Background noise of satellite-to-ground quantum key distribution

Miao Er-long\textsuperscript{1}, Han Zheng-fu\textsuperscript{1,3}, Gong Shun-sheng\textsuperscript{2}, Zhang Tao\textsuperscript{1}, Diao Da-sheng\textsuperscript{1} and Guo Guang-can\textsuperscript{1}

\textsuperscript{1} Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei, Anhui 230026, People’s Republic of China
\textsuperscript{2} Wuhan Institute of Physics and Mathematics of the Chinese Academy of Sciences, People’s Republic of China
E-mail: zfhan@ustc.edu.cn

New Journal of Physics 7 (2005) 215
Received 1 July 2005
Published 10 October 2005
Online at http://www.njp.org/
doi:10.1088/1367-2630/7/1/215

Abstract. The influence of background light on satellite-to-ground free-space quantum key distribution (QKD) is investigated. By comparing the number of noise photons to that of the signal photons per pulse, the technical requirements for a practical system are evaluated. We show that satellite-to-ground QKD is feasible with currently available technology even under full moonlight.

Contents

1. Introduction 2
2. Background light noise and methods of prevention 2
   2.1. Time-gate filter .................................. 3
   2.2. Frequency (wavelength) filter ........................... 3
   2.3. Spatial filter .................................... 4
3. Background light 5
4. System efficiency and influence of the atmosphere 5
5. Conclusion 7
Acknowledgments 7
References 7

\textsuperscript{3} Author to whom any correspondence should be addressed.
1. Introduction

In 1984, Bennett and Brassard [1] proposed a scheme for secure quantum key distribution (QKD) which came to be known as the BB84 protocol and was first demonstrated by Bennett et al [2] in 1989 over 32 cm in free space. Over the past five years IBM, QinetiQ, NEC and id Quantique have conducted QKD experiments through more than 50 km long optical fibre in the laboratory. In 2002, QKD over a distance of 67 km was achieved in a commercial optical cable under Lake Geneva by Gisin’s group [3]. Recently, we achieved highly stable QKD over 125 km of optical cable between Peking and Tianjin in China, and over 150 km in the laboratory [4]. All this progress indicates that the technology of point-to-point QKD over optical fibre has reached maturity. Now, one-to-any and any-to-any network protocols [5]–[12] have become a topic of hot interest. It is anticipated that a practical local QKD network will emerge in the near future.

However, it is difficult to distribute the quantum key through more than 200 km of fibre because of absorption losses and the low single-photon detection efficiency. Free space QKD is now attracting new attention [13]–[19] because of its low-transmission loss. It is well known that the density of the atmosphere decreases rapidly with the increase of altitude, so transmission losses caused by atmospheric absorption can be neglected beyond a height of 10 km. Therefore, satellite-to-ground QKD is always applicable in principle if only the transmission losses have to be considered. However, due to the complexity of the atmospheric layers, there are many other factors besides transmission losses that have a detrimental influence, such as weather, vortices, cirrus clouds, etc. A crucial question is whether the information carried by single photons can be distilled at the ground station after being transmitted through the atmosphere over thousands of kilometres. Following the efforts of several groups [13]–[16], in 2002 Hughes et al [17] were the first to realize free-space QKD over a distance exceeding 10 km. This was then surpassed by Weinfurter’s group who achieved a record of 23.4 km on the mountain tops of the Alps [18]. This distance exceeds the height of the atmospheric air mass, thus proving that satellite-to-ground QKD could be realized if atmospheric absorption were the only factor to be considered. Once this is realized, local area network QKD systems can be connected by satellites to form worldwide area network systems. Rarity et al [19] proposed three schemes to realize satellite-to-ground QKD in 2002. They calculated the losses, quantum key rate and dark counts, and concluded that with current technology satellite-to-ground QKD is feasible in principle. However, they did not make particular mention of the background light, which is the main cause of the quantum-bit error rate (QBER). In fact, background light is far more serious than the dark counts of the single-photon detector (SPD). How to overcome the background noise is one of the crucial technologies in satellite-to-ground QKD. In this paper, we put the sender Alice on the satellite and the receiver Bob on the ground, according to the scheme of [19]. We pay particular attention to the effects of the background light. The technical requirements of the satellite-to-ground QKD system are obtained by analysing the noise photons from the background received by the system according to the brightness of the sky.

2. Background light noise and methods of prevention

Just as in classic communication, successful QKD depends on the signal-to-noise ratio (SNR). Classic communication can increase the signal power or decrease the noise of the environment to
improve the SNR, but QKD uses a single photon as a quantum bit (qubit) to carry the information and no pulse is allowed to contain more than one photon, so the only way to improve the SNR is to decrease the noise.

The SNR is defined as the average number of signal photons to the number of noise photons per pulse detected by the SPD. Dark counts and background light are the two main noise sources. Silicon-based avalanche photodiodes can have a dark count less than 25 counts s$^{-1}$. In free space, the beam path is open to the outside so any background radiation can enter the system as noise, especially during satellite-to-ground QKD. In most situations background light contributes far more to the noise than the dark counts of the detector so it is crucial to shield the system from the background.

There are two classes of background light in the sky. One is the radiation or reflection from the sun, moon and stars. This light travelling through the atmosphere will be scattered by molecules, aerosols, fog and clouds, then collected by the receiving telescope as background noise. Even on a moonless night this noise is detected by the SPD. The other class is light created by human beings, such as city light scattered by the environment, but this can be avoided by selecting a suitable site far from cities. In this paper, only the former type of background is considered. In addition, the satellite itself may be illuminated by the sun and become an important noise source even at night. For our purpose, we will take the bright satellite as a sixth magnitude star. Generally, three methods can be used to shield against the noise light and improve the system SNR, as discussed below.

2.1. Time-gate filter

In order to decrease the number of background photons, as well as the dark counts, most of the time the SPD is in the off mode. Only when the signal photons are expected to arrive is a narrow time gate opened to allow them to enter the photodiode, thus noise photons arriving outside the time window are blocked. The narrower the time gate, the more efficient this method is. However, a narrow time gate requires precise knowledge of the signal photon’s arrival time, that is, precise synchronization between the sender and receiver is needed. There are two ways to achieve this. One utilizes a local 10 MHz quartz crystal oscillator and a software-controlled phase-lock loop driven by the detected photon signal, by means of which the system can be synchronized to 1 ns [20]. The other method [21] uses a periodic bright pulse of a different wavelength as precursor to open a time gate for the subsequent signal photon. The former has a key rate of several hundred bits per second and needs timing adjustment every 100 ms. The latter has a key rate comparable to the attenuated signal pulses but has the problem that light interference from the bright synchronous pulse must be avoided and coaxiality of the two different wavelengths must be maintained. In fact, satellite-to-ground QKD must be assisted by an acquisition, tracking and pointing (ATP) system, whose synchronized beacon light can serve as the QKD synchronization signal. Currently, we prefer the latter method.

2.2. Frequency (wavelength) filter

Usually the background light is of continuous wavelength so a narrow band filter must be used before the detector. The three most commonly used filters are the interference, birefringence and atom filters. Interference filters have a bandwidth of approx. 10–0.2 nm and a transmittance...
The bandwidth of birefringence filters is 0.1 nm while the transmittance is below 20%. Atom filters are relatively better with a bandwidth of 0.01 nm and transmittance above 90% [24], so they seem to be the best selection. However, a satellite is a moving target so the Doppler effect has to be considered if an atom filter is used. If the source is located on the satellite and the observer on the ground, the detected frequency \( f \) is given by

\[
f = f_0 \frac{v}{v - v_r},
\]

where \( f_0 \) is the emission frequency of the source. For a source wavelength of 650 nm and satellite velocity of 7.8 km s\(^{-1}\), the Doppler shift will be approximately 0.01 nm, which needs to be compensated if atom filters are used. In addition, the output wavelength of a diode laser drifts by approx. 0.12 nm/°, thus the temperature must be controlled within 0.1°.

2.3. Spatial filter

In principle, the smaller the numerical aperture (NA) of the detector, the less background noise collected. However, a small NA requires a highly precise ATP system, and in addition, changes in the weather and atmosphere also have to be considered.

2.3.1. ATP precision. An ATP system is needed to establish the optical link between two remote targets before communication and key distribution so its stability and efficiency are crucial factors. In free-space optical communication the spot size at the collecting telescope should be small enough so that most of the signal light can be collected, and this requires small divergence of the signal beam as well as a highly precise ATP system. If the ATP aberration is ±\( \varepsilon \), the spot size of the beam should be big enough to cover the receiving telescope at this aberration. A big spot on a relatively small telescope means low-collection efficiency. In other words, the ATP aberration determines the spot size of the receiving beam and the receiving efficiency. To our knowledge it is not difficult to achieve an accuracy better than 10 µrad in an ATP system now. This means that the field of view of the collecting telescope and the spot size must be bigger than the 10 µrad aberration. Atmospheric turbulence will degrade the situation and its influence will be discussed in the following section.

2.3.2. Atmosphere turbulence. Turbulence can lead to both spreading and wandering of the laser beam. If the beam diameter is smaller than the scale of the turbulent current, the direction of the beam will change randomly. Moreover, there are lens and speckle effects of the turbulence. Typical wander will be approximately 10 µrad if the receiving station is on a high-altitude mountain (over 2000 m). At worst, this wander can reach 100 µrad at sea level. Following the scheme of [19], we suppose that the sender Alice is on the satellite and the receiver Bob is on a 2000 m high mountain. According to their data and taking into consideration the effective thickness of the atmosphere, we estimate that the wander and spreading caused by the turbulence will be less than 1 m.
3. Background light

If the telescope parameters and brightness of the sky are given then the noise received by the system can be computed. The power received by telescope $P_b$ can be expressed as follows:

$$P_b = H_b \times \Omega_{\text{fov}} \times A_{\text{rec}} \times \text{B}_{\text{filter}},$$  \hspace{1cm} (2)

where $H_b$ is the brightness of the sky background in $\text{W m}^{-2} \text{Sr} \mu\text{m}$, and $A_{\text{rec}}$, $\Omega_{\text{fov}}$ and $\text{B}_{\text{filter}}$ are the telescope aperture, field of view and filter bandwidth respectively. It is easy to see from equation (1) that reducing the field of view and using a narrowband filter helps to decrease the noise. Reducing the aperture will reduce the noise as well as the signal so it is not an effective way to improve the SNR. A time gate blocks noise outside the gate so the SNR will be relatively improved. The value of $H_b$ changes greatly with weather conditions. In table 1 typical values for the background noise are listed [22, 23]. For a bandwidth from 0.53–1.06 $\mu\text{m}$, the brightness of an illuminated cloud is 120–240 $\text{W m}^{-2} \text{Sr} \mu\text{m}$. We take 150 $\text{W m}^{-2} \text{Sr} \mu\text{m}$ as a typical value.

Here, the receiving telescope’s aperture is 1 m ($A_{\text{rec}} = 0.785 \text{m}^2$), the time gate 1–3 ns and the receiving field 100 $\mu\text{rad}$, with the turbulence influence taken into consideration. Based on current technology, we can obtain the number of background photons received per pulse for several typical conditions in a satellite-to-ground QKD system.

For the observer on the ground, reflection from the satellite is also an important source of noise. In table 1, we take this as a sixth magnitude star, and the number of noise photons it creates is added as the second term in the boxes containing a ‘+’ sign. The sum is the actual number of photons received by the system. It is evident that the reflection from the satellite is not a significant part of the background.

4. System efficiency and influence of the atmosphere

It is known that when the atmosphere is clear there is very high transmittance in certain windows. Higher than 10 km above sea level the atmosphere becomes rarefied, and absorption and scattering can be neglected. In clear weather the transmittance can be improved to 65% by selecting a proper wavelength [20], but in bad weather when there are clouds, rain or fog, noise and losses increase so quickly that QKD fails. This is the problem encountered in all free-space communication. If the ground station can be established on a high mountain, most losses caused by the atmosphere can be avoided. The divergence half-angle $\theta$ of a Gaussian beam with radius $\omega_0(1/e^2)$ is given by

$$\theta = \frac{\lambda}{\pi\omega_0},$$  \hspace{1cm} (3)

where $\lambda$ is the laser wavelength and $\omega_0$ is equal to half the diameter $D$ of the collimating telescope. Considering the satellite’s allowed payload, we take $D = 10 \text{ cm}$, transmission distance $L = 1000 \text{ km}$ and $\lambda = 650 \text{ nm}$. After propagation over 1000 km the spot size becomes 8 m in diameter (it should be less than 10 m to account for atmospheric turbulence). In order to receive the signals from the satellite an ATP system with an accuracy better than 5 $\mu\text{rad}$ is required. If we intercept a large Gaussian beam of diameter $2\omega$ with a small telescope of diameter $D_T$ then

New Journal of Physics 7 (2005) 215 (http://www.njp.org/)
the collected fraction is

$$\eta = 1 - \exp \left[ -\frac{2D_T^2}{(2\omega^2)} \right] \approx \frac{D_T^2}{2\omega^2}. \tag{4}$$

Here, we take $D_T = 1$ m so the losses are 17 dB. If the transmittance is 60%, SPD efficiency 70%, number of photons per pulse 0.1 and coupling efficiency 80%, then the number of signal photons received by the ground station is $6 \times 10^{-4}$ per pulse. At present, the dark count of silicon-based SPD is about 25 counts s$^{-1}$ which will cause $2.5 \times 10^{-7}$ counts pulse$^{-1}$ if the width of the time gate is 10 ns, which contributes less than 0.2% to the error rate. Compared with the data in table 1, background light contributes far more than the dark counts of the SPD and is thus the main source

| Conditions | Cloudy daytime | Hazy daytime | Clear daytime | Full moon clear night | New moon clear night | Moonless clear night |
|------------|----------------|--------------|---------------|----------------------|---------------------|---------------------|
| Relative brightness | 1.0 | $10^{-1}$ | $10^{-2}$ | $10^{-5}$ | $10^{-6}$ | $10^{-7}$ |
| Typical brightness (W m$^{-2}$ Sr $\mu$m) | 150 | 15 | 1.5 | $1.5 \times 10^{-3}$ | $1.5 \times 10^{-4}$ | $1.5 \times 10^{-5}$ |
| Photons pulse$^{-1}$ | | | | | | |
| $\theta = 100 \mu$rad $B = 0.2$ nm $t = 3$ ns | 7.4 | $7.4 \times 10^{-1}$ | $7.4 \times 10^{-2}$ | $7.4 \times 10^{-5}$ | $7.4 \times 10^{-6}$ | $7.4 \times 10^{-7}$ |
| $\theta = 100 \mu$rad $B = 0.2$ nm $t = 1$ ns | 2.5 | $2.5 \times 10^{-1}$ | $2.5 \times 10^{-2}$ | $2.5 \times 10^{-5}$ | $2.5 \times 10^{-6}$ | $2.5 \times 10^{-7}$ |
| $\theta = 10 \mu$rad $B = 0.01$ nm $t = 1$ ns | $1.3 \times 10^{-1}$ | $1.3 \times 10^{-2}$ | $1.3 \times 10^{-3}$ | $7.4 \times 10^{-6}$ | $1.3 \times 10^{-7}$ | $1.3 \times 10^{-8}$ |
| $\theta = 10 \mu$rad $B = 0.2$ nm $t = 3$ ns | $7.4 \times 10^{-2}$ | $7.4 \times 10^{-3}$ | $7.4 \times 10^{-4}$ | $7.4 \times 10^{-7}$ | $7.4 \times 10^{-8}$ | $7.4 \times 10^{-9}$ |
| $\theta = 10 \mu$rad $B = 0.2$ nm $t = 1$ ns | $2.5 \times 10^{-2}$ | $2.5 \times 10^{-3}$ | $2.5 \times 10^{-4}$ | $2.5 \times 10^{-7}$ | $2.5 \times 10^{-8}$ | $2.5 \times 10^{-9}$ |
| $\theta = 10 \mu$rad $B = 0.01$ nm $t = 3$ ns | $3.7 \times 10^{-3}$ | $3.7 \times 10^{-4}$ | $3.7 \times 10^{-5}$ | $3.7 \times 10^{-8}$ | $3.7 \times 10^{-9}$ | $3.7 \times 10^{-10}$ |
| $\theta = 10 \mu$rad $B = 0.01$ nm $t = 1$ ns | $1.3 \times 10^{-3}$ | $1.3 \times 10^{-4}$ | $1.3 \times 10^{-5}$ | $1.3 \times 10^{-8}$ | $1.3 \times 10^{-9}$ | $1.3 \times 10^{-10}$ |
of noise. If we take 10% error rate as the security limit for QKD, then the noise counts must be less than $6 \times 10^{-5}$ counts pulse$^{-1}$. In fact, there are also other factors that increase the error rate through depolarization of the signal, such as cirrus clouds, the Faraday effect of the ionosphere, reflection at curved mirrors and satellite rotation and vibration. So far theory and experiments show that their total influence is less than 2%, and some of them can be corrected and avoided. As an estimate it can be assumed that their combined error rate is less than 5%, so the system can tolerate a background noise of up to $3 \times 10^{-5}$ counts pulse$^{-1}$.

From the above calculations, we can deduce the requirements and conditions for the realization of a practical system. As shown in table 1, satellite-to-ground QKD can be realized at the right of the black thick line. But on the left, security is ruined by the noise. If adaptive optics could be used to reduce the influence of the atmosphere, signal-receiving efficiency could be improved and the system would be able to resist higher background noise [25]. In addition, in practical QKD, coherent states are used that contain on average 0.1 photons pulse$^{-1}$ as the source because real single-photon sources are difficult to obtain. But a source that contains multiphotons becomes insecure due to increased losses with increasing transmission distance. There have been recent studies [26] and some proposals [27, 28] on how to overcome this problem. For example, Lo et al [29], Scarani et al [30] and Wang [31] have proposed the so-called decoy state protocol. They proved that the coherent state is a good source for secure QKD for a certain error rate, and that the system is still secure in spite of high losses if decoy states are used. With all these new emerging technologies and methods it is hopeful that ground-to-satellite QKD can be realized in even more difficult situations.

5. Conclusion

In this paper, we have discussed the main source of noise, i.e. background noise, encountered in satellite-to-ground QKD and the ways to overcome it. We have computed the noise counts and their influence on the system. Results show that, on a moonless night, it is fairly easy to realize satellite-to-ground QKD, while at new moon and full moon more advanced technologies such as higher precision ATP systems, narrower atom filters etc are required. In the daytime, however, it is very difficult to avoid the influence of noise and keep the system in the secure region. Nevertheless, all-day satellite-to-ground QKD could become a reality with the development of new optics and semiconductor technology.

Acknowledgments

Special thanks are given to Professor Wu Ling-An for her great help in the syntax. This work was funded by the National Fundamental Research Program of China (grant no. 2001CB309301), National Natural Science Foundation of China (grant no. 60121503) and the Innovation Program of the Chinese Academy of Sciences.

References

[1] Bennett C H and Brassard G 1984 Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (New York: IEEE) pp 175–9
[2] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 J. Cryptology 5 3–28
[3] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 New J. Phys. 4 41
[4] XiaoFan M O et al 2005 Opt. Lett. in press
[5] Phoenix S J D, Barnett S M and Townsend P D 1994 J. Mod. Opt. 42 1155
Townsend P D, Phoenix S J D and Blow K J 1994 Electron. Lett. 30 1875
[6] Yoshihiro N et al 2003 US Patent Specification 2003002674
[7] Deng F G, Liu X S and Ma Y J 2002 Chin. Phys. Lett. 19 893
[8] Gingrich R M, Kok P and Lee H 2003 Phys. Rev. Lett. 91 217901
Guo G P and Guo G C 2003 Phys. Lett. A 318 337
Kozhekin A E, Molmer K and Polzik E 2000 Phys. Rev. A 62 033809
[9] Biham E, Huttner B and Mor T 1996 Phys. Rev. A 54 2651
[10] Xue P, Li C F and Guo G C 2002 Phys. Rev. A 65 022317
[11] Hirose S et al 1997 Inform. Process. Lett. 62 189
[12] Townsend P D et al 1997 Nature 385 47
Townsend P D et al 1997 Electron. Lett. 33 188
Townsend P D et al 1998 Opt. Fiber Technol. 4 345
Townsend P D et al 1993 European Patent Application EP3307121.9
Townsend P D et al 1993 European Patent Application EP3307121.0
[13] Buttler W T, Hughes R J, Kwiat P G, Luther G G, Morgan G L, Nordholt J E, Peterson C G and
Simmons C M 1998 Phys. Rev. A 57 2319
Buttler W T, Hughes R J, Kwiat P G, Lamoreaux S K, Luther G G, Morgan G L, Nordholt J E, Peterson C G
and Simmons C M 1998 Phys. Rev. Lett. 81 3283
[14] Hughes R J, Buttler W T, Kwiat P G, Lamoreaux S K, Morgan G L, Nordholt J E and Peterson C G 2000
J. Mod. Opt. 47 549
Buttler W T, Hughes R J, Lamoreaux S K, Morgan G L, Nordholt J E and Peterson C G 2000 Phys. Rev. Lett.
84 5652
[15] Hughes R J, Nordholt J E, Derkacs D and Peterson C G 2002 New J. Phys. 4 43
Kurtsiefer C, Zarda P, Halder M, Weinfurter H, Gorman P, Tapster P R and Rarity J G 2002 Nature 419 450
[16] Rarity J G, Tapster P R, Gorman P M and Knight P 2000 New J. Phys. 4 82
Rarity J G, Rarity J G, Gorman P M and Tapster P R 2001 J. Mod. Opt. 48 1887
[17] Buttler W T, Hughes R J, Lamoureaux S K, Morgan G L, Nordholt J E and Peterson C G 2000 Rev. Lett.
84 5652–5
[18] Leinert Ch et al 1998 Astron. Astrophys. Suppl. Ser. 127 1
[19] Hansen V 1983 J. Appl. Meteorol. 23 772–80
[20] Xue-wu C, Fa-quan L, Zhao-xiang L, Dai Yang and Shun-sheng G 2003 Opt. Optoelectronic Technol. 1-1
[21] Tyson R K et al 2002 J. Opt. Soc. Am. A 19 753
[22] Lütkenhaus N and Jahn M 2002 New J. Phys. 4 44
[23] Scarani V, Acin A, Gisin N and Ribordy G 2002 Preprint quant-ph/02211131
[24] Lu Y J, Luobei Zhu and Ou Z Y 2005 Phys. Rev. A 71 032315
[25] Lo H -K, Xiongfei Ma and Kai Chen 2005 Phys. Rev. Lett. 94 230504
[26] Scarani V, Acin A, Ribordy G and Gisin N 2004 Phys. Rev. Lett. 92 057901
Wang X -B 2005 Phys. Rev. Lett. 94 230503