FSO-QKD protocols under free-space losses and device imperfections: a comparative study

Mitali Sisodia,* Omshankar, Vivek Venkataraman and Joyee Ghosh†

Quantum Photonics Lab, Department of Physics, Indian Institute of Technology Delhi, New Delhi, 110016, India

Abstract

Quantum key distribution (QKD) is a technique to establish a secret key between two parties through a quantum channel. Several QKD protocols have been proposed and implemented over optical fibers or free-space links. The main challenge of operating QKD protocols over a free-space link is atmospheric losses. In this paper, we have studied and compared the performance of single and entangled photon based QKD protocols by evaluating the quantum bit error rate and secure key rate for terrestrial free-space quantum communication by considering different free-space losses, such as geometrical losses, atmospheric losses as well as device imperfections.

Keywords: Quantum key distribution, Quantum bit error rate, Secure key rate, Geometrical losses, Atmospheric losses, Bell parameter.

1 Introduction

Classically, the security of information sent from one place to the other is mainly based on the popular Rivest-Shamir-Adleman (RSA) algorithm [1], which relies on the computationally extensive task of factorizing the product of two large prime numbers. This method hinges on the computational complications of certain mathematical tasks and is thus vulnerable to technological progress. Hence, there is a need to develop robust protocols to secure the shared information. Quantum cryptography and in particular, quantum key distribution (QKD) fulfills this criterion by taking advantage of the fundamental quantum physical properties such as (i) no cloning theorem, where any unknown quantum state cannot be copied; (ii) measurement collapse the quantum system to one of the possible quantum state, and (iii) irreversiblity of measurements implying that an output state cannot be used to generate an input state. The first QKD protocol was

---

*Email: mitalisisodiyadc@gmail.com

†Email: joyee@physics.iitd.ac.in

proposed by C. H. Bennett and G. Brassard in 1984 [2] utilizing qubits encoded through the polarization property of single photons. Later, several QKD protocols and their security proofs against an eavesdropper have been studied [3–14]. Various sources of single and/or entangled photons (flying qubits) have proved to be good candidates for quantum communication.

In 1989, the first table-top QKD experiment has been performed over a 32 cm quantum channel length [15]. Quantum communication schemes can be performed using optical fibers, terrestrial free-space optical (FSO), and satellite-based FSO implementations. Although there have been numerous implementations of QKD protocols that are optical-fiber based, the length of communication achieved have been only a few hundreds of kilometeres due to the limitation of an exponential increase of fiber losses with length [16–19]. On the other hand, a FSO (terrestrial and satellite) channel has proved to be a promising quantum channel providing secure quantum communication for longer distances (globally) and overcoming the problem of limited distant quantum communication through fibers [20–30] for longer distances. The main challenge of implementing QKD protocols over free-space link is due to atmospheric losses [31]. Other parameters such as timing, weather, protocol, place (ground), etc. [32] also play important roles. The free-space losses can be broadly categorized into geometrical losses and atmospheric losses. Every protocol has distance limitations due to these losses that grow with the transmission distance. Several studies mention these losses however a thorough quantitative study of the effect of the free-space losses (particularly geometrical and atmospheric losses) for various standard QKD protocols are not sufficiently investigated so far. Some of the FSO-based QKD protocols are-Bennett and Brassard, 1984 (BB84) [2], six-state [3], Ekert, 1991 (E91) [4], and Bennett, Brassard, and Mermin, 1992 (BBM92) [5]. Their performance comparison for particular distances (different length scales) have not been studied in detail. In this paper, we have theoretically compared the performance of free-space prepare-and-measure-based (BB84 and six-state) and entanglement-based (BBM92 and Ekert91) QKD protocols for different channel lengths and studied the effect of atmospheric losses on the quantum bit error rate (QBER) and the secure key rate (SKR). We have also explored the impact of device imperfections through detection efficiencies, losses and other parameters.

The paper is organized as follows: in Sections 2 and 3, we discuss QBER, SKR and free-space losses, the calculation of QBER and SKR for single-photon based QKD protocols (BB84 and six-state) are discussed in Section 4. In Section 5, entangled-photon based QKD protocols (E91 and BBM92) have been discussed. Finally, in Section 6, we have concluded the results.

Figure 1: Flow chart showing the steps involved in a general QKD protocol. In Ekert's protocol, one step is added that is Bell's inequality test which is performed during sifting process.

2 Quantum Bit Error Rate (QBER) and Secret Key rate (SKR)

Quantum bit error rate (QBER) evaluates the information leakage to an unauthorized third party (Eve) or due to imperfection of the physical devices. It is an important criterion to evaluate the performance of various QKD systems and has been calculated for various fiber-based or free-space QKD protocols [16–28]. It is defined as the ratio of the wrong bits to the total number of bits received and can be expressed as [9]

$$Q = \frac{N_{wrong}}{N_{total}} = \frac{N_{error}}{N_{correct+error}} \cong \frac{N_{error}}{N_{sift}}, \tag{1}$$

where N_{sift} is the sifted key when Alice and Bob choose the compatible basis and $N_{error}(\ll N_{sift})$ represents the error in the total number of bits. When, the QBER that determines the security of the QKD protocol (ideally $Q = 0$; lower the value of QBER, higher the security of the protocol or vice versa) is higher than the threshold value (vary for different QKD protocols; e.g., 11% for BB84 and 12.6% for six-state protocol [13]) then they discard and repeat the QKD protocol. The non-zero value of QBER is due to free-space losses, Eve's presence, noises, imperfections in the physical devices, etc. A secret key can only be generated if the mutual information (I_{AB}) of Alice and Bob is greater than Eve's information $\left(I_{E(n)}\right)$ [6, 13]. The secret key rate (SKR) is expressed as

$$S = n_{sift}\left[I_{AB} - I_{E(n)}\right], \tag{2}$$

where $I_{AB} = 1 - h(Q) = 1 + Q\log_2(Q) + (1-Q)\log_2(1-Q)$, $h(Q)$ is the Shannon entropy, $h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$ and n_{sift} is the basis reconciliation factor (when

Alice and Bob choose compatible bases).

3 Free-space losses (Geometrical/Atmospheric)

The main challenge of implementing QKD protocols over free-space optical (FSO) channel is the free-space losses such as absorption, scattering, diffraction, turbulence, etc. and are categorized in two parts (1) geometric (2) atmospheric [6] that hinder the photon propagation in FSO channel. The geometric losses occur due to the spreading of the beam propagating from the transmitter to the receiver [33–35]. It can be calculated as $\left[\frac{d_r}{d_t + DL}\right]^2$, where d_r and d_t are the diameters of the receiver and transmitter apertures, respectively, D is the beam divergence and L is the channel length. The atmospheric attenuation is described by the Beer-Lambert's law $\tau = \exp(-\alpha L)$ dB/km, where α is the atmospheric attenuation coefficient that include the absorption and scattering of the atmospheric medium [35]. Thus, the total atmospheric loss can be expressed as

$$T = \left[\frac{d_r}{d_t + DL}\right]^2 \exp\left(-\alpha L\right). \tag{3}$$

Table1 shows the total channel losses that one can expect from geometrical and atmospheric losses considered for different channel length scales: lab-scale, outside-lab and larger-scale distances. As evident, for large channel lengths, the loss is mainly dominated by the atmospheric losses (α) that exponentially increases with L. While for smaller channel lengths (lab scale), the channel loss is mainly dominated by the geometrical losses.

Table 1: Typical values of the total channel losses for different channel lengths.

L(m)	d_t(mm)	d_r(mm)	D(mrad)	α(dB/km)	Channel loss (dB)
10 (lab-scale)	10	10	0.025	0.1	0.02
500 (outside-lab)	10	12	0.025	0.1	5.68
30,000 (larger-scale)	10	100	0.025	0.1	30.64

4 Single-photon based QKD protocols (BB84 and six-state)

QKD protocols, based on single-photons, are routinely implemented using attenuated pulsed lasers due to the challenge of obtaining sources of true single-photons. Such attenuated laser sources are prone to information leakage through photon number splitting (PNS) attack due to multiphoton pulse generation. A need for true single photon sources have led to the research efforts in color centers [36], quantum dots [37], atoms [38], trapped ions in a cavity [39], etc. Another popular technique for single-photon sources exploits the

Figure 2: Variation of QBER and SKR for BB84 protocol as a function of channel loss (T) for different detector efficiency (η) and noise count probability (P_{nc}).

second-order susceptibility ($\chi^{(2)}$) of a nonlinear material through spontaneous parametric down-conversion (SPDC) in which an intense laser interacts with a nonlinear material to generate two down-converted photons (idler/signal). Conditioned on the detection of an idler photon, the signal photon can be used as a resource of heralded single photon source. Such heralded sources can be a promising candidate for implementing the single photon based QKD protocols such as BB84 [2] and six-state [3].

BB84 is a four non-orthogonal state-based protocol in which Alice (sender) prepares a string of single photons in one of the four polarization states $|\uparrow\rangle$, $|\downarrow\rangle$, $|\nearrow\rangle$ and $|\nwarrow\rangle$ and send it to Bob (receiver) who randomly performs the measurement in the rectilinear $\{|\uparrow\rangle, |\downarrow\rangle\}$ or diagonal $\{|\nearrow\rangle, |\nwarrow\rangle\}$ bases and use the photons for key generation measured in the same basis. An extended version of BB84 (six-state protocol) has been proposed with more tolerance to noise that enhances the security compared to BB84 [3]. In this protocol, six states $|\uparrow\rangle$, $|\downarrow\rangle$, $|\nearrow\rangle$, $|\nwarrow\rangle$, $|\circlearrowleft\rangle$, and $|\circlearrowright\rangle$ in three bases [1] (rectilinear, diagonal and circular) is used. The extra choice of basis creates an obstacle on Eve's measurement path and produces higher error rate. Consequently, Alice and Bob can easily detect the Eve's presence. In both the protocols, Alice and Bob keep the photons which are measured in the same basis ($\frac{1}{2}$ and $\frac{1}{3}$ probability for BB84 and six-state protocol, respectively [13]). For both the protocols, the error in the shifted key is calculated by measuring the QBER [Eq.1]. There are mainly two contributions to N_{error} (P_{opt} and P_{nc}) for single-photon based protocols. Thus, the total QBER can be calculated as [9]

$$Q = P_{opt} + \beta \frac{P_{nc}n}{T\eta q\mu}, \tag{4}$$

where $\beta = \frac{1}{2}$ for BB84 protocol and $\frac{2}{3}$ for the six-state protocol, P_{opt} is the probability of

---

[1]where $|\uparrow\rangle(|\downarrow\rangle) = |H\rangle(|V\rangle)$, $|\nearrow\rangle(|\nwarrow\rangle) = \frac{|H\rangle+|V\rangle}{\sqrt{2}}(\frac{|H\rangle-|V\rangle}{\sqrt{2}})$, $|\circlearrowleft\rangle(|\circlearrowright\rangle) = \frac{|H\rangle+i|V\rangle}{\sqrt{2}}(\frac{|H\rangle-i|V\rangle}{\sqrt{2}})$.

Figure 3: Variation of QBER and SKR for six-state protocol as a function of channel loss (T) for different detector efficiency (η) and noise count probability (P_{nc}). For top row graphs, $P_{nc} = 10^{-5}$ and for bottom row graphs, $\eta = 0.6$.

incorrect detections of the photons due to imperfect interference or polarization contrast, P_{nc} is the probability of overall noise counts that include the detector dark counts and the background counts, q (1 or 0.5) is used to correct the non-interfering path combinations, n is the number of detectors, η is the detector efficiency, T is the channel transmittance, and μ is the mean photon number ($\mu = 1$ for single photon sources). The secret key rate for BB84 and six-state protocol is calculated as [13]

$$S_{BB84} = \frac{1}{2}\nu_S T \left[1 + 2Q \log_2 Q + 2(1 - Q) \log_2(1 - Q)\right], \tag{5}$$

$$S_{six-state} = \frac{1}{3}\nu_S T \left[1 + \frac{3Q}{2} \log_2 \frac{Q}{2} + \left(1 - \frac{3Q}{2}\right) \log_2 \left(1 - \frac{3Q}{2}\right)\right]. \tag{6}$$

where ν_S is the heralded single photon counts at the sender's side. For the present study, we have considered a type-0 SPDC source with a brightness (photon-pairs per unit mW pump power) of $\nu_S = 0.64 \times 10^6$ cps/mW from Ref. [40].

Figures 2 and 3 show the calculated QBER and SKR for BB84 and six-state protocols, as a function of the channel loss at different detector efficiencies ($\eta = 0.4, 0.6, 0.8$) and noise count probabilities ($P_{nc} = 10^{-5}, 10^{-4}, 10^{-3}$) for $q = 0.5$, $\mu = 1$, $P_{opt} = 0.001$, $\nu_S = 0.64 \times 10^6$ cps , $n = 4$. In these figures, the black dashed-dotted line shows the threshold value of QBER for the respective protocols. A maximum threshold of 11% and 12.6% ($\eta = 0.4$, black dotted line in Figures 2 and 3) for BB84 and six-state protocol yield a noise tolerance of 33dB and 36dB, respectively. The noise tolerance increases with an increase (decrease) of the detector efficiency (noise count probability). Moreover, the SKR is high when channel losses are low and decreases sharply to the threshold limit of 33dB and 36dB, respectively, corresponding to the threshold value of QBER. We infer

6

that detectors with high efficiency, that affect the overall noise counts, are required to tolerate high channel losses or longer channel lengths.

Figure 4 shows the calculated SKR of BB84 and six-state protocol at different channel losses for $\eta = 0.6$ and $P_{nc} = 10^{-5}$. Since, the six-state protocol utilizes three MUBs, more information about the Eve's presence can be obtained, resulting in a higher bit error rate threshold and higher noise tolerance.

Figure 4: Comparison between the BB84 and six-state protocol with respect to channel loss for $\eta = 0.6$ and $P_{nc} = 10^{-5}$.

5 Entanglement-based QKD protocols

Artur Ekert proposed the first entanglement-based QKD protocol [4] by exploiting the maximally entangled states that violate the Clauser-Horne-Shimony-Holt (CHSH) inequality [41]. It utilizes the three randomly selected bases to measure the polarization of the entangled-photon. The extra basis is required to perform the Bell's inequality test that directly detects the presence of an eavesdropper without revealing the key information. Nonlinear optical techniques like, SPDC and spontaneous four-wave mixing (SFWM) have been capitalized to generate the polarization entangled-photon. Such entangled-states intrinsically increase the security of the shared information, govern by the inherent quantum nature of the source. The degree of violation of a Bell inequality is used to quantify the quality of entanglement between the photon-pairs, for which Bell parameter (S_{CHSH}) is calculated as

$$S_{CHSH} = |E\left(\theta_A^1, \theta_B^1\right) + E\left(\theta_A^1, \theta_B^3\right) - E\left(\theta_A^3, \theta_B^1\right) + E\left(\theta_A^3, \theta_B^3\right)|, \qquad (7)$$

where $E\left(\theta_A^i, \theta_B^j\right)$ is the correlation coefficient at two different orientation of the analyzers of Alice and Bob corresponding to different chosen bases, i and j, respectively.

Here are the different cases of the calculated S parameter:

- $|S_{CHSH}| \leq 2$ implies an extreme case of destruction of entanglement signifying the classical nature of the source with no chance of a key generation.

7

- $|S_{CHSH}| = 2\sqrt{2}$ represents a perfectly entangled state (maximum value of the violation of the Bell's inequality). This is an ideal scenario.

- For $2 < |S_{CHSH}| < 2\sqrt{2}$ implies a real situation with Eve's presence and/or noise detection. The sifted key may not be discarded and can be used to generate a secret key after classical post-processing algorithms, used for error correction and privacy amplification.

We consider a SPDC source that generates entangled photon-pairs and sends them through the turbulent medium (atmosphere) to the receiver stations A(Alice) and B (Bob). One of the maximally entangled polarization state can be expressed as:

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(|H\rangle_A |V\rangle_B + e^{i\varphi} |V\rangle_A |H\rangle_B \right), \tag{8}$$

where, H and V are the polarizations of the photon-pair and φ is the relative phase. The randomly chosen orientation of the analyzer angles at A and B are $(\theta_A^1, \theta_A^2, \theta_A^3 = 0, \frac{\pi}{8}, \frac{\pi}{4})$ and $(\theta_B^1, \theta_B^2, \theta_B^3 = -\frac{\pi}{8}, 0, \frac{\pi}{8})$, respectively. For $\varphi = \pi$ and $(\theta_A^1, \theta_A^3, \theta_B^1, \theta_B^3) = (0, \frac{\pi}{4}, -\frac{\pi}{8}, \frac{\pi}{8})$, a maximal value $(2\sqrt{2})$ of S_{CHSH} is reached for the $|\psi\rangle$ state, for which the correlation coefficient can be calculated as [42]

$$E\left(\theta_A, \theta_B\right) = N\left[-\cos2\theta_A\cos2\theta_B + \cos\varphi \sin2\theta_A\sin2\theta_B\right],$$

where N is a constant that depends on the noise counts and atmospheric losses, leading to a reduction in S_{CHSH} and defined as [42]

$$N = \frac{p_s \eta_t^2}{p_s \left[\eta_t + 2P_{nc}\left(1 - \eta_t\right)\right]^2 + 2p_1 P_{nc} \left[\eta_t + 2P_{nc}\left(1 - \eta_t\right)\right] + 4p_0 P_{nc}^2}.$$

where, $p_s = T_A \cdot T_B$ is the Bell state probability with $T_{A(B)}$ (Eq. 3) being the tranmission cofficient of the receiver stations A(B) [2], $p_1 = p_{H_A} + p_{V_A} + p_{H_B} + p_{V_B}$ is the sum of the probability of a single-photon state calculated as: $p_{H_A} = \frac{1}{2}\left(T_A\left(1 - T_B\right)\right)$, $p_{H_B} = \frac{1}{2}\left(T_B\left(1 - T_A\right)\right)$, $p_{V_A} = p_{H_A}$, $p_{V_B} = p_{H_B}$ (H and V are the horizontal and vertical modes, respectively). Here η_t is the total detection efficiency which is the product of detector efficiency (η) and photon collecting efficiency ($\eta_c = 0.6$).

The variation of the Bell parameter as a function of channel loss with different detection efficiencies (η) and probability of noise counts (P_{nc}) is shown in Figure 5. It is evident that entanglement can survive and tolerate higher losses for lower noise counts (black dashed line). The purple solid line shows the threshold of Bell's inequality ($S_{CHSH} = 2$) signifying a witness of the entanglement or non-locality (quantum phenomenon). Although an implementation of the Ekert's (E91) protocol is partly complicated as it requires the Bell's inequality test to detect Eve's presence, however it has the quality of utmost and unconditional security (more secure even for devices that are not trusted) and can be

---

[2]We have considered Alice's and Bob's stations to be exposed to equal losses ($T_A = T_B$).

Figure 5: Effect of the channel losses on the entanglement quality for different detection efficiencies and noise counts.

used in a special case where other protocols (e.g., BBM92, BB84) fail to perform. The E91 protocol is a fully device-independent QKD (DIQKD) protocol, which facilitates the unconditional security without any trusting the QKD device [43].

In 2007 [44], Acin et al. derived a formula for unconditional security bound $I_E = h\left(\frac{1+\sqrt{S^2/4-1}}{2}\right)$ and the relation $S_{CHSH} = 2\sqrt{2}\left(1-2Q\right)$ for the E91 protocol. It is clear that when $Q \cong 14.6\%$ then $S_{CHSH} = 2$, and therefore no secure key can be generated. In Figure 6, we have plotted the QBER and SKR as a function of channel loss for different detection efficiences and probabilities noise counts using

$$S_{E91} = \frac{1}{3}\nu_s T \left[1 - h(Q) - h\left(\frac{1+\sqrt{S_{CHSH}^2/4-1}}{2}\right)\right]. \tag{9}$$

The necessary condition (Bell's inequality violation) or the need of an extra basis to calculate the amount of information leaked by eavesdropper was removed by Bennett, Brassard, and Mermin in their 1992 protocol (BBM92) [5]. In this entanglement-based BBM92 protocol, Alice and Bob use two mutually unbiased bases (rectilinear or diagonal) to randomly perform the measurement on the entangled photons (entanglement version of the BB84 protocol). The classical error correction and privacy amplification part is similar to the BB84 protocol. In this protocol, a central SPDC source generates entangled photon pairs, one of which is sent to Alice while the other photon is sent to Bob. Alice and Bob randomly choose the basis to perform the measurement on the incoming photons. In an ideal scenario (no eavesdropping), if Alice and Bob choose the same basis, then their measurement outcome will always be same or completely correlated as the two photons of an Einstein–Podolsky–Rosen (EPR) pair are correlated. Thus a symmetric key (sifted key) is generated (which is discarded when they measure in the different bases). Then, they perform classical error correction and privacy amplification to estimate the QBER. Any attempt of an eavesdropper to intervene (on the source or on the photons) will destroy the entanglement and introduce an error in the sifted key. This is the witness of entanglement in BBM92 protocol, while Eve's information is bounded by evaluating

9

Figure 6: Plots of the QBER and SKR in terms of channel loss with varying η and P_{nc} for E91 protocol. For top row graphs, $P_{nc} = 10^{-5}$ and for bottom row graphs, $\eta = 0.6$.

Bell's inequality whose violation (non-locality) is the witness of entanglement in Ekert91 protocol.

In an entanglement-based QKD protocol, imperfections in the entangled photon pair sources are characterized by the two photon interference visibilites based on the polarization correlations V_{HV} and $V_{\pm 45}$ in the HV and $\pm$ bases, respectively. Intrinsic QBER of a QKD system is calculated as $q_i = \frac{1-V_{tot}}{2}$, where $V_{tot} = \frac{V_{HV}+V_{\pm 45}}{2}$ which can be directly calculated by performing two-photon interference measurements [30].

We consider two situations in the BBM92 protocol:

(1) When the source at Alice's side

(2) When the source placed in the middle.

In both cases, the raw key rate is half of the detected coincidence rate,

$$r_{sig} = \frac{1}{2} r_c T, \tag{10}$$

where r_c is the coincidence rate corresponding to single event rates r_1 (Alice's detector) and r_2 (Bob's detector) which include detector efficiencies and T is the transmission of the entire quantum channel. The accidental coincidence rate where only one detector is exposed to the background events is given by [28] ,

$$r_{a(single)} = \frac{1}{2} (r_1 - T r_c) (r_{bg} + T (r_2 - r_c)) \tau_c, \tag{11}$$

When the source is in the middle, both detectors are exposed to the background events in which case the accidental coincidence rate is expressed as:

$$r_{a(both)} = \frac{1}{2} (r_{bg} + T (r_1 - r_c)) (r_{bg} + T (r_2 - r_c)) \tau_c, \tag{12}$$

10

Figure 7: Variation of QBER and SKR with respect to channel loss for different values of η and P_{nc}, when source at Alice's side (BBM92). For top row graphs, $P_{nc} = 10^{-5}$ and for bottom row graphs, $\eta = 0.6$.

where r_{bg} is an external background event rate calculated as $r_{bg} = P_{nc}r_1(r_2)$, τ_c is a coincidence time interval. The total QBER is [28],

$$Q = \frac{1}{r_{sig} + r_a} \left(q_i r_{sig} + \frac{1}{2} r_a \right). \tag{13}$$

We have adapted the value of the parameters from an experimental study that considers [40]: $\nu_S = r_1 = r_2 = 0.64 \times 10^6$, $r_c = \eta^2 \eta_c^2 r_1$; where η_c is the photon collection efficiency into the fiber and η is the detector efficiency, and $\tau_c = 2$ ns, $q_i = 0.043$ [28].

When the source is in the middle both arms are exposed to detector error, background counts and other losses. Hence there impact is doubled in comparison to the situation when the source is at Alice's or Bob's side (only one arm exposed to the losses and errors), therefore QBER is always higher in the second case of BBM92. Figures 7 and 8 show the effect of free-space losses on QBER and SKR for different detector efficiencies and noise count probabilities. The entanglement-based QKD is a basis-independent QKD because the state emitted from the EPR source is independent of the measurement bases in Alice's and Bob's side [45]. The unconditional security in these cases are established by Koashi and Preskill [12] and improved by Ma, Fung, and Lo [45]. The secret key generation rate for the BBM92 protocol at the QBER threshold value of 11% is,

$$S_{BBM92} = \frac{1}{2}\nu_S T \left[1 - f(Q) h_2(Q) - h_2(Q) \right]. \tag{14}$$

here, $f(Q)$ is the bidirection error correction efficiency as a function of error rate. The values of $f(Q)$ for different error rates may be found in Ref. [46].

Figure 9 shows the QBER and SKR comparing the two above situations of the BBM92 protocol. We see that when the source is in the middle, the protocol tolerates higher channel losses, almost double compared to the situation when the source is at Alice's

Figure 8: QBER and SKR with varying η and P_{nc} in terms of channel loss, when source placed in the middle (BBM92). For top row graphs, $P_{nc} = 10^{-5}$ and for bottom row graphs, $\eta = 0.6$.

Figure 9: Comparison of BBM92 QKD protocol as a function of channel losses when source is Alice 's side and at the middle for $\eta = 0.6$ and $P_{nc} = 10^{-5}$.

side.

6 Conclusion

We have theoretically studied and compared four different QKD protocols based on single-photon (BB84 and six-state) and entanglement-photons (Ekert91 and BBM92) by evaluating the QBER and SKR for free-space losses and device imperfections. The role of detector efficiency and noise counts for different channel losses is studied and shown in Figures 2, 3, 5-8. It is shown that an increment in the channel loss leads to a higher QBER resulting in a lower SKR for both single-photon and entangled-photon based QKD protocols. The detector efficiency greatly affects the QBER and SKR for larger channel loss (channel length) due to the exponential rise of channel losses compared to lower

channel lengths (especially in lab-scale implementations). The numerically calculated values of the QBER and SKR are considered for QKD protocols at different length scales: lab-scale, outside-lab and larger-scale distances is shown in Table 2.

Table 2: The expected QBER and SKR for different QKD protocols at different channel lengths for $\eta = 60\%$ and $P_{nc} = 10^{-5}$.

Channel Length	BB84		Six-state		BBM92		E91	
	QBER (%)	SKR (bits/sec)	QBER (%)	SKR (bits/sec)	QBER (%)	SKR (bits/sec)	QBER (%)	SKR (bits/sec)
10 m	0.107	3.11×10^5	0.105	2.09×10^5	5.18	1.16×10^5	0.006	2.1×10^5
500 m	0.125	0.84×10^5	0.12	0.57×10^5	5.22	0.31×10^5	0.007	1.8×10^5
30 km	7.6	86	5.21	132	5.24	106	7.17	4.42

Since, the atmospheric losses are inevitable and cannot be controlled, to obtain a low QBER, near-to-perfect devices are desirable that have high efficiency and minimal losses. In this study, we have considered practical values of different parameters (detector's efficiency, background counts, coincidence rates, diameter of the receiver and transmitter apertures, beam divergence etc.) for different QKD protocols pertaining to practical systems. We have shown that secret key generation is possible even under atmospheric losses within certain ranges of parameter values. Also, a comparative study of the protocols under the single photon/ prepare-and-measure technique as well as the entanglement-based technique (Figures 4 and 9) show that the single (entangled) photon based six-state (BBM92) protocol tolerates higher channel losses compared to BB84 (E91) protocol. Two cases of source (entangled photon) position for BBM92 protocol are considered and compared (Figure9), which proves that when the source is placed in the middle it can tolerate higher channel losses (almost double) as compared to the situation when the source is placed at Alice's side. A benefit of such comparative studies is to facilitate researchers with parameters and values from a practical consideration helping them to select high performace based QKD protocol for free-space under considered atmospheric conditions. The present theoretical work can be utilized by experimentalists to implement practical QKD protocols under different conditions and can be extended for longer distances or for satellite based applications.

References

[1] Vernam, G.S.: Cipher printing telegraph systems: For secret wire and radio telegraphic communications. Journal of the AIEE, **45**, 109-115 (1926)

[2] Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE InternationalConference on Computers, Systems and Signal Processing, Bangalore, India, 10-19 December 1984, pp. 175–179 (1984)

[3] Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. **81**, 3018 (1998)

[4] Ekert, AK.: Quantum Cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991)

[5] Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell's theorem. Phys. Rev. Lett. **68**, 557 (1992)

[6] Scarani,V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev,M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301 (2009)

[7] Xu, F., Ma, X., Zhang, Q., Lo, H.K., Pan, J.W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phy. **92**, 025002 (2020)

[8] Inamori, H., Rallan, L., Vedral, V.: Security of EPR-based quantum cryptography against incoherent symmetric attacks. J. Phys. A Math. Theor. **34**, 6913 (2001)

[9] Gisin N, Ribordy G, Tittel W, Zbinden H.: Quantum cryptography. Rev. Mod. Phy. **74**, 145 (2002)

[10] Bechmann-Pasquinucci, H. and Gisin, N.: Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. Phy. Rev. A **59**, 4238 (1999)

[11] Lo, H.K.: Proof of unconditional security of six-state quantum key distribution scheme. Quantum Inf. Comput. **1**, 81 (2001)

[12] Koashi, M., Preskill, J.: Secure quantum key distribution with an uncharacterized source. Phys. Rev. Lett. **90**, 057902 2003.

[13] Pirandola, S., Andersen, UL., Banchi, L., et al.: Advances in quantum cryptography. Adv. Opt. Photonics. **12**, 1012-236 (2020)

[14] Shor, PW., Preskil, l J.: Simple proof of security of the BB84 quantum key distribution protocol. Phy. Rev. lett. **85**, 441 (2000)

[15] Bennett, C. H., Brassard, G.: Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working! Sigact News **20**, 78–80 (1989)

[16] Boaron, A., Boso, G., Rusca, D., et al.: Secure quantum key distribution over 421 km of optical fiber. Phy. Rev. lett. **121**, 190502 (2018)

[17] Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N. et al.: Provably secure and practical quantum key distribution over 307km of optical fibre. Nat. Photonics, **9**, 163–168 (2015).

[18] Shi, Y., Moe Thar, S., Poh, H.S., Grieve, et al.: Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber. App. Phy. Lett. **117**, 124002 (2020)

[19] Yin, H.L., Chen, T.Y., Yu, Z.W., Liu, H., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016)

[20] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H. et al.: Entanglement-based quantum communication over 144km, Nat. Phys. **3**, 481–486 (2007)

[21] Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F. et al.: Experimental demonstration of free space decoy-state quantum key distribution over 144 km, Phys. Rev. Lett. **98**, 010504 (2007)

[22] Marcikic, I., Lamas-Linares, A., Kurtsiefer, C.: Free-space quantum key distribution with entangled photons, Appl. Phys. Lett. **89**, 101122 (2006)

[23] Yin, J., Cao, Y., Li, Y.H., Ren, J.G., Liao, S.K., et al.: Satellite-to-ground entanglement-based quantum key distribution. Phys. Rev. Lett. **119**, 200501 (2017)

[24] Takenaka, H., Carrasco-Casado, A., Fujiwara, M., Kitamura, M., Sasaki, M., Toyoshima, M.: Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. Nat. Photonics **11**, 502–508 (2017)

[25] Liao, S.K., Cai, W.Q., Liu, W.Y., Zhang, L., et al.: Satellite-to-ground quantum key distribution. Nature **549**, 43–47 (2017)

[26] Yin, J., Cao, Y., Li, Y.H., Liao, S.K., et al.: Satellite-based entanglement distribution over 1200 kilometers. Science **356**, 1140–1144 (2017)

[27] Yin, J., Li, Y.H., Liao, S.K., Yang, M., Cao, Y., et al.: Entanglement-based secure quantum cryptography over 1,120 kilometres. Nature **582**, 501-505 (2020)

[28] Peloso, M.P., Gerhardt, I., Ho, C., Lamas-Linares, A., Kurtsiefer, C.: Daylight operation of a free space, entanglement-based quantum key distribution system. New J. Phy. **11**, 045007 (2009)

[29] Erven, C., Couteau, C., Laflamme, R., Weihs, G.: Entangled quantum key distribution over two free-space optical links. Opt. Express **16**,16840-16853 (2008)

[30] Scheidl, T., Ursin, R., Fedrizzi, A., et al.: Feasibility of 300 km quantum key distribution with entangled states. New J. Phy. **11**, 085002 (2009)

[31] Villaseñ, E., Malaney, R., Mudge, K.A., Grant, K.J.: Atmospheric effects on satellite-to-ground quantum key distribution using coherent states. In GLOBECOM 2020-2020 IEEE Global Communications Conference, pp. 1-6. IEEE. ,December (2020)

[32] Liorni, C., Kampermann, H., Bruß, D.: Satellite-based links for quantum key distribution: beam effects and weather dependence. New J. Phy. **21**, 093055 (2019)

[33] Mushtaq, M.T., Yasir, S.M., Khan, M.S., Wahid, A., Iqbal, M.S.: Analysis of internal design parameters to minimize geometrical losses in free-space optical communication link. Acta Phys. Polonica A **134**, 275-277 (2018)

[34] Bloom, S., Korevaar, E., Schuster, J., Willebrand, H.: Understanding the performance of free-space optics. J. Opt. Netw. **2**, 178–200 (2003)

[35] Tang, X.: Polarisation shift keying modulated free-space optical communication systems. University of Northumbria at Newcastle (United Kingdom). (2012)

[36] Aharonovich, I., Castelletto, S., Simpson, D.A., et al.: Diamond-based single-photon emitters. Rep. Prog. Phys. **74**, 076501 (2011)

[37] Pelton, M., Santori, C., Vuckovi, J., et al.: Efficient source of single photons: a single quantum dot in a micropost microcavity. Phy. Rev. Lett. **89**, 233602 (2002)

[38] McKeever, J., Boca, A., Boozer, A.D., et al.: Deterministic generation of single photons from one atom trapped in a cavity. Science, **303**, 1992-1994 (2004)

[39] Higginbottom, D.B., Slodicka, L., Araneda, G., et al.: Pure single photons from a trapped atom source. New J. Phy. **18**, 093038 (2004)

[40] Steinlechner F, Trojek P, Jofre M, Weier H, Perez D, et al.: A high-brightness source of polarization-entangled photons optimized for applications in free space. Opt. Express **20**, 9640 (2012)

[41] Bell, J. S.: On the Einstein Podolsky Rosen paradox, Phys. Physique Fizika **1**, 195 (1964)

[42] Semenov, A.A., Vogel, W.: Entanglement transfer through the turbulent atmosphere. Phy. Rev. A **81**, 023835 (2010)

[43] Acin, A., Gisin, N., Masanes, L.: From Bell's theorem to secure quantum key distribution. Phys. Rev. Lett. **97**, 120405 (2006)

[44] Acin, A., Brunner, N., Gisin, N., et al.: Device-independent security of quantum cryptography against collective attacks. Phys. Rev. Lett. **98**, 230501 (2007)

[45] Ma, X., Fung, C.H.F., Lo, H.K.: Quantum key distribution with entangled photon sources. Phy. Rev. A **76**, 012307 (2007)

[46] Waks, E., Santori, C., Yamamoto, Y.: Security aspects of quantum key distribution with sub-Poisson light. Phy. Rev. A **66**, 042315 (2002)