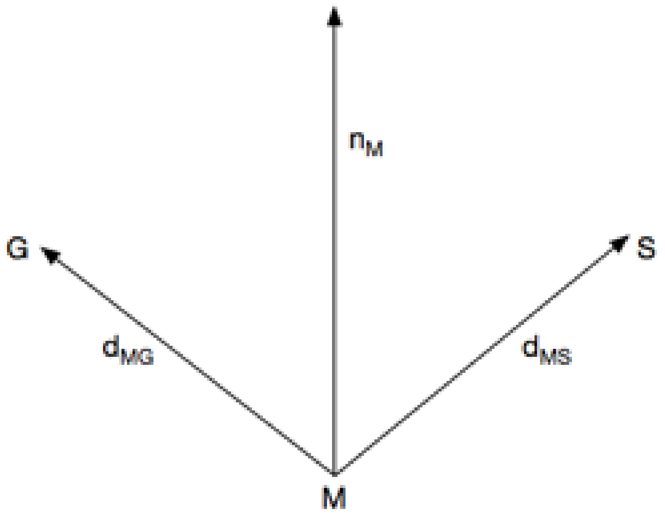

Figure 13: $\bar{n}_M$ is the normal to the surface of M mirror which can be calculated from the directional vectors pointing from the mirror toward G generator ($\bar{d}_{MG}$) and the S ground station ($\bar{d}_{MS}$). The directional vectors and the normal vector have to be normalized.

Assuming that all of the vectors are normalized and have a length of 1, we can write the following equations:

$$(7) \qquad \bar{n}_{M_1}=\bar{d}_{M_1G}+\bar{d}_{M_1S_1}$$
$$\bar{n}_{M_2}=\bar{d}_{M_2G}+\bar{d}_{M_2S_2}$$

where

$\bar{d}_{M_1G}$ and $\bar{d}_{M_2G}$ are the normalized direction vectors pointing from the mirrors towards the generator,

$\bar{d}_{M_1S_1}$ and $\bar{d}_{M_2S_2}$ are the normalized direction vectors pointing from the mirrors towards the ground stations,

$\bar{n}_{M_2}$ and $\bar{n}_{M_2}$ are the normals to the surfaces of the mirrors, which have to be normalized.

When the normals to the mirrors' surfaces are known, we have to decide the basis of the quantum states. I have assumed that the basis states includes an "up" vector which points to the North, the travel direction of the photon *(which is the generator-mirror direction)* and the cross product of these two. However, these bases can be arbitrary vectors which are perpendicular to each other.

After we have chosen our basis, these basis can be represented as 3 perpendicular vectors which have to be reflected on the mirrors using the law of reflection. This gives us the reflected basis vectors:

$$(8) \qquad \bar{b}_x{}' = \bar{b}_x - 2(\bar{b}_x \;\; \bar{n}_M)\bar{n}_M$$

where $\bar{b}_x{}'$ is a reflected basis state *(x stands for one of the three vectors)*, $\bar{b}_x$ is the original basis state and $\bar{n}_M$ is the normal of the mirror where the reflection occures.

When the reflected basis states (which will be received by the ground stations) are known, we have to determine the direction of the original "up" vector which is visible from the ground station looking towards the mirror. This is a simple vector pointing to the North Pole and have the same inclination and right angle as the incoming photon's direction vector.

If both the original "up" vector of the ground station and the received "up" vector are known, we can easily calculate the angle between the two vectors using the following equation:

$$(9) \qquad cos(\theta) = \frac{\bar{a} \cdot \bar{b}}{|\bar{a}| \; |\bar{b}|}$$

where the two "up" vectors are $\bar{a}$ and $\bar{b}$ and $|\bar{a}| = \sqrt{a_x^2 + a_y^2 + a_z^2}$ is the magnitude of the vector. Using the inverse cosine function we can determine the θ angle which is the angle of rotation of the quantum basis states.

The equations 7, 8 and 9 give us the angle of rotation at given satellites positions. Using numerical analysis with very small position changes, we can calculate the angles at different satellite positions. For this we have to introduce a small t and calculate the positions of the satellites at every t time.

As the initial position of the satellites and the parameters of the orbit are assumed to be known, we can calculate the velocity of the satellites. From these we can calculate the position of the satellite after t time:

$$(10) \qquad S' = S + \bar{v} * \;\; t$$

where S' is the new position of the satellite S after t while travelling with $\bar{v}$ velocity

At the new position we also have to recalculate the distance between the orbiting bodies and the new direction/magnitude of the velocity.

By choosing a sufficiently small t and using the equations 7,8,9,10 one after another to calculate the positions after every elapsed t , we can calculate the angle of rotation for every specified time and position. From the calculated data we can also calculate the difference between two angles at two specific times, which gives us the angular velocity of the rotating quantum state basis and shows how fast the basis are rotating.

6 Data analysis and results

I have also ran simulation using the methods and equations described in the previous chapter. For this purpose, I have developed a custom application using Python language utilizing OpenGL for 3D graphics using the PyCharm Community Edition integrated development environment from JetBrains. The results of these simulations and the analysis of the calculated results are described in this section.

6.1 Maximum distance between satellites

Using the equations described above, I have calculated the maximum distance between the satellites where they are both closest to the perigee with different orbital heights. For the minimum distance between the laser beam and the surface of Earth, I have decided to use 100km which is the altitude of the Karman line, the boundary between the Earth's atmosphere and outer space. Below this altitude, the photon beam may be significantly distorted by atmospheric effects. For the eccentricity of the orbit, I chose $6.677\ 10^{-4}$ which is approximately the eccentricity of the International Space Station's (ISS) orbit.

Altitude of orbit at perigee	Satellite distance
400 km	3987.6 km
800 km	6182.5 km
1200 km	7863.1 km
1600 km	9312.1 km
2000 km	10624.6 km

Table 3: The calculated distance values at specific satellite altitudes for an orbit with $6.677\ 10^{-4}$ eccentricity.

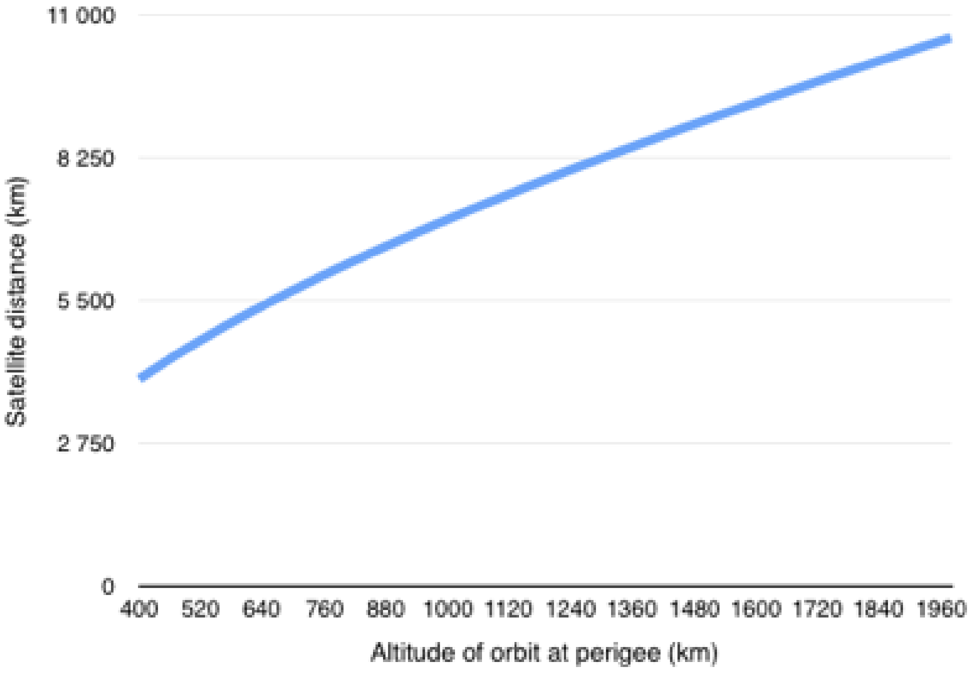

Figure 14: The line chart shows the required minimum satellite distances at different altitudes for an orbit with $6.677\ 10^{-4}$ eccentricity.

From Table 3, the values read that if the altitude of the satellites at the perigee is 400km, the distance between two communicating satellites can not be more than 3987.6km when they are both equal distance and closest to the perigee. If they are further away, we have to take into account that the photon beam, used during the quantum communication, may be distorted by the atmosphere or even blocked by the Earth at extreme satellite distances.

For the next simulation, I chose a larger 0.2 eccentricity for the orbit to see how the values change, as it is summarized in Table 4.

Altitude of orbit at perigee	Satellite distance
400 km	4376.6 km
800 km	6804.9 km
1200 km	8677.7 km
1600 km	10302.5 km
2000 km	11782.3 km

Table 4: The calculated distance values at different satellite altitudes for an orbit with 0.2 eccentricity.

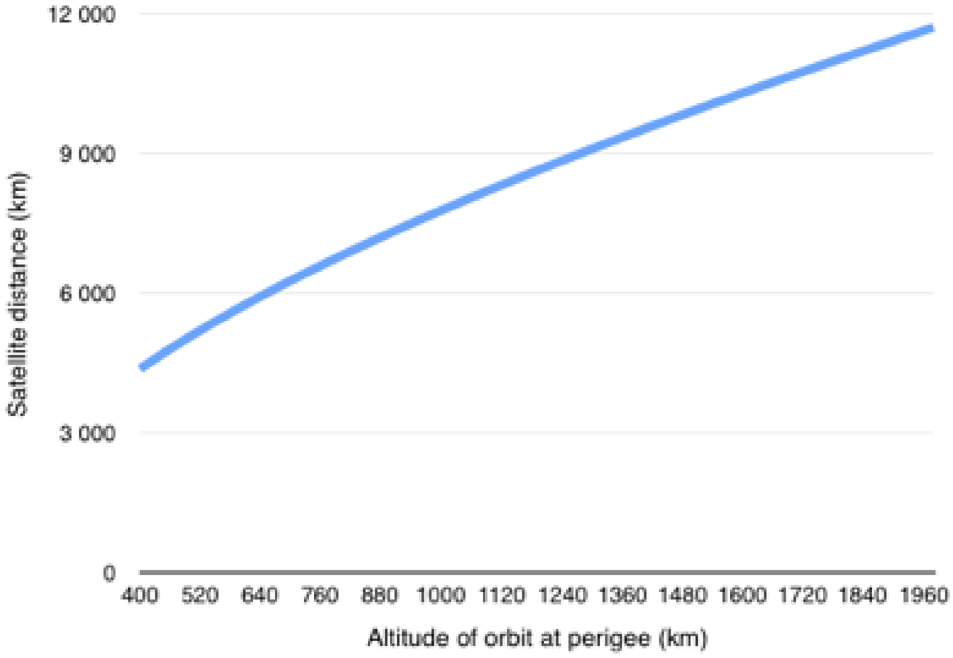

Figure 15: The line chart shows the required minimum satellite distances at different altitudes for an orbit with 0.2 eccentricity.

Comparing the values it is visible, that the allowed maximum distance between the satellites is more if the orbit has a bigger eccentricity.

During the following simulations I have set the parameters using these results, so that the laser beam between two communicating satellites may not reach the atmosphere.

6.2 Rotation of quantum basis states

To simulate the rotation of the quantum basis states, I have used $6.677\ 10^{-4}$ as the eccentricity of the orbit and 400km as the altitude of the satellites at the perigee, which are similar to the attributes of the International Space Station.

In this scenario (see Fig. 12), the initial longitude of the generator, as viewed from the Earth is 3° to the east, M2 mirror is 18° to the east and M1 mirror is 12° to the west. The satellites are orbiting to the west.

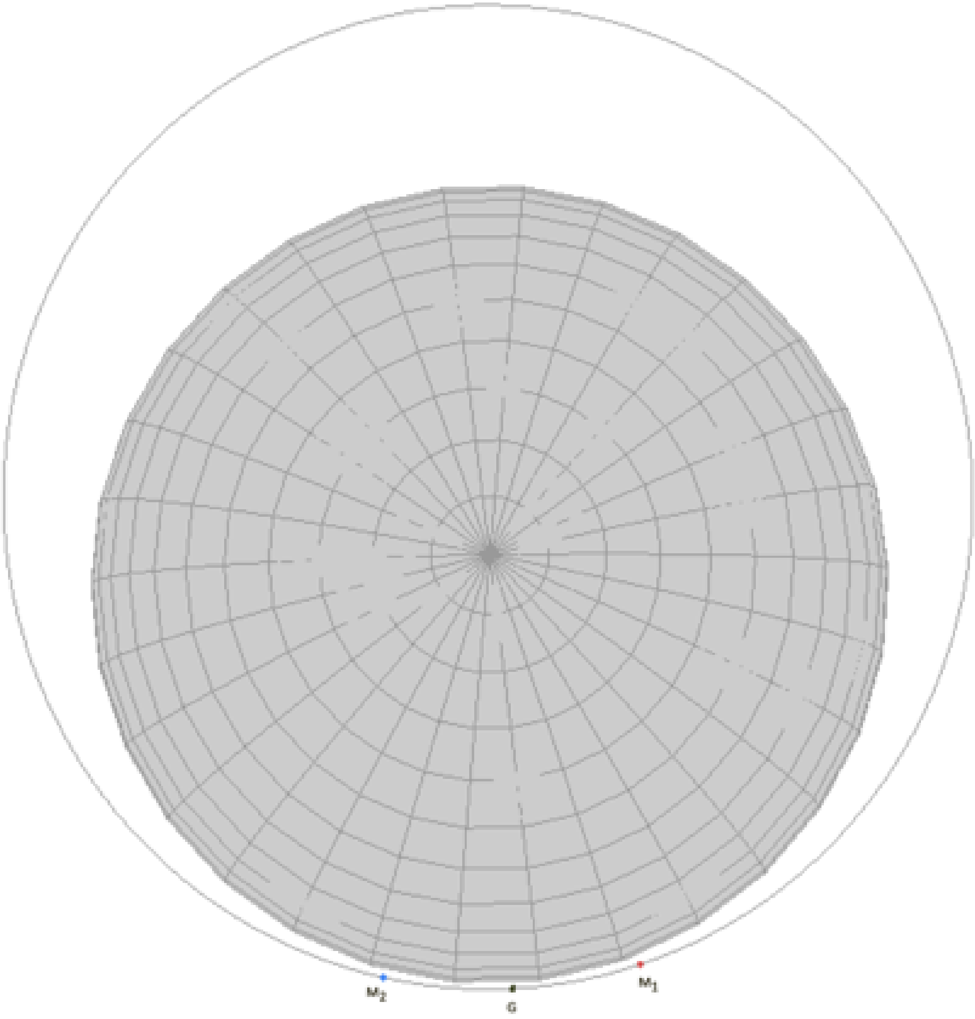

Figure 16: the simulated orbit viewed from the north. The satellites on the figure from left to right are M_2 , G and M_1

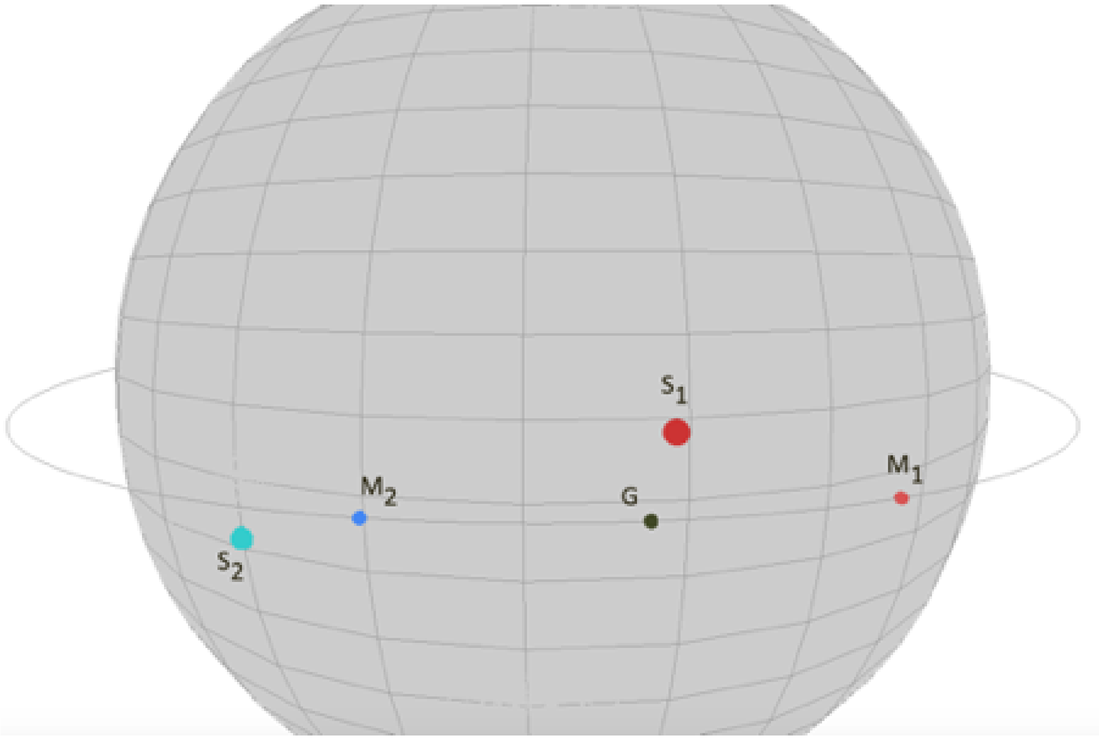

Figure 17: S1 ground station has been placed on the northern hemisphere at 5° latitude, 5° longitude. S2 ground station is located on the southern hemisphere at -5° latitude, -30° longitude.

The ground stations are configured, so that they can establish a quantum channel with a satellite only if the zenith angle is smaller than 60°. If the zenith angle is larger than 60°, the laser beam would have to travel across much more atmosphere which would cause great distortion.

The calculations mentioned before (moving the satellites, recalculating the velocity and distance from the center of Earth, recalculating the rotation of the basis states) are repeated at very small time intervals.

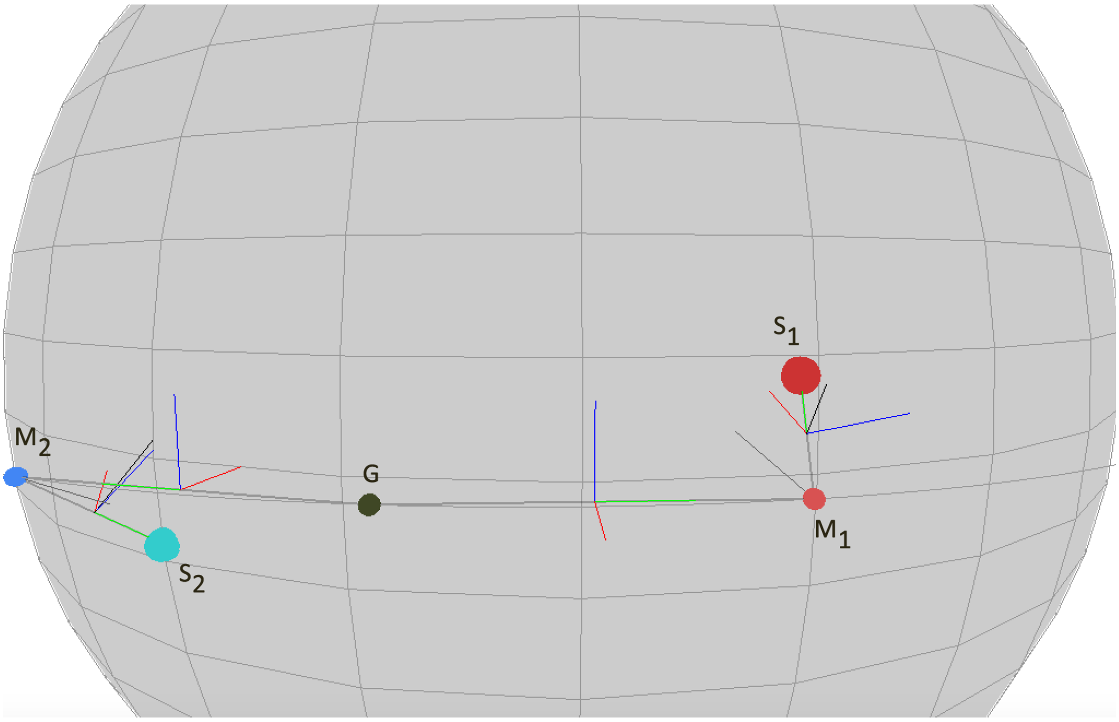

Figure 18: the satellites are visible from the ground stations under 60° Zenith angle, so an active quantum communication is possible. The lines connecting the satellites and the stations indicate a quantum communication. The three vectors in the middle of these lines indicate the basis states and the blue vector means the "up" vector. On the mirror-ground station connections the black line indicates the true "up" vector which is visible from the ground station's perspective. The difference between this black "up" vector and the received "up" vector is the angle of rotation.

As a result of the simulation it is clear, that the basis states are rotated when received by the ground stations. The moving satellites cause this rotation to continuously change during the communication and for this rotation countermeasures have to be taken at the ground stations.

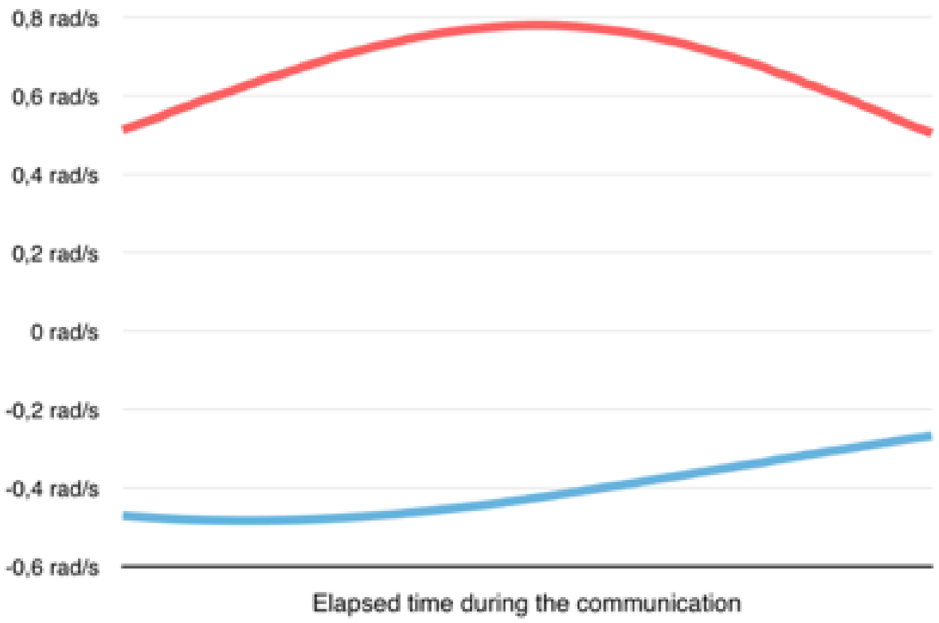

Figure 19: This line chart shows the required rotation during the simulated quantum communication. The S_2 base station (illustrated by the top, red line) had to rotate the bases at a rate of 0.5 rad/s but the speed of the rotation was the fastest when the M_2 satellite was the closest. The same is visible on the bottom, blue line which shows the speed of basis rotation at S_1 base station.

A negative speed of rotation means that the received “up” base is getting closer to the original “up” direction. On the northern hemisphere this means a counter clockwise rotation, while on the southern hemisphere it is the opposite.

These results clearly indicate that if the photons are generated or refelcted by a moving satellite, the received quantum basis states are possible rotated. That also means that even during a few seconds of communication the speed of this rotation changes in time, which has to be actively corrected as the photons are received.

7 Conclusion

In this TDK paper I have described the basic concepts of orbital mechanics, quantum communication and quantum key distribution. I have examined the current state-of-art of quantum key distribution and free-space quantum communication. I have proposed an entanglement based QKD satellite network using mirrors to increase the coverage. For this network I have calculated the maximum distance allowed between the satellites to minimize the atmospheric distortion of the transferred quantum states. I have also ran simulations to determine the rotation of the basis states which has to be corrected by the ground stations for the received photons.

8 References

[1] Simon Singh, “The Code Book”, Anchor Books (2000)

[2] D.Stucki et al, “High rate, long-distance quantum key distribution over 250km of ultra low loss fibers”, New J. Phys. 11 075003 (2009)

[3] N.Sangouard, C. Simon, H. Riedmatten, N. Gisin, “Quantum repeaters based on atomic ensembles and linear optics”, Rev.Mod.Phys.83, 33 (2009)

[4] H. Curtis, “Orbital Mechanics for Engineering Students”, Elsevier Butterwort-Heinemann (2005)

[5] S.Imre, F. Balázs, “Quantum Computing and Communications - An Engineering Approach”, Wiley (2004)

[6] A.Einstein, B.Podolsky, N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”, Phys. Rev. 47, 777 (1935)

[7] J.S.Bell, “Speakable and unspeakable in quantum mechanics”, Cambridge University Press (1987)

[8] A.Einstein to M.Born “The Born - Einstein Letters” (1971)

[9] W. K. Wootters, W.H.Zurek, “A single quantum cannot be cloned”, Nature 299, 802-803 (1982)

[10] A.R. Calderbank, P.W.Shor, “Good Quantum Error-Correcting Codes Exist”, Phys.Rev.A, Vol.54, No.2, pp.1098-1106 (1996)

[11] C. H. Bennett, G. Brassard. "Quantum cryptography: Public key distribution and coin tossing", “*Proceedings of IEEE International Conference on Computers, Systems and Signal Processing”*, volume 175, page 8. New York, 1984.

[12] C. H. Bennett “Quantum cryptography using any two nonorthogonal states”, Phys. Rev. Lett. 68, 3121, 25 May 1992

[13] A.K.Ekert, “Quantum cryptography based on Bell’s theorem”, Phys.Rev.Lett 67, 661 (1991)

[14] Hitesh Singh, D.L. Gupta, A.K.Singh, “Quantum Key Distribution Protocols: A Review”, IOSR-JCE Vol.16 (2014)

[15] F.Grosshans, “Continuous variable quantum cryptography using coherent states”, Phys. Rev. Lett. 88, 057902 (2002)

[16] Ch.Silberhorn, “Continuous Variable Quantum Cryptography - beating the 3 dB loss limit”, Phys. Rev. Lett. 89, 167901 (2002)

[17] H-K Lo, X.Ma, K.Chen, “Decoy State Quantum Key Distribution”, Phys. Rev. Lett. 94, 230504 (2005)

[18] National Security Agency of the United States, “Cryptography Today” published on www.nsa.gov (2015)

[19] D.Elser et al, “Satellite Quantum Communication via the Alphasat Laser Communication Terminal”, Int.Conf.on Space Opt. Sys. and Appl. (2015)

[20] C.Simon et al, “Entanglement over global distances via quantum repeaters with satellite links”, Phys.Rev.A 91, 052325 (2015)

[21] S. Nauerth et al, “Air to Ground Quantum Communication”, Nature vol.7 382-386 (2013)

[22] J-P.Bourgoin et al, “Free-space quantum key distribution to a moving receiver”,Opt.Express 23, 33437 (2015)

[23] J.Yin et al, “Experimental single-photon transmission from satellite to Earth” (2013)

[24] G.Vallone et al, “Experimental single photon exchange along a space link of 7000km”, Phys.Rev.A 93, 010301 (2016)

[25] J-P. Bourgoin, “Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations”, Phys.Rev.A 92, 052339 (2015)

[26] National Space Science Center of China, “China launches first-ever quantum communication satellite” published on english.nssc.cas.cn (2016)

[27] B.Qi et al, “Free-space reconfigurable quantum key distribution network”, IEEE ICSOS conference (2015)

[28] G.Vallone et al, “Quantum interference along satellite-ground channels” (2015)

[29] M.Lasota, R.Filip, V.C.Usenko, “Robustness of quantum key distribution with discrete and continuous variables to channel noise” (2016)

[30] L. Y. Xie, L. F. Wei, “Enhancing the detection probability of single waveguided-photon by cavity technique”, (2016)

[31] D.E.Bruschi et al, “Spacetime effects on satellite-based quantum communications”, Phys.Rev.D 90, 045041 (2014)

[32] B.Heim et al, “Atmospheric continuous-variable quantum communication” (2014)

[33] G.Vallone et al “Turbulence as a Resource for Quantum Key Distribution in Long Distance Free-Space Links”, Phys.Rev.A 91, 042320 (2015)

[34] X-M. Jin et al, “Towards quantum communication in free-space seawater” (2016)

[35] P. Jouguet et al “Experimental demonstration of long-distance continuous-variable quantum key distribution”, Nature Photonics 7, 378-381 (2012)

[36] S.Tokunaga, K. Shirasaki, T. Hirano “Free-space continuous-variable Quantum Cryptography”, CLEOE-IQEC conference (2007)

[37] A.L. Buck, “Effects of the Atmosphere on Laser Beam Propagation”, Applied Optics Vol.6 No.4 (1967)

[38] A.A.Semenov, “Homodyne detection for atmosphere channels”, Phys.Rev.A 85, 013826 (2012)