A report on
Decoy State Quantum Key Distribution

Indian Academy of Sciences' Summer Research Fellowship Program, 2017

Raman Research Institute

Ramanan Sekar
Summer Research Fellow
Guide: Dr.Urbasi Sinha
July 21st, 2017

Abstract

Ever since Bennett and Brassard introduced their quantum key distribution(QKD) scheme in 1984, the field of QKD has seen tremendous progress towards commercialization. Unlike classical cryptographic schemes, QKD, a sub-topic of quantum cryptography, stands strong in its security only bounded by the laws of physics, meaning no matter how advanced the technology gets, what is prohibited will be prohibited. However, the original BB84 saw some downfalls when practical sources are considered, resulting in poor secure key generation rates. The idea of decoy state QKD was proposed to improve the status quo, and has since enjoyed considerable attention and significant importance bequeathed upon it. This report basically tracks the fundamentals of BB84 and its problems, how the decoy state idea proved to be a worthy solution to them, along with some mathematical background and information about the details of the decoy state idea, and two important experimental milestones are also discussed.

Acknowledgements

I thank Dr.Urbasi Sinha and the Indian Academy of Sciences for giving me this opportunity to learn so much about research. This experience widened my perspective and introduced me to new aspects of science and research that I had not encountered before thereby imbibing me with inspiration and optimism. I also thank Rishab Chatterjee for all those long hours in the library discussing about the literature. I thank Kaushik Joarder and Ashutosh Singh for helping me understand all the subtle and important experimental details. I finally thank Sudipta Dash for sticking around with me for 8 weeks and being a partner in learning about quantum information.

Contents

1 Introduction

The interesting dynamic between transparency and secrecy has always been an integral part of the human experience. The fundamental role that secrecy plays to determine an individuals personal relationships to the rise and fall of countries is evident when a survey of history is taken. Julius Caesar famously used the eponymously named Caesar cipher to communicate military information so that his opponents don't have an idea of what strategies are being adopted. Similarly, in a more recent timeline, the Germans used the Enigma machine to encrypt information to communicate messages to their troops in World War 2 and it was only through breaking the Enigma code that the British were able to subdue the German forces.

It quickly becomes clear that the entire field of cryptography, made rigorous by Shannon by the burgeoning field of classical information theory, is essential to both strengthen oneself with the secrecy of information and to weaken an opponent by exploiting the loopholes in the cryptographic methods. Generally speaking, cryptography is the process of scrambling a piece of information in a very specific way so as to not have an adversary gain the knowledge of the information but such that the party to which the information is to be delivered to is able to decode the scrambled message to obtain the actual message. The process of scrambling a message through a specific process is known as encryption, and the reverse process of getting back the original information is known as decryption. Cryptography can be divided into two parts, namely Asymmetrical cryptosystems and Symmetrical cryptosystems [1], and the distinction lies with the crucial object known as the key. They key functions as the physical key, which is used to lock objects, in this case actual messages, and also to unlock objects, in this case encrypted messages. The traditional lock and key arrangement where a single key is used to lock a particular box and only that specific key can be used to unlock that very same box is called symmetric key cryptography. Here, a message is encoded with a key, and the receiver has the same key, only with which, the message can be decoded. The domain where two separate keys exist, one for encoding and the other for decoding, is called asymmetric key cryptography.

Modern cryptographic protocols such as the RSA encryption system, which is a form of asymmetric cryptographic system, has a security that has been relied upon to communicate bank account pin numbers, online transactions, and so on. However, the security of such systems primarily depend on the computational complexity of the problem and not on any unconditional limitation of an eavesdropper who is trying to extract the secret message. For example, the RSA encryption scheme's security relies on the fact that is easy to multiply two large prime numbers than to factorize a specific large number into two prime factors. It is true that current supercomputers would take years to decode a message with the practical limitations posed by the RSA scheme, however, as the prowess and capabilities of technology evolves exponentially on a daily basis, it is possible that in the near future, a computer could be invented which is able to factor a number into its prime factors much faster than what current computers can do. For instance, the advent of quantum computers poses a threat to the security of the RSA scheme [2] due to the exponential speedup obtained by using Shor's algorithm. As the proverbial saying goes, this necessity leads to the conclusion that a cryptographic scheme needs to be introduced the security of which is independent of the practical limitations on the technology of the times, and instead is dependent on the immutable and universal laws of physics, which will remain true regardless of the time and the technology. This leads us to the field of Quantum Cryptography.

Let us revisit the idea of keys in a cryptographic protocol. While they are admittedly a small part of a larger domain of secret communications, they are still vital to the functioning of any specific algorithm or protocol. In the symmetric key cryptography scheme, it is mandatory that both the parties engaging in secret communication have the same secret key. While troubles of security of encoded message are still looming questions, the primary question that pops up is one that is concerned with the distribution of the keys. Since the entire protocol would rely on the secrecy and security of the key, it is crucial to safely distribute the key between the two parties. The key needs to be distributed through a trusted messenger or a courier, and to ensure the security of either can turn out to be an intractable job, resulting in unintelligible yet significant loopholes than can be exploited by an adversary seeking to obtain the information. This process of secure key distribution, combined with the idea of using the laws of physics to dictate the security of communications, gave birth to the field of Quantum Key Distribution (QKD). Introduced first in 1984 by Bennett and Brassard [3], the field of study has bloomed from just theoretical undertakings to practical and commercial applications with guaranteed security that is essential for communication that is sensitive and classified information.

This report is an exploration of a very specific form of QKD, namely Decoy State QKD, and is organized as follows: after the introduction, details about the original protocol proposed by Bennett and Brassard, known as BB84, is presented. Furthermore, problems with this protocol is elaborated and the decoy state idea is introduced as a solution, and its facets are ironed out. Finally, few experimental implementations of the decoy state protocol is given.

2 BB84 protocol

2.1 Basic idea

The basic idea behind any QKD protocol relies with the nature of an entity with quantum mechanical properties. The fundamental mode of communication takes place using the qubit, which is a quantum superposition of a two state system, with particular states representing 0 and 1. The qubit $|\psi\rangle$ is given by

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$

where 'a' and 'b' are complex numbers, the modulus squared of which represents the probability of measuring the corresponding state. For setting up a QKD setup, consider two main parties, traditionally called Alice and Bob. Let the eavesdropper who listens in to the conversations be called Eve. A conventional QKD setup consists of a quantum channel and a classical channel. The quantum channel is used to transmit quantum information and the classical channel is used to convey regular information that will be used to generate final secret keys. As we are interested in testing the robustness of a protocol when an all powerful eavesdropper exists, we assume that Eve has access to both quantum and classical channel and that Eve must not deliberately contribute to the chatter occurring in both the channels. Due to the properties of quantum states, Eve cannot intercept an incoming qubit without disturbing its state, and furthermore, Eve also cannot make a copy of the incoming qubit due to the limitations posed by the no-cloning theorem. The fact that Eve inadvertently introduces an error in the qubits due to measuring them is the reason for the security of a QKD system, as the eavesdropper's presence can be easily detected.

2.2 The protocol

Coming back to the specific case of the BB84 protocol, as elaborated earlier, it consists of Alice and Bob having access to a quantum and a classical channel. Consider the quantum object used in this case to be the polarization states of a single photon. As shown in Figure 1, the states of polarization in the rectilinear basis are either horizontal or vertical, or it could be in the diagonal basis, either being in the 45° direction or in the 135° direction. Alice makes sure that all the other properties of the single photon are the same, such that the only degree of freedom left is the polarization. Hence, in any particular basis, either rectilinear or diagonal, the two orthogonal states are assigned a '0' or a '1'.

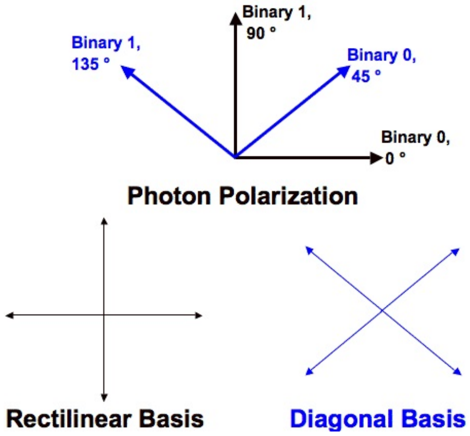
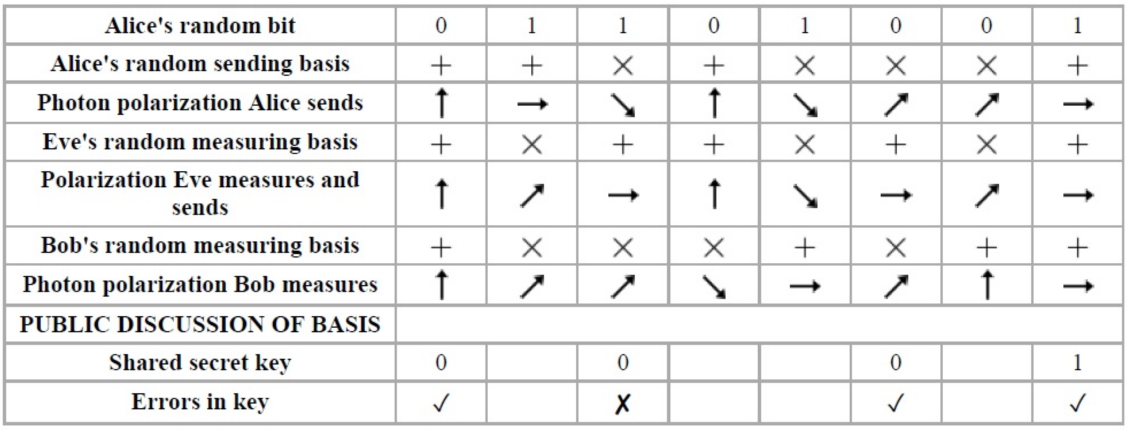


Figure 1: Polarization states, from [4]

Alice initially has two sets of binary strings, which is randomly arranged. The first string will be used by Alice to choose the basis, and the second string will be used as the bit to be used as the key, and the value of this bit will be encoded in the specific polarization state in the basis chosen earlier. Since all other properties except for the polarization are the same, this single photon effectively behaves as a qubit. Alice then sends this qubit through the quantum channel to Bob, who then receives it. Bob does not know the basis chosen by Alice, hence he randomly chooses either the rectilinear or the diagonal basis and performs a measurement on the single photon. If Bob had initially chosen the correct basis, the measurement he makes will give the right bit value that Alice sent. If on the other hand, Bob makes a wrong basis choice, he will be measuring the polarization state in an non-orthogonal basis, resulting in the probability of either getting the bit wrong or the bit right. Because the probabilities split into 50-50 event, this implies that Bob will have the right bit value for 75% of the time. After the transmission is over, Alice reads out her sequence of basis on the classical channel to Bob, and Bob simultaneously reads out his. They both discard the bits where they have used different basis, ensuring that ideally, they would both have a shared correct sequence of bits because using the same basis ensures having the same bit value.

2.3 Attacks and remedies

Consider now the role of Eve. Eve's powers are only limited by the laws of physics, and we award Eve the power to listen in on both the quantum and classical channel. Eve can perform an attack known as the intercept resend attack, which is a conventional attack where Eve intercepts an incoming qubit, measures it, and sends out an identical qubit to the one that she measured to Bob. The effects of this attack can be illustrated with the help of Figure 2, which contains an arbitrary sequence of bits generated by Alice in a particular basis, with Eve intercepting and resending it, and the final effect it has on Bob's measurement and bits. As stated earlier, the power of QKD lies with the fact that an eavesdropper invariably introduces some errors into the final sifted bits shared by Alice and Bob.



Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Eve's random measuring basis	+	×	+	+	×	+	×	+
Polarization Eve measures and sends	↑	↗	→	↑	↘	→	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↗	↘	→	↗	↑	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		0			0		1
Errors in key	✓		✗			✓		✓

Figure 2: Example detailing Eve's influence for a sample set of bits, from [5]

Just as Bob, Eve does not know the basis in which Alice sends and guesses it. The only events when Eve introduces errors is when Alice and Bob have measured in the same basis, but Eve has not. When Eve and Bob measure in the same basis as Alice, there are no errors introduced and Eve will gain information. However, if Eve measures in the wrong basis, having a probability of 50%, and if Bob measures in the right basis sent by Alice, he will get a random result with a probability of 50%, and the probability that this will result in a mismatch of bit values is the product, which is 25%. Hence, as shown in the figure above, we see that one among the 4 shared sifted bits has introduced an error.

To combat this, after basis reconciliation, Alice and Bob sacrifice a specific number of bits and compute the quantum bit error rate (QBER), which denotes the error rate in Bob's bits when both have the same basis. If this value exceeds a certain limit, which in this case is 25%, they abort the protocol as they have identified the presence of an eavesdropper. If it doesn't exceed, they continue with the protocol and perform classical error correction on the shared bits. This will reduce the errors, ideally, to zero. To further reduce the amount of information than a hypothetical eavesdropper might have, they also perform a procedure called privacy amplification. After all this is done, they will be sure that they have a shared secret key that can be used alongside any classical cryptographic protocol.

2.4 Practical problems

A typical experimental setup for implementing the original BB84 protocol using polarization states is shown in Figure 3, taken from [1]. The transmitter Alice consists of four laser diodes, each emitting coherent light with a specific polarization. This is attenuated to produce weak coherent states, where the average photon number is approximately 1. The light now obeys quantum mechanical properties. The laser diodes are chosen by a random number generator. The light is guided through a series of beam-splitters (BS) into an optical fiber. When this light reaches the receiving end at Bob, an initial polarization correction is made through half-wave plates accounting for polarization angle change while traveling through the fiber. The light is then sent through a 50:50 BS, which functions as the random basis selection for Bob. This is known as passive selection, as external interference is not necessary. When the light is in the rectilinear basis and the basis is selected right, the light is passed through a polarizing beam-splitter (PBS), where the horizontally polarized light is transmitted and vertically polarized light is reflected into the respective detectors. For the diagonally polarized light, when the basis is chosen right, an initial half-wave plate set at 22.5° ,thereby converting the light to the rectilinear basis and the same measurement process is carried out here too.

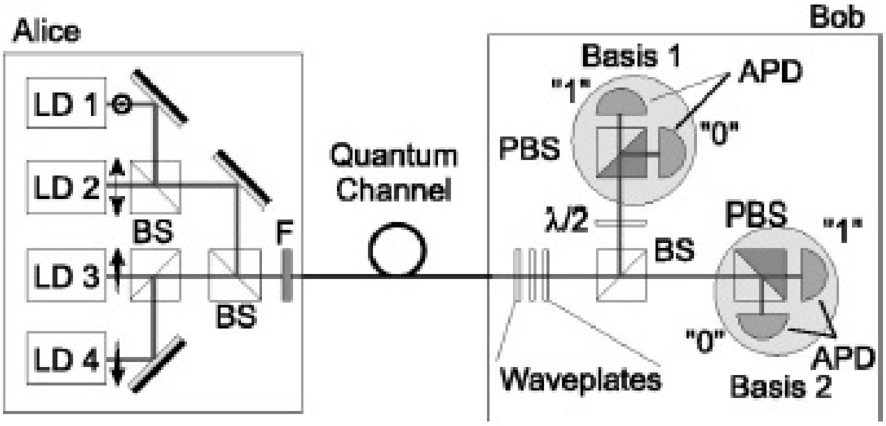


Figure 3: Experimental setup of BB84 protocol with polarization encoding

A glaring problem is evident when one closely observes the nature of the source. The original BB84 protocol ideally was proposed under the usage of single photons, however, ideal single photons are difficult to produce with conventional sources such as laser diodes. For a weak coherent state, the number of photons i in any particular signal follows a Poisson distribution with the probability of of i photons being in a signal given by $P_i = e^{-\mu}\mu^i/i!$, where μ is the average number of photons in a signal. Hence, any given signal if not attenuated properly will lead to the production of multiphoton signals, leaving way for Eve to exploit this fact. We bestow upon Eve the power to know the number of photons in any given signal. Eve can now block all single photon signals sent by Alice, and in the multiphoton signals, split it such that she keeps one for herself and sends the rest to Bob. Eve stores these photons. After the transmission, when Alice announces the basis on the classical channel, Eve then measures these photons in the corresponding basis, and now will have the entire information about the key that Alice and Bob now share. This attack is known as the photon number splitting (PNS) attack [6], and poses a threat to the unconditional security of BB84 due to practical constraints.

3 Secure key generation rate

The applicability of any given key distribution protocol is quantified by the secure key generation rate, which denotes the rate at which unconditionally secure keys can be generated between two parties. In order to understand the effects of practical limitations on the secure key generation rate, one needs to be acquainted with certain terminologies.

The yield Y_i is the conditional probability that Bob has a detection event given that Alice sends out i photons. This basically denotes the event that Bob has a ”click” in his detector, when Alice sends out that many number of photons. One can define the total gain Q_μ of the signal state as the weighted mean of the yields of all the number of photons, given by

$$Q_\mu = \sum_{i=0}^{\infty} Y_i P_i = \sum_{i=0}^{\infty} Q_i \tag{1}$$

where $Q_i = Y_i P_i$ are the individual gains and the definition of P_i follows from the previous section. One also needs to quantify the error rate. The error rate e_i of an i photon signal sent by Alice is the event that Bob's detection amounts to an error given that Alice sends out i photons. The total error associated with a detection event is the product that the i photon signal actually results in a detection event and that the detection event amounts to an error, which is basically the product of the yield and the error rate, given by $Y_i e_i$. If E_μ is taken to be the QBER of the signal state, the weighted mean of the total error is now given by

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} Y_i e_i P_i \tag{2}$$

Let η be the transmittance of the entire setup for a single photon, including the channel and Bob's detector efficiency. Then, $\eta_i = 1 - (1-\eta)^i$ is the transmittance of i photons. If Y_0 is the background event rate which consists of dark counts and detection due to stray light, then ideally, the yield Y_i can be expressed as

$$Y_i = Y_0 + \eta_i - Y_0 \eta_i \approx Y_0 + \eta_i \tag{3}$$

as both Y_0 and η_i are small, their product is even smaller. Similarly, the product of an error given a detection event $Y_i e_i$ is given by a product of probability of an error given a background event, and the probability of an error given there is a detection event but the error results from the detector

$$e_i Y_i = e_0 Y_0 + e_d \eta_i \tag{4}$$

where e_0 is assigned to be half as background events are random, and e_d is the error due to misalignment in the optics resulting in the wrong detector clicking. Although equations (3) and (4) represent ideal scenarios, they provide an opportunity to arrive at closed form expressions for the total gain and the QBER. Using (3) in (1), we get $Q_\mu = \sum_{i=0}^{\infty}(Y_0 + \eta_i)e^{-\mu}\mu^i/i!$, which on further simplification yields

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{5}$$

Going through similar steps by using (4) and (3) in (2), we arrive at an expression for QBER as

$$E_\mu Q_\mu = e_0 Y_0 + e_d(1 - e^{-\eta\mu}) \tag{6}$$

An analysis was made to arrive at the rate at which secure keys can be generated according to the practical BB84 protocol, by taking into consideration of imperfect sources producing multiphoton signals and also the information acquired by Eve throughout this entire process by [7], and they were able to use results from classical information theory and the consequences of classical post processing done with the sifted bits to get an expression for the lower bound of secure key generation rate R given in bits/signal state, as

$$R \geq q\left\{-Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)]\right\} \tag{7}$$

Here, Q_1 is the gain of the single photon signal as defined earlier, and denotes the event that a detection event is due to a single photon and e_1 denotes the error rate due to the single photon signal. H_2 here is the binary Shannon entropy, and denotes the amount of information gained or the amount of uncertainty in a particular information. It is said that the entropy in a given message is maximum when the all possible signals in the message are equally likely to occur. q here is the basis reconciliation factor and for the BB84 protocol, it is a half.

The inequality above contains several terms. The total gain and the QBER are experimentally measured quantities. For example, if C_μ is the number of counts of Bob for the signal state, and N_μ is the number of signal states sent by Alice,then the gain is just the ratio of the two quantities given by $Q_\mu = C_\mu/N_\mu$. For QBER calculation, one needs to sacrifice a specific portion of the signal states and then compare the bits of that portion, and determine the rate at which error creeps up. However, the gain of the single photon signal and the error rate of the single photon signal cannot be determined experimentally, as the source is a practical one and generates multiphoton signals randomly. Therefore, one needs to estimate both Q_1 and e_1. [7] went about this issue pessimistically, assuming that all multiphoton signals will be intercepted and split by Eve, when this certainly isn't the case practically. This condition would be given by $1 - (Q_1/Q_\mu) = p_{multi}/Q_\mu$, where p_{multi} is the probability that the signal emits a multiphoton signal. From this, one can also pessimistically estimate e_1 by taking it to approximately be the ratio of total QBER to the gain of the single photon state as $e_1 = (E_\mu Q_\mu)/Q_1$. Inserting these estimate into (7), one gets the key generation rate as

$$R \geq q\left\{-Q_\mu H_2(E_\mu) + Q_1[1 - H_2(\frac{E_\mu Q_\mu}{Q_1})]\right\} \tag{8}$$

For elucidating the scaling of the secure key generation rate as given by (8), one can make several simple assumptions. First, assume that $Y_0 \ll \eta$ and $\eta \ll 1$, and also since $\eta\mu \ll 1$, one can have a linear approximation of the exponential terms. By performing these approximations on (5) and (6), and inserting them into (8), and finding the derivative of R with respect to μ, one can find the optimal average photon number that maximizes this lower bound. Solving for μ in $\frac{dR}{d\mu} = 0$, one finds that $\mu \sim O(\eta)$. Since R scales as the product of η and μ, one finds that $R \sim O(\eta^2)$. This has dramatic implications. Firstly, we know that the transmittance is an exponentially decreasing function of the length of the channel. If the key generation rate scales as the square of the transmittance, the distance within which secure keys can be obtained is drastically reduced. Furthermore, due to pessimistic estimates, the lower bound of the secure key rate is further reduced. This effect compounds and produces only a very short distance and very low key rate of operation for the BB84 protocol considering the practical difficulties, and one needs to come up with a new way of tackling this problem in order to improve the current state of affairs.

4 Decoy State QKD

4.1 Basic idea

The idea of combating the PNS attack with something called the decoy state protocol came about in 2003, when Hwang in [6] proposed that one could, in addition to signal states, use something called decoy states in the protocol which would only be used to detect the eavesdropper and not used for generating keys. However, the security proof given by Hwang was not rigorous, as it involved a few assumptions regarding the average photon number. The complete details about the mathematical background and the security proofs were ironed out by [8],[9], and [10].

The birth of decoy state QKD came from the following necessities:

- In the original BB84 protocol, it was not possible to detect Eve attacking the protocol with a PNS attack, as Eve could optimize her attack so that the loss of information appeared as though the photons had been lost due to the attenuation of the channel

- The estimates for the secure key generation rate were overtly pessimistic as tighter estimates could not have been found with just using two experimental parameters

The crux of decoy state QKD is that in addition to using signal states which will be used for generating keys, Alice also sends Bob a certain fraction of decoy states. These decoy states will not be used for generating keys, but practically, will be used to detect the presence of the eavesdropper when Eve is attacking with the PNS attack. The decoy states has the exact same properties as that of the signal state except for different average photon numbers. All other properties of signal and decoy states are the same, including the wavelength, dispersion, polarization, etc. The only variable between the signal and decoy states is the different mean photon numbers, and as the source is probabilistic, anyone who intercepts the channel will not know whether a specific signal is a signal state or a decoy state. This is the power harnessed by decoy state QKD. Therefore, the decoy states are generated in the exact same way as the signal states, and they also have the four polarization states in case of polarization encoding, and they also travel through the same quantum channel.

In this protocol, Alice inserts in randomly a predetermined fraction of decoy states amid the signal states. Although the final ratio of signal to decoy states is known, where the signal and decoy states are introduced will not be known beforehand. The decoy state protocol permits the use of conventional hardware like laser diodes for transmission, meaning one of the attractive features of decoy state protocol is that it allows the usage of multiphoton signals. Eve on seeing any incoming signal will not know if it belongs to the signal state or the decoy state, and hence will devise an attack that attacks both signal and decoy states evenly. She performs a PNS attack and hence splits off a certain fraction of the photons and keeps it to herself, and sends the rest to Bob. An important and a logical assumption is introduced now. Since the individual yields Y_i and error rates e_i are only functions of the number of photons i, and since the signal and decoy states in theory have any number of photons in a given signal, we take the yields of the decoy states and yields of the signal states to be the same, and we also take the error rates of the decoy and signal state to also be the same, summarized as

$$\begin{aligned} Y_{i(d)} = Y_{i(s)} = Y_i, \\ e_{i(d)} = e_{i(s)} = e_i \end{aligned} \tag{9}$$

Because both the yields and the error rates are the same, one can mathematically estimate the lower bound of all the Y_is and the upper bound of all the e_is. This when introduced into the expressions for the gain and QBER, results in the lower bound for the gain Q_μ^L and the upper bound for the QBER E_μ^U. Since Eve is changing the number of photons, the yields and the error rates as experienced by Bob will also change. However, the individual yields and error rates are not experimentally measurable quantities, but as we have seen, their cumulative effect will be felt on the lower bound of the total gain and the upper bound of the QBER. Hence, when Eve attacks, the yields and error rates will change, which in turn violates the bounds dictated earlier through estimation.

After the transmittance of signal and decoy states is over, Alice now reads out the sequence in which she sent the signal and decoy states, and Bob assigns his detection events as either signal or decoy states, and they both calculate the gains and error rates. If Eve has meddled with the signal in any way, Alice through her calculation will find out the violation of the bounds of the error rate and gains, thereby giving away the presence of Eve. Alice and Bob now abort the protocol.

If the gains and error rates are within the bounds, they carry on with the protocol. It doesn't mean that Eve isn't there, but that the interference of Eve is negligible and that secure keys can be generated within the distance that they are working in. After reading out the sequence, Alice now proceeds with the original BB84 protocol, as in reading out the sequence of basis in the classical channel and the protocol continues forward as described earlier. To figure out the lower bound of the secure key generation rate that they are entitled to, they once again need to estimate single photon gains and error rates. This issue is also solved by decoy state QKD, as the mathematical setup of the entire problem will lead to tighter estimates of the required quantities, thereby improving the value of the key rate. We will also see that using decoy state QKD also increases the distance of operation by changing the scaling of the key rate with the transmittance.

4.2 Two decoy state protocol

The two decoy state protocol is a form of decoy state QKD where the number of decoy states used is two, and is mathematically constructed in [9]. Let us say that the signal state and the two decoy states have an average photon number given by μ, ν_1 and ν_2 respectively, according to the condition that $\nu_1 + \nu_2 < 1$ and $\nu_1 + \nu_2 < \mu$ and also that $\nu_2 < \nu_1$ The gains and QBERs associated with the signal and decoy states is given by

$$\begin{aligned} Q_\mu = \sum_{i=0}^{\infty} Y_i e^{-\mu} \mu^i / i!, E_\mu Q_\mu = \sum_{i=0}^{\infty} Y_i e_i e^{-\mu} \mu^i / i!, \\ Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i e^{-\nu_1} \nu_1^i / i!, E_{\nu_1} Q_{\nu_1} = \sum_{i=0}^{\infty} Y_i e_i e^{-\nu_1} \nu_1^i / i!, \\ Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i e^{-\nu_2} \nu_2^i / i!, E_{\nu_2} Q_{\nu_2} = \sum_{i=0}^{\infty} Y_i e_i e^{-\nu_2} \nu_2^i / i! \end{aligned} \tag{10}$$

First, we aim to estimate the lower bound of the background event yield Y_0. To do so, take Q_{ν_1} and Q_{ν_2} and multiply it by the exponentials of the other average photon number and subtract them, resulting in

$$\begin{aligned} \nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1} \leq (\nu_1 - \nu_2) Y_0, \\ \Rightarrow Y_0 \geq Y_0^L = \frac{\nu_1 Q_{\nu_2} e^{\nu_2} - \nu_2 Q_{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2} \end{aligned} \tag{11}$$

This lower bound Y_0^L can be used for further determining the lower bound of the single photon yield Y_1. To do so, consider the rearranged expression $\sum_{i=0}^{\infty} Y_i \mu^i / i! = Q_\mu e^\mu - Y_0 - Y_1 \mu$. Once again, using the expressions for gains from decoy states, we have

$$\begin{aligned} Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} &= (\nu_1 - \nu_2) Y_1 + \sum_{i=2}^{\infty} Y_i \frac{(\nu_1^i - \nu_2^i)}{i!}, \\ &\leq (\nu_1 - \nu_2) Y_1 + \frac{\nu_1^2 - \nu_2^2}{\mu^2} \sum_{i=2}^{\infty} Y_i \frac{\mu^i}{i!}, \\ &\leq (\nu_1 - \nu_2) Y_1 + \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_\mu e^\mu - Y_0^L - Y_1 \mu), \\ \Rightarrow Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu_1 - \mu\nu_2 - \nu_1^2 + \nu_2^2} & (Q_{\nu_1} e^{\nu_1} - Q_{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu^2} (Q_\mu e^\mu - Y_0^L)) \end{aligned} \tag{12}$$

Here we have used a mathematical inequality that says that $a^i - b^i \leq a^2 - b^2$ whenever $0 < a+b < 1$ and $i \geq 2$. The last expression is the lower bound of the single photon yield, and the lower bound of the gain of the single photon signal state is given by $Q_1^L = Y_1^L e^{-\mu} \mu$.

Similarly, we can calculate the upper bound of the single photon error rate by using the expressions for the QBER of decoy states and the final result is

$$e_1 \leq e_1^U = \frac{E_{\nu_1} Q_{\nu_1} e^{\nu_1} - E_{\nu_2} Q_{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_1^L} \tag{13}$$

Now we have all the necessary estimates of the upper bound of the single photon error rate and the lower bound of the single photon gain. While these estimates are quite tight and do provide an accurate lower bound of the key generation rate, one can debate about the values of the average photon numbers of the decoy state and explore the optimal choice of the average photon numbers.

The vacuum+weak decoy state protocol is said to be the optimal two decoy state protocol. The vacuum state essentially means that $\nu_2 = 0$, or that Alice simply doesn't send any signal. The weak decoy state is one which has an average photon number much smaller than the mean photon number of the signal state. This particular combination is the one that is most exploited and made use of in practical implementations of decoy state QKD. One can also have infinite decoy states, which is termed to be the theoretical limit. However, it requires a lot of complex hardware and intricate sorting of the decoy states on Bob and Alice's side. The two decoy state protocol can reach very close to the theoretical limit of infinite decoy states, hence the two decoy state protocol is the most widely adopted form of decoy state QKD, and furthermore, the vacuum+weak protocol is the preferred one. One can show that the vacuum+weak protocol is the optimum one by showing that the lower bound of yield is a decreasing function of ν_2 and that the upper bound of error rate is an increasing function of ν_2, thereby indicating that the lowest value of ν_2 would give the optimum performance, which in this case is zero. For finding the bounds for this specific case, just substitute $\nu_2 = 0$ into the expressions for the bounds.

4.3 Key generation rate

[8] tweaked the expression for the key generation rate provided by [7] to accommodate the effects of inefficient and practical error correction, given by the quantity $f(e) \geq 1$, which is the bidirectional error correction efficiency and is a function of the error rate, and is equal to 1 for perfect error correction. The modified key generation rate expression is now

$$R \geq q\left\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1^L[1 - H_2(e_1^U)]\right\} \tag{14}$$

where the lower and upper bound of single photon gain and error rates is inserted from the estimates derived in the previous section. The first effect of this improved estimate is that instead of pessimistically assuming that Eve will have the access to all multiphoton signals, one can give a more realistic estimate of these quantities, which increases the value of the secure key generation rate. Secondly, we apply the same approximations that we made in section 3 with equations (5) and (6) to the key rate equation given above, and we get

$$R \approx q\left\{-\eta\mu f(e_d)H_2(e_d) + \eta e^{-\mu}\mu[1 - H_2(e_d)]\right\} \tag{15}$$

Finding the μ that maximizes this lower bound by taking $\frac{dR}{d\mu} = 0$ and solving for μ, we find that μ does not scale with the transmission efficiency at all, and is independent of it. In other words, $\mu \sim O(1)$. Since the key generation rate, as we can see, scales as the product of μ and η, now scales linearly with the transmission efficiency, or in other words, $R \sim O(\eta)$. This decrease from quadratic scaling to linear scaling provides an enormous increase of distance within which secure keys can be established. The numerical simulation done by [8] with earlier experimental data showing the variation of the lower bound of the key generation rate with respect to distance of operation is shown in Figure 4. We see that the original [7] result has a much lower rate, and a much shorter distance of about 30km due to reasons discussed earlier. The decoy state method now increases the distance to 140km and also increases the value of the key generation rate.

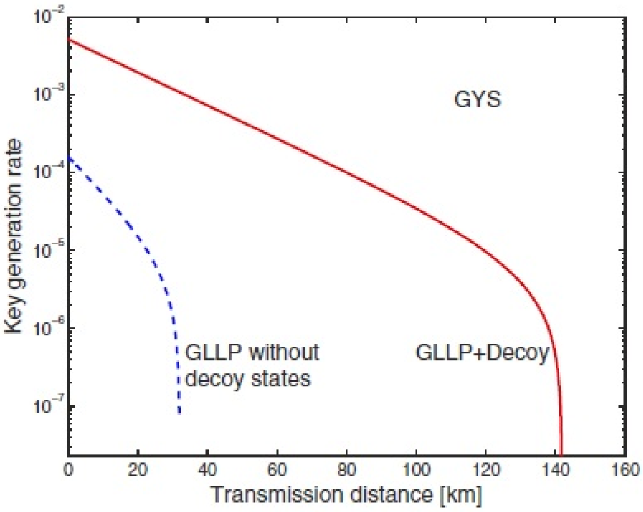


Figure 4: Secure key generation rate with respect to distance

In summary, we can say that

- Decoy state QKD provides an improvement in the distance due to linear scaling of key generation rate with transmittance
- Decoy state QKD provides an increase in the value of the key generation rate due to better estimates
- Decoy state QKD provides a way of detection of an eavesdropper when the eavesdropper is attacking the quantum channel with PNS attack
- Decoy state QKD provides the advantage of using conventional sources with attenuators, instead of going for single photon sources.

5 Experimental Implementations

5.1 Optical Fiber

The main paper based on which this discussion is going to be made is [11], which basically implements the decoy state QKD protocol with polarization encoding through optical fiber over 200km, back in 2010. They had beaten the previous record of 140.6km in optical fiber. They have used polarization encoding for carrying this out.

The general method that is preferred for implementing a BB84 protocol over optical fiber is phase encoding, where the bit is encoded in the phase of the light that is passed, and the nature of interference at the receiving end determines the bit value received by Bob. Phase encoding is generally preferred as in polarization encoding, the polarization undergoes a change in the polarization angle, resulting in the received light having a different polarization than the sent light. However, phase encoding schemes demand exceptional synchronization techniques. Synchronization is crucial for the operation of a practical QKD system so as to time tag the received pulses with the sent pulses for keeping accurate record of the sequence. High frequency synchronization is necessary so as to reduce the errors that creep into the detection events. In general, when phase encoding schemes are used, the detectors are used in a gated mode operation. The gated mode operation is basically setting a specific time window for having a detection event, and only considering the validity of a detection event if it falls within this window. This can either be done by predetermining the time of flight, or in other applications, if two detectors are used, the detection event of one detector can be used to gate the detection event of the other detector. Moreover, phase encoding scheme is an active measurement scheme, where Bob has to actively interfere with the setup to randomly choose the basis of measurement, where he synchronizes the received pulse with his choice for the phase at his side. The detectors have to be run in a gated mode because as explained earlier, dark counts will creep into the measurements, and the final key that can be distilled decreases.

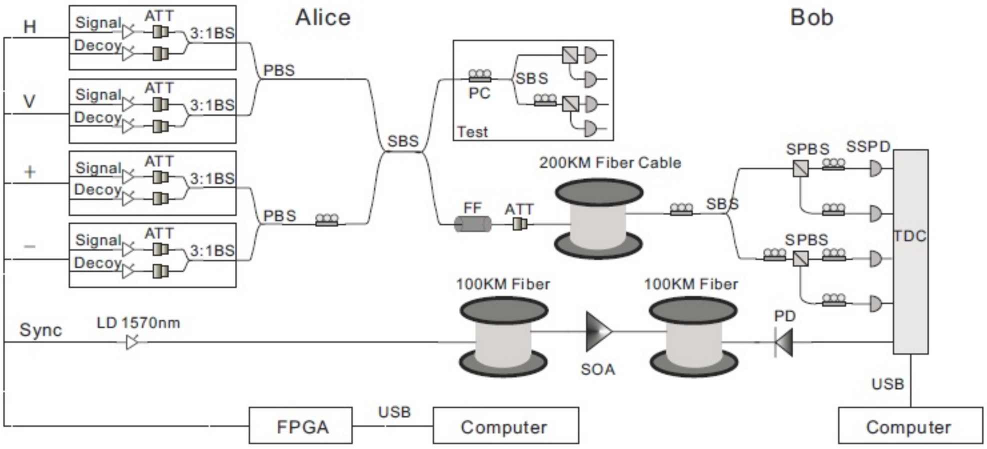


Figure 5: Experimental setup of [11]

In this particular experiment, the authors have used a superconducting single photon detectors (SSPD) which are basically single photon detectors, and the reason for using them is the high repetition rate, which denotes how fast a detector can detect a photon, and be ready to detect another one that is incoming. Furthermore, SSPDs can be run in an always on mode, where the gating operation need not be done. This, combined with the passive measurement system in polarization encoding, greatly simplifies the problem of synchronization. However, in polarization encoding, one requires an accurate local clock which can be used to time stamp events. In this experiment, the authors have opted for a synchronization pulse to time stamp events. They go on to say that this method decreases the dark count rate by half. The setup of this experiment is shown above in Figure 5.

The transmitting side consists of 8 laser diodes, with 4 for generating signal states with 4 polarization states, and 4 for generating decoy states, with 4 polarization states.

This experiment uses the vacuum+weak decoy state protocol. Each diode has its own attenuators, hence the average photon numbers of the signal and decoy states are set to be 0.6,0.2 and 0. A 4bit pseudo random number generator decides which state to send. If the first two bits are 00, the vacuum state is selected and no diode is triggered. If the first two bits are 01, the weak decoy state is triggered, and if the first two bits are 10 or 11, the signal state is triggered. The last two bits determine which polarization state to trigger, unless of course if the first two bits are 00. This results in the ratio of signal to the two decoy states is set to be 2:1:1. The light after attenuation is passed through a 3:1 BS, and then through a PBS, and then through a BS. The last BS will send half of the incoming photons through the optical fiber. The photons are passed through a bandpass filter FF of width 0.2 nm, so that the offset of wavelengths among the 8 diodes is within 0.2nm.

The fiber, as discussed earlier, introduces a shift in the polarization of the photons. This needs to be curbed, and hence, this experiment involves the use of automatic polarization controller (APC). The APC works on the basis of feedback control. Here, a certain fraction of the photons in the fiber is split and periodically, Alice sends a known polarization state. This separate split is used to measure the change in the polarization angle, and the control signal to correct this is sent to an electronic polarization controller (EPC). The EPC is then used to convert this control voltage into stretching and stressing the fiber, and this functions as the polarization controller.

The receiving end is the typical detection setup discussed in section 2.3. First, after polarization control, a BS functions as the passive basis selector, and if the basis is rectilinear, the photons just pass through a PBS and then into SSPDs, and if the basis is diagonal, the polarization is corrected with a another polarization controller, this time with known polarization control, so as to convert the diagonal basis into rectilinear basis, and then into PBS and SSPDs. Four of the SSPDs have an efficiency of 4% and one of them has an efficiency of 3%. This low efficiency is counteracted with a high repetition rate, meaning a large number secure keys is generated just by operating the entire setup at 320MHz. The repetition rate of the SSPDs is about 70MHz. The detection system is enhanced with the synchronization pulses, which are generated along the signal pulses at the transmitting end with a laser diode, which is amplified about halfway through, and a photodetector(PD) is used to detect this light. The detection window between the SSPD and the PD is taken to be 1.5ns, meaning any detection event that falls outside this window is neglected. This reduces the dark count rate by half, further improving the key generation rate.

The estimates for the secure key rate follows directly from the earlier discussion on two decoy state protocol. Here, let C_0, C_μ, C_ν be the counts by Bob for the vacuum, signal and weak decoy state respectively. If N_0, N_μ, N_ν are the total number of vacuum, signal and weak decoy states sent by Alice, then the gains are given by $Q_0 = C_0/N_0, Q_\mu = C_\mu/N_\mu.Q_\nu = C_\nu/N_\nu$. The lower and upper bounds of single photon gains and error rates are estimated as described earlier, and the role of statistical fluctuations is also taken into account. Statistical fluctuations are the result of having a finite data size, which essentially means that a sample would not be representative of the true probability distributions. The values are computed and inserted into the key generation rate expression described earlier, to get R. However, this is only in bits/signal state. To get the secure key rate in bits per second, one needs to use the following expression

$$K_\mu = \frac{1}{2}(1 - L_\mu)RN_\mu \tag{16}$$

where L_μ is the fraction of bits used for calculation of QBER. K_μ divided by the time of operation of protocol gives the secure key generation rate in bits per second. The experimental values obtained in this experiment are given in Table 1 below. The counts of vacuum, weak decoy and signal states is 3263,77157 and 449467. The time of operation is 3089 seconds, and 10% of signal states is used for QBER calculation. A secure key generation rate of 12.560Hz is obtained.

Table 1: Experimental parameters of [11]

Parameter	Value	Parameter	Value	Parameter	Value
length	200km	Q_μ	9.0941x10^{-7}	e_1	0.0496
f	320MHz	Q_ν	3.1223x10^{-7}	R	1.7445x10^{-7}
N	9.8848x10^{11}	Q_0	1.3204x10^{-8}	K_μ	3.8799x10^{4}
E_μ	0.0196	Q_1	1.2788x10^{-6}	K_μ/T	12.560Hz

5.2 Free-space

The eventual gold standard for quantum communications is the use of satellites for global communications. Although using optical fiber is an attractive option when communicating in short distances, the attenuation provided by them limits the maximum achievable distance in 100s of km. For secret communication from one continent to another, one needs to opt for free-space communication, and the obvious answer to this is using satellites. However, to establish the fact that quantum communications can be done using a satellite, one needs to take into account all possible satellite motions such as fast angular velocities with large angular accelerations, random and vibrational motions, and establishing a steady and accurate link even in the presence of high attenuation of the order of 50dB. This paper [12] goes ahead with this proposition, and is a direct and full-scale experimental verification of the feasibility of ground-satellite quantum key distribution by simulating several parameters that an actual setup would face while establishing a quantum channel between the satellite and the ground.

Global communication is facilitated with low earth orbit(LEO) satellites, which are situated at a distance of approximately 400-800km. The LEO satellites have a maximum angular velocity of 20mrads^{-1}, and a maximum angular accelration of 0.23 mrads^{-2}. The atmospheric attenuation is in between the ranges of 30-50dB. To completely verify the feasibility of building a steady quantum channel while generating secure keys at a high rate, and keeping the QBER low, one would need an actual satellite to go determine it. No other aerial vehicle would provide the simultaneous simulation of the three main factors, namely the fast motion, the random motions and vibrations, and a high loss channel. Therefore, the authors of this paper verify this by individually simulating the effect of the three factors and checking if a secure, steady and an accurate quantum channel could be established. They go about doing this with the vacuum and weak decoy BB84 protocol with polarization encoding. Unlike optical fibers, in free-space applications, the go to encoding scheme is polarization encoding, as the atmosphere offers very little change in the polarization angle, if at all any. The rapid angular motion is simulated with a turntable as the transmitter, which functions as the satellite, and a steady receiver, which functions as the ground station. The random and vibrational motion is simulated with a hot air balloon as the transmitter, and a stationary receiver as the ground station. The high loss environment is simulated with the transmitter at an elevated height, above the receiver, where the atmospheric attenuation is calculated to be around 50dB which is the maximum, and then testing whether a significant secure key rate is obtained. The experimental setup of this experiment is shown in Figure 6.

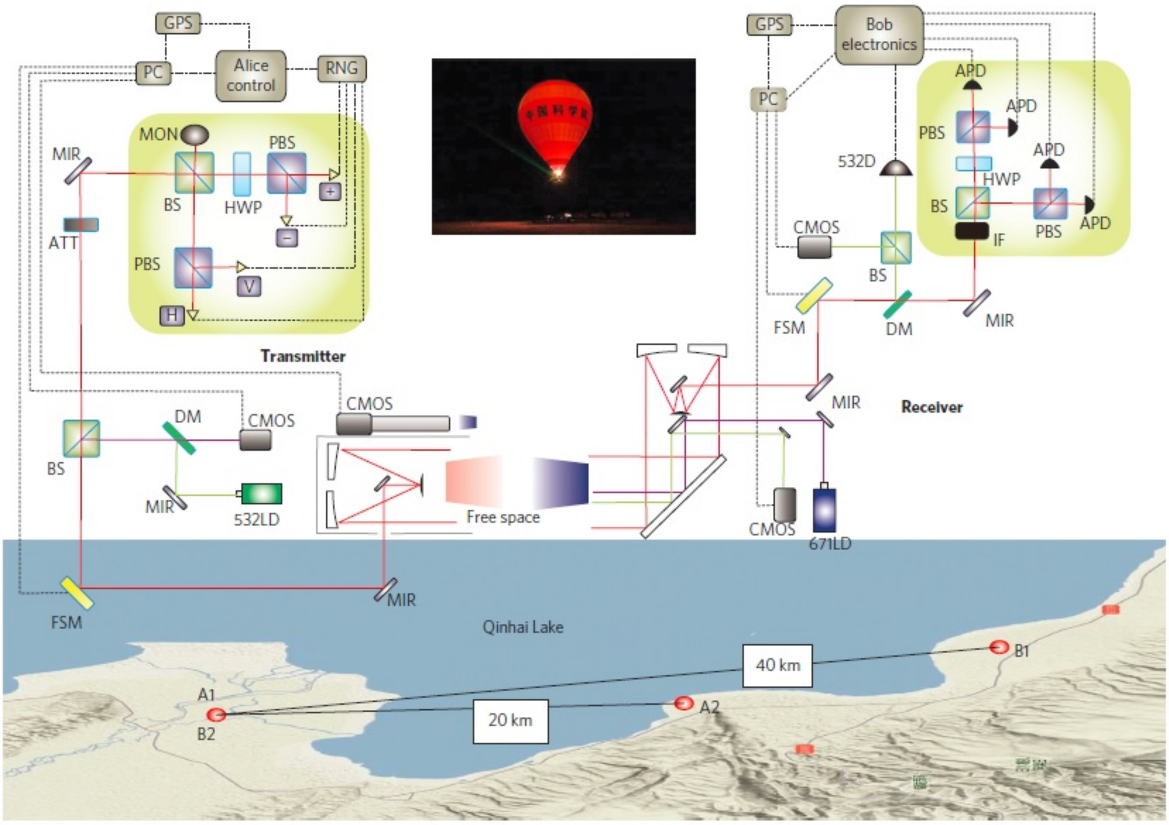


Figure 6: Experimental setup of [12]

The transmitter consists of four laser diodes for the four polarization states that emit 1ns pulses at 850nm wavelength. The decoy states are generated by varying the input voltage applied to the diodes. The diodes are chosen such that the difference in wavelengths is within 0.05nm so that the different states are not distinguishable. The four diodes are chosen by a random number generator, and the PBS is used to channel the light generated into a single path. The half wave plate (HWP) is used to convert light in the rectilinear basis into diagonal basis. There is also a monitor on Alice's side so as to check the power output. A fluctuation of more than 5% would mean that the entire protocol is stopped and started from scratch. The attenuator converts the light into weak coherent pulses. This light is then transmitted through a BS, reflected by a mirror and into the telescope, which hails this signal to the receiver. The receiver also consists of a telescope, which channels the light to a mirror, which reflects it and this light passes through an interference filter (IF), which basically acts as a bandpass filter. The detection setup follows the typical model, where a BS is used for passive basis selection, and the light that is polarized in the rectilinear basis is allowed to pass through a PBS and into detectors, and the diagonally polarized light is passed through a HWP and then into a PBS, and the detectors. Unlike the previous experiment, this uses a normal avalanche photodiode (APD).

An important aspect involved in simulating a ground-satellite communication link is using tracking lights or beacon lights to ensure that the light that is transmitted falls within the aperture of the receiving telescope. There are two sets of beacon lights used here, one in the receiving end and one in the transmitting end. A beacon light from the receiver is sent at a wavelength of 671nm, in the same way that light is sent from the transmitting end. This light is collected at the transmitter, and is passed through a fast steering mirror (FSM) which is a dynamically movable mirror to ensure that depending on the placement of the receiver, the light that is incident on the transmitting telescope is passed through the same channel for analysis. This light passes through the same BS that the 850nm light comes through, and is reflected past a dichroic mirror (DM) to the camera. Another beacon light, which also functions as a synchronizing pulse, is emitted at 532nm from the transmitter. This is reflected off of the DM, and through the FSM and through the transmitting telescope. This, once incident on the receiving telescope, passes through another FSM for tracking purposes, and is reflected off of a DM in the receiver side, and passes through a BS. A fraction of this light will be used for synchronization purposes for time stamping the events, and the rest will be used for tracking purposes.

The tracking plays an absolutely crucial role in this experiment, and will play a crucial role in every satellite-ground communication experiments. The authors have devised an acquisition, tracking and pointing (ATP) system for this. The FSM is connected to the ATP. In both the transmitter and receiver, there are two sets of ATP systems, a coarse ATP and a fine ATP. The coarse ATP consists of a coarse pointing mechanism, coarse camera and a coarse controller. The fine ATP consists of a fine pointing mechanism, a fine camera and a fine controller. The beacon light is incident on the coarse camera and through image processing algorithms, one can determine the offset. The corrective action for this offset is given to the coarse controller, which then controls the coarse pointing mechanism to point the system in the right direction. The coarse ATP has an accuracy of $\pm 200\mu$rad. The fine pointing mechanism has the exact same process, and has an accuracy of $\pm 5\mu$rad. This completes the entire experimental setup of this particular paper.

Firstly, the rapid angular motion is simulated with a transmitter mounted on a turntable, which gives maximum angular velocities of about 21mrads^{-1} and a maximum angular acceleration of 8.7mrads^{-2}, which covers the range of motions of a typical LEO satellite. The counting rate of the APDs is 5000Hz, and the total loss is about 40dB. This was carried out over a distance of 40km, and the final secure key rate that was obtained is about 159.41bps. Secondly, the random and vibrational motion, along with atmospheric turbulence, was simulated by mounting the transmitter on top of a hot air balloon, with the stationary receiver stationed about 20km from the hot air balloon. The main objective was to establish a steady and an accurate optical link between the transmitter and the receiver. Problems were created due to jolting and shaking of the hot air balloon. The ATP was able to successfully track the hot air balloon even when the random motion of the balloon caused it go out of the line of sight for the beacon light within 3-5 seconds.

The secure key rate that was obtained was 268.87bps. Finally, the high loss environment was simulated with the transmitter at an elevated height compared to the receiver, with a straight line distance of 96km. The environment and experimental parameters were chosen such that the loss was around 50dB, which exceeds the average attenuation faced for LEO satellites. Here, both the transmitter and receiver are stationary. A secure key rate of 48.03bps was obtained. The values of the various parameters related with the experiment is listed in Table 2 below.

Table 2: Experimental parameters of [12]

Parameter	Turntable	Hot-air balloon	High-loss environment
N	2.7x10^{10}	3.15x10^{10}	1.59x10^{11}
Q_μ	5.34x10^{-5}	5.90x10^{-5}	4.41x10^{-6}
Q_ν	2.17x10^{-5}	2.42x10^{-5}	2.36x10^{-6}
E_μ	2.73%	2.35%	4.04%
Q_0	3.00x10^{-6}	2.69x10^{-6}	4.30x10^{-7}
R	6.38x10^{-6}	1.08x10^{-5}	1.92x10^{-6}
K_μ/T	159.41	268.87	48.03

6 Conclusion

The exponential pace at which technology has evolved over the years, and the similarly exponential pace at which new challenges emerge to that technology has been the catalyst behind the digital era of the 21st century. It is what has led to this point of securing a communication channel based on the laws of physics and not by any other practical constraints informs us that we have reached an apogee in technological revolution. It is what has led to the birth of QKD in the form of BB84 in 1984, and it is what will continue to drive the future technologies: a desire to extract maximum possible performance or security from a particular system. Toshiba has modified the BB84 protocol in a very specific way [13], and on combining with the decoy state idea, they were able to reach secure key rates of the order of 1Mbps, which is almost enough to establish secure video calls. This technology has also been commercialized by them and industries at the forefront will be eager to use it. The idea of secure communication has also been extended to networks, with quantum networks based on the decoy state idea with the BB84 protocol being established in Tokyo [14], with 6 nodes in the network. The network has been designed in a way as to enable any two nodes to share a secret key. Further development has been made in the field of QKD regarding the measurement device and how it is vulnerable to certain exploitation by Eve, thereby research has gone into development of measurement device independent (MDI) QKD systems [14,15]. In 2016, the MDI-QKD system was combined with the decoy state idea to establish secure keys between two parties separated by almost 400km via optical fiber. This is more than the limit given by the original BB84 even while assuming ideal conditions. It is therefore prudent to expect the combination of MDI QKD and decoy states to lead the stage in further QKD evolution. The frontier of all this endeavor would be to establish global quantum communication systems with satellites, and work has been steadily being done in this particular area [16]. It won't be too long before the 21st century would be dubbed as the quantum era, with the advent of quantum computing and quantum information, and it will also be fascinating to see where these forays will take us all.

7 References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74, 145 (2002).
2. M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge Univ. Press, Cambridge, 2000).
3. C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Com- puters, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175-179
4. http://www.cse.wustl.edu/ jain/cse571-07/ftp/quantum/fig2.gif
5. "Quantum Key Distribution" Wikipedia page
6. W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).
7. D. Gottesman, H.-K. Lo, N. Lutkenhaus, and J. Preskill, Quantum Inf. Comput. 4, 325 (2004).
8. H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005).
9. X. Ma et al., Phys. Rev. A 72, 012326 (2005)
10. X. -B. Wang, Phys. Rev. Lett. 94, 230503 (2005); e-print quant-ph/0411047
11. Liu, Y. et al. Decoy-state quantum key distribution with polarized photons over 200 km. Opt. Express 18, 8587?8594 (2010).
12. Wang, J.-Y. et al. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. Nature Photon. 7, 387?393 (2013).
13. Lucamarini, M. et al. Efficient decoy-state quantum key distribution with quantified security. Opt. Express 21, 24550?24565 (2013).
14. Lo, H.-K., Curty, M. Tamaki, K. Secure quantum key distribution. Nature Photon. 8, 595?604 (2014).
15. H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. 117, 190501 (2016).
16. Vallone, G.; Bacco, D.; Dequal, D.; Gaiarin, S.; Luceri, V.; Bianco, G.; Villoresi, P. Experimental Satellite Quantum Communications. Phys. Rev. Lett. 2015, 115, 040502.