BBM92 quantum key distribution over a free space dusty channel of 200 meters

Sarika Mishra¹,², Ayan Biswas¹,², Satyajeet Patil¹,², Pooja Chandravanshi¹, Vardaan Mongia¹,², Tanya Sharma¹,², Anju Ran¹,², Shashi Prabhakar¹, S Ramachandran³ and Ravindra P Singh¹

¹ Quantum Science and Technology Laboratory, Physical Research Laboratory, Ahmedabad 380009, India
² Indian Institute of Technology, Gandhinagar 382355, India
³ Aerosol Monitoring Laboratory, Physical Research Laboratory, Ahmedabad 380009, India

E-mail: sarika@prl.res.in

Received 4 February 2022, revised 21 April 2022
Accepted for publication 12 May 2022
Published 30 May 2022

Abstract
Free-space quantum communication assumes importance as it is a precursor for satellite-based quantum communication needed for secure key distribution over longer distances. Prepare and measure quantum key distribution (QKD) protocols like BB84 consider the satellite as a trusted device, which is fraught with security threat looking at the current trend for satellite-based optical communication. Therefore, entanglement-based protocols must be preferred, so that one can consider the satellite as an untrusted device. The current work reports the effect of atmospheric aerosols on the key rate obtained with BBM92 QKD protocol, an entanglement-based QKD protocol over 200 m distance, using an indigenous facility developed at Physical Research Laboratory (PRL), Ahmedabad, India. Our results show that concentration and extinction coefficient of atmospheric aerosols play a major role in influencing the observed sift key rate, and eventually, the secure key rate. Such experiments are important to validate the models to account for the atmospheric effects on the key rates achieved through satellite-based QKD.

Keywords: entanglement through atmosphere, entanglement-based QKD, quantum communication, Atmospheric aerosols

(Some figures may appear in colour only in the online journal)

1. Introduction

In classical communication, the security of encryption keys for parties communicating with each other is an ongoing challenge. Even after 50 years of digital communication, the security depends upon the rigor of breaking the encryption, which may compromise the security of encrypted messages sent through a public channel once a quantum computer intercepts them. The demand for secure communication has increased with the development of quantum computers having sufficient numbers of good quality qubits becoming a practical reality. It has already been shown that by using Shor’s algorithm [1–3] the encryption used in key distribution between communicating parties [4] can be broken. Quantum key distribution (QKD), on the other hand, relies on the principles of quantum mechanics, like uncertainty principle, no-cloning theorem and monogamy of entanglement to securely distribute keys between the communicating parties [5, 6]. These principles make QKD safe even against a quantum computer while making no assumptions on Eve’s technological capability.

Every QKD protocol has distance limitations as the loss and disturbance in the channel increase with the transmission distance. Entanglement-based QKD (EBQKD) is ideal for long-distance quantum communication i.e. from satellite-to-ground, as it can make two distant ground stations communicate securely. In this case, irrespective of the satellite
distributing entangled photon pairs can be trusted or not the security is not compromised. It must be noted that the satellite-to-ground EBQKD has already been performed [7, 8]. The current limitation of using EBQKD is the low key rate, as the entangled photon pairs are generally produced via spontaneous parametric down-conversion (SPDC) [9, 10] process which is not very efficient. The two factors that contribute to low key rates are low-efficiency of the photon-pair generation, and loss of photons in the communication channel. Low efficiency can be compensated with the high-brightness high-fidelity photon-pair sources. On the other hand, one of the ways to mitigate the effect of channel is by studying its effect on parameters controlling the QKD. The controlled and quantitative studies to observe the influence of atmospheric conditions such as the presence of particulate matter (PM) or aerosols have not been considered earlier. In this study, we account the presence of aerosols and show its effect on the secure key rate, for the first time.

Atmospheric aerosols, solid or liquid particles suspended in air, are produced by natural sources and anthropogenic emissions. Mineral dust and sea salt particles are produced from natural sources while sulfate, nitrate, black carbon, and organic carbon are emitted primarily from emissions of fossil fuel and biomass burning/biofuels and/or converted into particles through gas-to-particle conversion mechanism. Atmospheric aerosols/PM can scatter and absorb the solar/shortwave radiation. For carrying out satellite-to-ground based communication, EBQKD, such as BBM92 protocol is the most suitable as it does not require a trusted node [11, 12]. In this article, we report the implementation of BBM92 protocol at the indigenously developed communication channel facility at PRL, and the effect of dust/atmospheric channel on the secure key rate. This is the first attempt, in India, which eventually will form a strong base for the future long-distance quantum communication.

The article is structured as follows: section 2 contains preliminaries about the BBM92 protocol, the entangled photon-pair source, and the indigenous facility built to study the atmospheric channel. Section 3 contains the results obtained and the related discussion. And finally, the concluding remarks are presented in section 4.

2. Background

BBM92 is a QKD protocol which involves pairs of entangled photons and can be regarded as an entanglement-based version of the BB84 protocol. BB84 is a prepare and measure based QKD protocol where Alice randomly generates polarization states using random number generators whereas in BBM92 the randomness is inherent to the entangled photon pairs. The basic block diagram of the BBM92 protocol is shown in figure 1.

In this protocol, a common sender Charlie generates a pair of entangled photons and sends them to Alice and Bob through a quantum channel. Quantum channels can be free-space, water or optical fiber. Alice and Bob independently perform their measurements on a random basis. Once the measurement is done, both declare their basis choices through the public channel. Only those measurements contribute to key for which Alice and Bob have chosen the same basis, and the rest of the measurements are discarded. The key formed after this process is referred to as sifted key. To compensate for any secrecy loss during the basis reconciliation through classical channel, error correction (EC) and privacy amplification (PA) are performed on sifted key to get a secure key. In our experiment, the quantum channel between Charlie and Alice is not exposed to atmospheric aerosols as both are co-located in the same room. However, the quantum channel between Charlie and Bob experiences the free-space dusty atmospheric channels corresponding to 35 and 200 m respectively. Please note that Alice and Charlie need not be co-located. They can be in different locations, however, in the current study because of limited space availability, Alice and Charlie are located in the same place.

2.1. Entangled photon-pair source

An in-house developed polarization-entangled photon-pair source which is highly efficient and bright was set up using type-0 ppKTP crystal [13] and placed in a Sagnac interferometer. The working principle of this setup is well explained in the article [14]. The schematic of the experimental setup is shown in figure 2 [14]. A continuous-wave laser at the wavelength of 405 nm and output power of ~5 mW is used to pump a 30 mm long type-0 ppKTP crystal with a period \( \Lambda = 3.425 \mu m \). A lens \( L_1 \) of focal length 400 mm is used to focus the pump beam on the crystal to generate entangled photons using a novel experimental scheme based on polarization Sagnac interferometer consisting of a dual-wavelength polarizing beam splitter cube (D-PBS), two half-wave plates HWP\(_3\), HWP\(_4\), and two high reflecting (R>99%) mirrors M\(_1\), M\(_2\) at 810 nm.
counting modules.

prism mirror, SMF: single-mode fiber, SPCM: single-photon bandpass filter of bandwidth 10 nm centered at 810 nm, PM:

L operate at 405 nm and 810 nm respectively. Lens L shown in the protocol diagram (figure

and getting reflected to reach the receiving end to Bob, as the quantum channel which includes going to the reflector at the receiving end with Alice and the other travels through nearby room. Out of every photon pair generated, one stays located in the present arrangement, while Bob is placed in the Charlie who prepares entangled photon-pairs and Alice are co-

ture and the placement of the equipment is shown in figure

D-PBS. The implemented scheme is robust against any optical path changes to produce SPDC photons in orthogonal polarizations with ultra-stable phase. The analyzer comprises a PBS and a HWP plate, and is used to measure the polarization entanglement of the generated photon pairs. The polarization entangled state generated from this method is:

\[ |\psi\rangle = \frac{1}{\sqrt{2}} (|HH\rangle + |VV\rangle). \]

2.2. Communication channel and their positioning

Our communication channel consists of arrangements on two buildings, located nearby, in the Thaltej campus of PRL. The sending and receiving ends are located on the same terrace in two separate rooms. There are two reflectors—one for a path length of 35 m and another for 200 m on the other building to reflect back the photons. The reflector consists of a 1 inch diameter mirror placed on a dedicated structure built for this purpose. The channels run through a free-space open atmosphere to investigate and quantify the effect of aerosols/dust on the protocols. The schematic of the building structure and the placement of the equipment is shown in figure 3. Charlie who prepares entangled photon-pairs and Alice are colocated in the present arrangement, while Bob is placed in the nearby room. Out of every photon pair generated, one stays at the receiving end with Alice and the other travels through the quantum channel which includes going to the reflector and getting reflected to reach the receiving end to Bob, as shown in the protocol diagram (figure 1). The complete optical setup is shown in figure 4. The experiment was performed at night (11 PM-5 AM Indian Standard Time, +05.30 hrs UTC), in order to ensure that there is no interference due to the direct sunlight.

3. Results and discussion

To quantify the influence of aerosols/dust present in the atmospheric channel on the secure key rate, we performed the experiment for 35 m channel on 8 May 2021, and 200 m channel on 10 May 2021. The atmospheric conditions for these two days are summarized in table 1. The extinction coefficient (Ext.) in the table represents the loss of photons due to absorption and scattering, which depends on the concentration of atmospheric aerosols, their size distribution, and refractive index. Aerosol characteristics reported here are measured in Aerosol Monitoring Laboratory, PRL. The extinction coefficient measured using CAPS PM monitor (Aerodyne Research Inc. USA) and aerosol size distribution and PM less than 2.5 micrometer diameter are measured using an aerosol spectrometer (GRIMM Aerosol Technik, Germany). The aerosol extinction coefficient on 10 May 2021 is lower by \( \sim 37\% \) (table 1) indicating a clear atmosphere and thereby more transmissivity through channel. Also, PM2.5 concentration is lower. Thus, choosing these two different days have provided the variability in the atmospheric conditions, most suitable for this study. Ahmedabad is a densely populated (ca.7 million) location with several small, medium and large-scale industries. Thar desert is located in the northwest direction of Ahmedabad. This environmental setting results in a pronounced amount of aerosol emissions from fossil fuel and biomass burning activities from their domestic usage and in vehicles as well as industries, and dust particles predominantly during pre-monsoon. In addition, two thermal power plants (located at a distance of 10 and 25 km respectively) also contribute to aerosol emissions. During the pre-monsoon season (May) the winds originate from and travel through the adjacent semi-arid and arid regions to the west of India, with typical wind speeds of about 3–4 m s\(^{-1}\) [15].

Ahmedabad experiences a typical tropical, humid climate with dry winter (low temperature and low relative humidity, and humid summer (high temperature and high relative humidity). In Ahmedabad, aerosol extinction coefficients exhibit a seasonal pattern; the values become higher due to lower wind speeds and shallow atmospheric boundary layer [15].

The channel transmissivity was measured by sending a beacon laser beam of 810 nm through the channels, which are found to be 94\% for 35 m and 70\% for 200 m, respectively. The loss in the quantum channel (optical link) is about 30\% for 810 nm wavelength. In Alice’s setup the loss due to single-mode fiber and detection efficiency makes it 90\%, whereas the same loss at Bob’s site is 60\%. Bob’s collection efficiency is more due to the use of multimode fiber for photon detection. Losses in the detection optics of both the systems is less than 1\%. The power of laser was measured before the launching
Figure 3. Arrangement of various components in the channel. It includes the location of Alice and Bob, and their setups. (a) Aerial view of free space entanglement-based QKD channel (Image courtesy: Google earth), (b) optical setup of Alice. Red solid lines indicate the direction of entangled photon pair. Out of each pair generated, one stays with Alice and another goes to Bob (c) non-LOS channel consist of one reflecting mirror, (d) front view of Alice and Bob room, (e) optical setup of Bob, (f) preparation of entangled photon pair source (EPS).

Figure 4. Schematic of the complete experimental setup that includes both optical and electronic arrangements. EPS: entangled photon source, FM: flip mirror, PM: prism mirror, M: mirror, F: filter, FC: fiber coupler, BS: beam splitter, PBS: polarization beam splitter, HWP: half wave plate, SMF: single-mode fiber, MMF: multi-mode fiber, SPCM: single-photon counting modules.

optics and after the collecting optics to estimate the channel transmissivity on both days. The use of a beacon laser was crucial for precise alignment, and also to make further corrections required, if any, due to the changes in breeze (winds) on both days.

Eight detectors are used in the experiment, four each for Alice and Bob respectively (figure 4). Analogous to any classical communication protocol, BBM92 also requires timing synchronization between communicating parties to distribute keys correctly. We connected the SPCM4 and SPCM8 to time-tagger ID900, and found the time-difference between Alice and Bob to be 120 ns for ~35 m, and 666 ns for ~200 m channels (figure 5), respectively, based on the histogram obtained for the two channels. The coincidences were measured with a time-window of 1 ns.

We started with the effect of channel on the entanglement distribution between Alice and Bob, and measured the H/V/D/A polarization visibilities. The brightness of the
Table 1. Extinction coefficient (Ext.) and particulate matter (PM2.5) concentrations are averages of hourly data from 11 PM to 5 AM obtained from the Aerosol Monitoring Laboratory, PRL. The extinction coefficients data correspond to 525 nm. The data when fitted with the Angstrom power law for urban aerosols (model) corresponding to 70% relative humidity (appropriate for April–May) yielded a wavelength exponent value of 1.5 for extinction coefficients between 525 and 800 nm. Mm: Mega meter.

| Date       | Ext. (Mm$^{-1}$) | PM2.5 (µg m$^{-3}$) |
|------------|-----------------|----------------------|
| 8 May 2021 | $\gamma_{35} = 76.41 \pm 7.78$ | $2.87 \pm 0.26$     |
| 10 May 2021| $\gamma_{200} = 48.67 \pm 6.70$ | $1.68 \pm 0.24$    |

Figure 5. Time delay between Alice and Bob for 200 meters as observed from coincidence histogram.

Figure 6. Obtained H/V/D/A graphs for 35 m channel taken on 8 May 2021. Solid lines are theoretical fit and lines of 98% confidence interval.

Figure 7. Obtained H/V/D/A graphs for 200 m channel taken on 10 May 2021. Solid lines are theoretical fit and lines of 98% confidence interval.

Table 2. Summary of the parameters obtained for 35 m channel on 8 May 2021, and 200 m channel on 10 May 2021.

| Parameters | 35 m | 200 m |
|------------|------|-------|
| Channel transmission (%) | 94   | 70    |
| CHSH Bell parameter (S) | $2.51 \pm 0.06$ | $2.54 \pm 0.06$ |
| Mean visibility (%) | $88.85 \pm 5.39$ | $90.99 \pm 5.89$ |
| QBER (%) | 5.58 | 4.50  |
| Sifted key rate (kbps) | 6.37 | 4.89  |
| Key rate after EC (kbps) | 6.01 | 4.20  |
| Key rate after PA (kbps) | 2.33 | 1.71  |
| Secure key rate (kbps) | 2.33 | 1.71  |

The entangled photon source is 0.3 KHz mW$^{-1}$ nm$^{-1}$ and the fidelity is 92.76%. The graphs corresponding to measurements for 35 m and 200 m are shown in figures 6 and 7. The visibilities obtained for 35 m channel on 8 May 2021 were 93.17%, 93.71%, 85.39% and 83.12% for H/V/D/A, respectively. The mean of these visibilities is 88.85%. For 200 m channel on 10 May 2021, the respective visibilities were 92.16%, 93.72%, 88.76% and 89.34%. The mean of these visibilities is 90.99%. The parameters obtained for both the distances are summarized in table 2. An $S$ value greater than 2 ensures that secure key distribution can be done over the given channel. These results show that the atmosphere (amount of atmospheric aerosols) plays a crucial role in modulating the visibilities. As the extinction coefficient is lower on 10 May (table 1), the visibilities are higher despite the channel length being longer. The total count rate is a combined effect of channel losses and the length of the channel.

The quantum bit-error-rate ($Q$) and sifted key rate (SKR) can be calculated as [16, 17]:

$$Q = \frac{1 - \text{Visibility}}{2}. \quad (2)$$

The value of $Q$ for 35 m is 5.58% and for 200 m it is 4.50%. The SKR can be calculated from the coincidence counts rates ($cc$) as:

$$R_{sift} = 4 \times cc. \quad (3)$$

The factor 4 accounts for the total of all four coincidences ($HH$, $VV$, $DD$ and $AA$), as the correct number of coincidences will contribute to total SKR. The secret key rate after the EC is given by:

$$R_{sec} = n \left( \frac{1}{2} - 2 \times Q - s \right), \quad (4)$$
where \( n \) is the number of bits left after EC, and \( s \) is the security parameter [18]. The lower value of \( R_{sec} \) is a direct consequence of worse atmospheric conditions, which is also consistent with the visibilities. The different key rates obtained for both the distances are summarized in table 2.

The measured channel transmission is 0.94 for 35 m and 0.70 for 200 m on the two dates of the experiment. As the atmospheric condition follows Beer–Lambert law [19], the transmission \( T \) of the channel can be written in terms of the number of photons sent \( (N_{in}) \) and the number of photons received \( (N_{out}) \) on the other end of the free space atmospheric channel as:

\[
T = \frac{N_{out}}{N_{in}} = Sc \ exp(-1.5 \times \gamma L),
\]

where \( Sc \) is the scaling parameter, \( \gamma \) is the extinction coefficient of the atmosphere, and \( L \) is the propagation length. The scaling parameter contains all the losses except the atmospheric effect. With the transmission information, we obtained the values \( Sc_{35} = 0.944 \) and \( Sc_{200} = 0.710 \), respectively. It is clear from equation (5) that both distance and extinction coefficient equally affect the channel transmissivity. In our study, the distances are of the order of tens of meters (35 and 200 m) and the extension coefficients are 76.41 and 48.67 Mm\(^{-1}\) on 8 May 2021 and 10 May 2021, respectively. For 200 m, photons are more exposed to the atmosphere than 35 m. Due to more exposure, many photons get scattered and absorbed by the atmospheric aerosol, thereby reducing the transmissivity and hence the secure-key rate.

Comparing the atmospheric conditions including the channel lengths for 8 May and 10 May, the transmission \( (T) \) ratios \( f \) can be written as:

\[
f = \frac{Sc_{35} \ exp(-1.5 \times \gamma_{35} L)}{Sc_{200} \ exp(-1.5 \times \gamma_{200} L)} = 1.34.
\]

From our channel and experiments, the similar ratios are observed for the coincidence rates \( (cc) \), SKR \( (R_{skf}) \) and secured key rates \( (R_{sec}) \), as shown by:

\[
\frac{cc_{35}}{cc_{200}} = 1.28,
\]

\[
\frac{R_{skf \ 35}}{R_{skf \ 200}} = 1.30, \quad \text{and}
\]

\[
\frac{R_{sec \ 35}}{R_{sec \ 200}} = 1.36.
\]

Similar R values suggest that the Beer–Lambert law is suitable for considering the atmospheric aerosols and is consistent with the quantum parameters observed from the channel. One of the reasons is the linear dependence of SKR on the coincidences observed per second. Moreover, the free space channel does not introduce any polarization changes to the photons [20, 21]. To obtain the key rates for any other day, the new factor \( f \) need to be calculated from equation (6) and similarly the other parameters can be obtained using equation (7).

To determine the secure key, the time tags for all the eight channels have been recorded using the eight-channel digital oscilloscope (Tektronix MSO68B 6-BW-2500). The oscilloscope has a bandwidth of 2.5 GHz, and it was used to record the TTL pulses coming from single-photon detectors with a sampling rate of 1.25 GS s\(^{-1}\) with an integration time of 40 ms to measure the key rate. The recorded data contains the voltage sample, and the arrival time is obtained from the rising edge of TTL pulses. The post-processing includes basis reconciliation, error estimation, EC, and PA, which are implemented in MATLAB. We have implemented a low-density parity-check (LDPC) EC code [22] with a code rate of 0.5 for EC. Choice of LDPC matrices closely depends on QBER and directly affects the secure key rate. Higher QBER indicates that more parity bits are needed to correct the errors which reduces the key rate.

Once error-corrected keys are generated, PA [23] is done via 2-universal Toepitz hash function. During PA, the length of the hashed output is chosen pertaining to the parity bits used in EC, QBER, and security parameter which decides the final length of the secure key.

4. Conclusion

In conclusion, we have implemented, BBM92 protocol, an EBQKD protocol, over 35 m and 200 m free-space atmospheric channel, and simultaneously studied the effect of atmospheric aerosols on the secure key rate. This is the first study of its kind where the extinction coefficient of atmospheric aerosols is used to study the variation of entanglement, QBER and key rate. We found that the key rate follows the extinction coefficient of the atmospheric aerosols on that particular day. As the key rate depends on the channel length, the larger the channel, the smaller will be the key rate. Further experiments are planned to study the effect for longer duration and to check the validity of models for estimating the key rate due to atmospheric conditions for the satellite-based quantum communications [24]. The present findings will be useful in setting up quantum communication network using satellites and enable a proper placement of entanglement photon-pair sources.

Data availability statement

All data that support the findings of this study are included within the article (and any supplementary files).

Acknowledgments

Authors thank Dr T A Rajesh and Vishnu Kumar Dhaker for providing the aerosol extinction and PM data for 8 and 10 May 2021. Authors also acknowledge the financial support from DST through the QuST program.
Conflict of interest

The authors declare no conflicts of interest related to this article.

ORCID iDs

Sarika Mishra  https://orcid.org/0000-0001-7645-7849
Shashi Prabhakar  https://orcid.org/0000-0002-7337-8755
S Ramachandran  https://orcid.org/0000-0003-4921-7887

References

[1] Shor P W 1994 Algorithms for quantum computation: discrete logarithms and factoring Proc. 35th Annual Symp. on Foundations of Computer Science (IEEE) pp 124–34
[2] Beckman D, Chari A N, Devabhaktuni S and Preskill J 1996 Phys. Rev. A 54 1034
[3] Ekert A and Jozsa R 1996 Rev. Mod. Phys. 68 733
[4] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[5] Bennett C and brassard G 1984 Quantum cryptography: Public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore) pp 175–9
[6] Ekert A K 1991 Phys. Rev. Lett. 67 661
[7] Yin J et al 2017 Phys. Rev. Lett. 119 200501
[8] Ribordy G, Brendel J, Gautier J D, Gisin N and Zbinden H 2000 Phys. Rev. A 63 012309
[9] Harris S E, Oshman M K and Byer R L 1967 Phys. Rev. Lett. 18 732–4
[10] Kwiat P G, Mattle K, Weinfurter H, Zeilinger A, Sergienko A V and Shih Y 1995 Phys. Rev. Lett. 75 4337–41
[11] Waks E, Zeevi A and Yamamoto Y 2002 Phys. Rev. A 65 052310
[12] Scherer A, Sanders B C and Tittel W 2011 Opt. Express 19 3004–18
[13] Steinlechner F, Gilaberte M, Jofre M, Scheidl T, Torres J P, Pruneri V and Ursin R 2014 J. Opt. Soc. Am. B 31 2068–76
[14] Jabir M and Samanta G 2017 Sci. Rep. 7 1–8
[15] Ramachandran S, Rajesh T and Cherian R 2021 Atmos. Res. 256 105573
[16] Scheidl T et al 2009 New J. Phys. 11 085002
[17] Neumann S P, Scheidl T, Selimovic M, Pivoluska M, Liu B, Bohmann M and Ursin R 2021 Phys. Rev. A, 104 022406
[18] Bennett C, Brassard G, Crepeau C and Maurer U 1995 IEEE Trans. Inf. Theory 41 1915–23
[19] Beer A 1852 Ann. Phys. 162 78–88
[20] Yin J et al 2020 Nature 582 501–5
[21] Ursin R et al 2007 Nat. Phys. 3 481–6
[22] Limei G, Qi R, Di J and Duan H 2020 Int. J. Theor. Phys. 59 1717–29
[23] Bennett C, Brassard G, Crepeau C and Maurer U 1995 IEEE Trans. Inf. Theory 41 1915–23
[24] Vasylyev D, Vogel W and Moll F 2019 Phys. Rev. A 99 053830