Performance optimization for quantum key distribution in lossy channel using entangled photons*

Yu Yang(杨玉)[1], Luping Xu(许录平)[1,†], Bo Yan(阎博)[1], Hongyang Zhang(张洪阳)[1], and Yanghe Shen(申洋赫)[2]

[1] School of Aerospace Science and Technology, Xidian University, Xi'an 710126, China
[2] Beijing Institute of Spacecraft System Engineering, Chinese Academy of Space Technology, Beijing 100094, China

(Received 28 April 2017; revised manuscript received 6 August 2017; published online 29 September 2017)

In quantum key distribution (QKD), the times of arrival of single photons are important for the keys extraction and time synchronization. The time-of-arrival (TOA) accuracy can affect the quantum bit error rate (QBER) and the final key rate. To achieve a higher accuracy and a better QKD performance, different from designing more complicated hardware circuits, we present a scheme that uses the mean TOA of M frequency-entangled photons to replace the TOA of a single photon. Moreover, to address the problem that the entanglement property is usually sensitive to the photon loss in practice, we further propose two schemes, which adopt partially entangled photons and grouping-entangled photons, respectively. In addition, we compare the effects of these three alternative schemes on the QKD performance and discuss the selection strategy for the optimal scheme in detail. The simulation results show that the proposed schemes can improve the QKD performance compared to the conventional single-photon scheme obviously, which demonstrate the effectiveness of the proposed schemes.

Keywords: quantum key distribution, time of arrival, quantum bit error rate, key rate

PACS: 03.67.Ac, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/26/11/110305

1. Introduction

In recent decades, the free space quantum key distribution (QKD)[1–3] has become a matured technic in the quantum communication field.[4–6] In the free space QKD, a crucial problem is to analyze the effects of practical noises on the QKD performance. The decrease in the number of signal photons caused by the transmission losses and the increase in the number of noise photons caused by background light commonly decide a lower signal-to-noise ratio (SNR).[7,8] A lower SNR will directly bring a higher quantum bit error ratio (QBER) and a lower key rate. It is not difficult to see that the effects of actual noises on the QKD performance essentially are its effects on the single photons. As the information carrier of QKD, the single photons play an important role in the keys extraction and time synchronization. Especially, the accuracy of the time of arrival (TOA) of a single photon can further affect the QBER and the final key rate. Specifically, the single photons sent by Alice are probed by single photon detectors (SPDs) of Bob. Alice and Bob have independent reference clocks and the difference cannot be completely eliminated. Then Bob records the TOAs of all the output signals of the SPDs using the time-to-digital convertor (TDC) and saves the TDC data to a local memory.[9,10] Therefore, the TOA accuracy reflects the system timing precision, which is affected by the time synchronization imperfection[11,12] and the system jitters caused by the single photons source,[13] detection device,[14,15] TDC,[10,16,17] etc. Moreover, these factors bring an inevitable result that the temporal distribution of the single-photon pulse is expanded. The width of the corresponding detection time window has to be set wider. For example, in Ref. [1], the cumulative effects of the timing jitter of the Alice electronics, reference clock noise, timing jitter of the photodetector, and noise in the timestamp unit led to a temporal distribution of signal events with a full width half maximum (FWHM) of 4 ns. Another work in Ref. [2], the cumulative effects of the timing jitter of the Alice electronics, GPS noise, timing jitter of the detector, timing jitter of TDC and other temporal noise led to a total temporal precision of signal events with a FWHM of 1.1 ns. At last, a lower SNR leads to an unsatisfactory QKD performance. Therefore, how to promote the TOA accuracy to improve the system timing precision, thereby optimizing the QKD performance is worth studying. This exactly is the original point of this paper.

To improve the TOA accuracy of a single photon, the conventional method is to design a kind of TDC with a higher precision, smaller dead time and lower jitter,[10,16] such as the TDC based on the field-programmable-gate-array (FPGA).[17–19] The FPGA-TDC with the resolution of 50 ps and the dead time of 30 ns, has been successfully used in the moving platform QKD experiment over 40 km, the floating platform QKD experiment over 20 km and the high-loss free space QKD experiment over 96 km.[2,10] However, the hard-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61573059, 61401340, and 61172138), the Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2016JM6035), and the Fundamental Research Funds for the Central Universities, China (Grant No. JB161303).

†Corresponding author. E-mail: xidian_lpx@163.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

ware complexity of designing the high-precision TDC makes this work difficult to be implemented easily. Moreover, the TOAs of the single photons obtained from this way would be inevitably limited by the hardware conditions. Therefore, the TOA accuracy could not be greatly improved through this conventional method.

In recent years, quantum entanglement has been maturely applied in quantum information processing, especially for the design of some quantum protocols, such as the quantum secret sharing protocol,[20,21] the quantum private comparison of equality (QPCE) protocol,[22,23] the quantum key management protocol,[24] and quantum signature protocol.[25] Therefore, how to use the entanglement nature to improve the TOA accuracy is an interesting problem. To avoid designing a high-precision TDC, in this paper, we use M entangled photons to achieve an improvement in the TOA accuracy and the performance optimization for the QKD system.

At first, a simple but efficient method is using M unentangled photons to replace a single photon, whose TOA accuracy is certainly better than that of a single photon. The entanglement can bring a better TOA accuracy in principle,[26,27] so employing M frequency-entangled photons has become an effective approach to improve the QKD performance. Nevertheless, the main drawback that entanglement is sensitive to the photon loss[28–30] is also inherited into this improved QKD scheme. If one or more of the photons fails to arrive at the detector because of the atmosphere attenuation and background noises, the M fully entangled photons will become useless for the QKD process. Addressing this problem, we further propose two schemes using partially entangled photons and grouping-entangled photons respectively.[31–33] These two entanglement schemes can enhance the TOA accuracy while resisting the photon loss. The TOA accuracy obtained from the partially entangled photons or the grouping-entangled photons is worse than that which stems from the fully entangled photons, the robustness of QKD would still be greatly improved. In this paper, we concretely introduce the partially entangled photons scheme and the grouping-entangled photons scheme. In the case of an ideal channel and of a lossy channel, the effects of these schemes on the QBER and the final key rate are further analyzed. Finally, the selection for the optimal scheme in the lossy channel, which depends on the comparisons of the QBER performance among these three schemes, is also presented.

2. The partially entangled photons scheme

Regarding a QKD system, it is important to record the arrival time of a single photon that is used for syncing Alice and Bob as well as performing keys extraction. Different from the conventional hardware approaches, we make use of the average TOA of M fully entangled photons to replace the TOA of a single photon. However, while improving the TOA accuracy of a single photon, this method also inherits the drawback of entanglement. In practice, once an entangled photon is lost, the TOA accuracy afforded by the entanglement scheme will become zero, which is fatal for the fully entangled photons scheme. For the sensitivity to loss, one may use the partially entangled photons to increase the resistance to loss, although at the cost of the TOA accuracy. The remaining TOA accuracy obtained from the partially entangled photons, however, is still better than that from the single photons.

2.1. Fully entangled photons scheme

Although the fully entangled photons scheme is easy to be affected by the photon loss, its accuracy is the highest of the four schemes. These schemes include the fully entangled photons scheme, the partially entangled photons scheme, the unentangled photons scheme, and the ordinary single photon scheme. Therefore, it is necessary to analyze the fully entangled photons scheme.

The TOA accuracy of M unentangled photons is

$$\Delta t_{\mathrm{un}} \gtrsim \frac{\Delta\tau}{\sqrt{M}}, \tag{1}$$

where $\Delta\tau^2$ is the variance of $\left|g(t_{i,k})\right|^2$, $\left|g(t_{i,k})\right|^2$ is the probability that the kth photon is received on the ith channel at time $t_{i,k}$. Similarly, the TOA accuracy of a single photon is

$$\Delta t \gtrsim \Delta\tau. \tag{2}$$

On the other hand, the TOA uncertainty of M frequency-entangled photons comes from[31]

$$\Delta t_{\mathrm{en}} = \frac{\Delta\tau}{M}. \tag{3}$$

Therefore, the gain in the time-of-arrival accuracy can be denoted as $\alpha = \Delta t_{\mathrm{en}}/\Delta t = 1/M$. This gain can also be applied into the time domain spread of a single-photon pulse $\Delta T_{\mathrm{en}} = \Delta T/M$, ΔT and ΔT_{en} are caused by a single photon and M frequency-entangled photons, respectively. Besides, ΔT can be interpreted as the minimum size of the coincidence window that directly affects the system temporal precision δ_{sys} of QKD. Thus, the gain $1/M$ is also appropriate for δ_{sys}, i.e.,

$$\delta_{\mathrm{sys_en}} = \frac{1}{M}\delta_{\mathrm{sys}}, \tag{4}$$

where $\delta_{\mathrm{sys_en}}$ and δ_{sys} are caused by M frequency-entangled photons and a single photon, respectively, δ_{sys} influences the QBER and the key rate directly, which is analyzed in the next section concretely.

2.2. Improvement of multiphoton scheme

To protect against the photon loss, we use partially entangled photons to increase the robustness of QKD. By contrast with the fully frequency-entangled photons, the first Q of

the M photons are maximally entangled and the other $M-Q$ photons are unentangled. The parameter Q characterizes the degree of entanglement of this partially entangled state. The TOA accuracy of this partial entanglement scheme is as follows:

$$\Delta t_Q = \frac{\Delta\tau}{\sqrt{M}}\sqrt{\frac{M-Q+1}{M}}, \tag{5}$$

where $\Delta\tau$ is the same as that in Eq. (1). From Eq. (5), we can see that this scheme corresponds to the fully entangled photons scheme when $M=Q$. As long as $Q>1$, the accuracy achievable is greater than that of the fully unentangled case, but not as high as that of the fully entangled case. The gain in accuracy is $\beta=\Delta t_Q/\Delta t=\sqrt{M-Q+1}/M$, and the gain in $\delta_{\rm sys}$ is

$$\delta_{{\rm sys}_Q} = \frac{\sqrt{M-Q+1}}{M}\delta_{\rm sys}. \tag{6}$$

However, there is a problem that needs our attention. The above discussion for the accuracy is based on the unit quantum efficiency $\eta=1$. Here, the channel quantum efficiency η expresses a possibility that one photon can be detected by Bob's receiver. The probability that all M photons reach Bob is given by η^M. Since the atmosphere attenuation and background noise, not all the M photons can be detected, namely $\eta\neq 1$. Thus, it is necessary to analyze the respective accuracy gain of these four schemes under $\eta\neq 1$.

For the fully entangled photons scheme, the uncertainty of the average TOA of M photons is given by

$$\Delta t_{\eta_{\rm en}}(r) = \frac{\Delta\tau}{M\sqrt{r\eta^M}}. \tag{7}$$

The result of Eq. (7) comes from the r experimental runs. For the M unentangled photons, i.e.,

$$\Delta t_{\eta_{\rm un}}(r) = \left[\sum_{m=1}^{M}\binom{M}{m}\frac{\eta^m(1-\eta)^{M-m}}{m[1-(1-\eta)^M]^2}\right]^{1/2}\frac{\Delta\tau}{\sqrt{r}}. \tag{8}$$

Therefore, the accuracy in the single-photon scheme is represented as

$$\Delta t_\eta(r) = \frac{\Delta\tau}{\sqrt{\eta r}}. \tag{9}$$

Besides, different from the principle of the partial entanglement scheme, quantum fault computation can be applied into calculating the TOA accuracy.[31] As shown in Fig. 1, each of the G groups is composed of $K=M/G$ frequency maximally entangled photons and G groups are entangled together.

The TOA accuracy in this grouping entanglement scheme is given by

$$\Delta t_{\eta_G}(r) = \frac{1}{2K\Delta\omega\sqrt{r[1-(1-\eta^K)^G]}} \times\left[\sum_{g=1}^{G}\frac{(G-g)\Delta\Omega^2+\Delta\omega^2}{g(G\Delta\Omega^2+\Delta\omega^2)}\binom{G}{g} \times\frac{(\eta^K)^g(1-\eta^K)^{G-g}}{1-(1-\eta^K)^G}\right]^{1/2}, \tag{10}$$

where $\Delta\Omega^2$ is the variance of $|\Phi(\Omega)|^2$, $\Phi(\Omega)$ is the pulse's spectrum function under the grouping-entangled state $|\Psi\rangle_G$. The $\Delta\omega^2$ is the variance of $|\phi(\omega,\Omega)|^2$, and $\phi(\omega,\Omega)$ is the pulse's spectrum function under $|\Omega\rangle_j$, $|\Omega\rangle_j$ is the state of the jth group of K photons for $j=1,\ldots,G$.

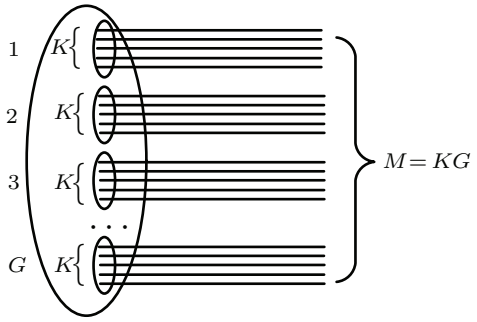


Fig. 1. The principle of grouping entanglement scheme.

According to the above discussion, the accuracy gains of these three schemes for $\delta_{\rm sys}$ are as follows:

$$\delta_{{\rm sys}_\eta_{\rm en}} = \frac{\Delta t_{\eta_{\rm en}}(r)}{\Delta t_\eta(r)}\delta_{\rm sys} = \Upsilon(M,\eta)\delta_{\rm sys}, \tag{11}$$

$$\delta_{{\rm sys}_\eta_{\rm un}} = \frac{\Delta t_{\eta_{\rm un}}(r)}{\Delta t_\eta(r)}\delta_{\rm sys} = \Lambda(M,\eta)\delta_{\rm sys}, \tag{12}$$

$$\delta_{{\rm sys}_\eta_G} = \frac{\Delta t_{\eta_G}(r)}{\Delta t_\eta(r)}\delta_{\rm sys} = \Theta(G,\eta)\delta_{\rm sys}. \tag{13}$$

3. Improvement of QKD performance

By virtue of the improvement on the time-of-arrival accuracy, the system timing precision of QKD can be increased effectively. Moreover, the increase of $\delta_{\rm sys}$ can further decrease the QBER and increase the final key rate. In this section, the improvements of QKD performance caused by different schemes are addressed here for completeness, especially in the case of an ideal channel and of a lossy channel.

Denoting μ, μ', 0 as the average photon number (intensity), and S_μ, $S_{\mu'}$, S_0 as the counting rates of decoy state pulses, signal state pulses and vacuum state pulses, respectively. According to Ref. [34], the error rate of signal state pulses is given by

$$E_{\mu'} = e + \frac{e^{-\mu'}s_0(\mu')}{2S_{\mu'}}, \tag{14}$$

where $E_{\mu'}$ is the error rate of signal state pulses, e is the practical error rate of nonvacuum pulses, and $e^{-\mu'}s_0(\mu')$ is the counting rate of vacuum state pulses.

In addition, we denote N_s as the counting rate of the authentic quantum signal, N_d represents the counting rate of dark counts and stray noises within the detection time window, namely,

$$N_d = N_n \frac{\Delta T}{1/f} = kN_n \delta_{sys} f,$$

where N_n is the counting rate of noises in each pulse period, f is the sending frequency of signal state pulses at Alice's side. The QBER has the following form:

$$E_{\mu'} = e + \frac{kN_n f \delta_{sys}}{2(N_s + kN_n f \delta_{sys})}. \quad (15)$$

The final key rate[35,36]

$$R_{\mu'} = S_{\mu'} \left\{ \Delta_1^{\mu'} \left[1 - H(E_1^{\mu'}) \right] - H(E_{\mu'}) \right\},$$

can be defined as

$$R_{\mu'} = S_{\mu'} \left\{ \Delta_1^{\mu'} \left[1 - H(E_1^{\mu'}) \right] - H\left(e + \frac{kN_n f \sigma_{sys}}{2(N_s + kN_n f \delta_{sys})} \right) \right\}. \quad (16)$$

Here, $H(x)$ is the binary entropy function, i.e., $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, $\Delta_1^{\mu'}$ is the fraction of single photon, i.e., $\Delta_1^{\mu'} = \mu' e^{-\mu'} s_1 / S_{\mu'}$, $E_1^{\mu'}$ is the QBER upper bound of single photons from signal states pulses as[2]

$$E_1^{\mu'} = \left(E_{\mu'} - \frac{e^{-\mu'}(1-r_0)S_0}{2S_{\mu'}} \right) \Big/ \Delta_1^{\mu'}.$$

3.1. QKD performance in ideal channel

The improvement of QKD performance on the ideal channel ($\eta = 1$) is the theoretical basis of that on the lossy channel ($\eta \neq 1$). Inserting Eq. (6) into Eq. (15), we obtain

$$E_{\mu'} = e + \frac{kN_n f \delta_{sys} \sqrt{M - Q + 1}}{2(MN_s + kN_n f \delta_{sys} \sqrt{M - Q + 1})}. \quad (17)$$

To demonstrate that the partially entangled photons are more tolerant to the loss of photons, equation (17) is plotted in Fig. 2. The QBER's rising tendency in each subgraph of Fig. 2 is similar. As shown in Fig. 2(b), the QBER increases with the increase of noise counts N_n, but the rate of increase of the QBER caused by the partially entangled photons ($Q < M$) is always less than that caused by a single photon and higher than that caused by M fully entangled photons ($Q = M$). Moreover, the rate of increase of the QBER declines with the increase of the degree of entanglement Q. On the other hand, the effect of entangled photons on QBER is more conspicuous with the increase of the number of photons M. For example, the QBER gap between a single photon and the fully entangled photons in Fig. 2(a) is less than that in Fig. 2(d).

The analysis of the key rate is analogous to that of the QBER. Inserting Eq. (6) into Eq. (16), we obtain

$$R_{\mu'} = S_{\mu'} \left\{ \Delta_1^{\mu'} \left[1 - H(E_1^{\mu'}) \right] - H\left(e + \frac{kN_n f \delta_{sys} \sqrt{M - Q + 1}}{2(MN_s + kN_n f \delta_{sys} \sqrt{M - Q + 1})} \right) \right\}. \quad (18)$$

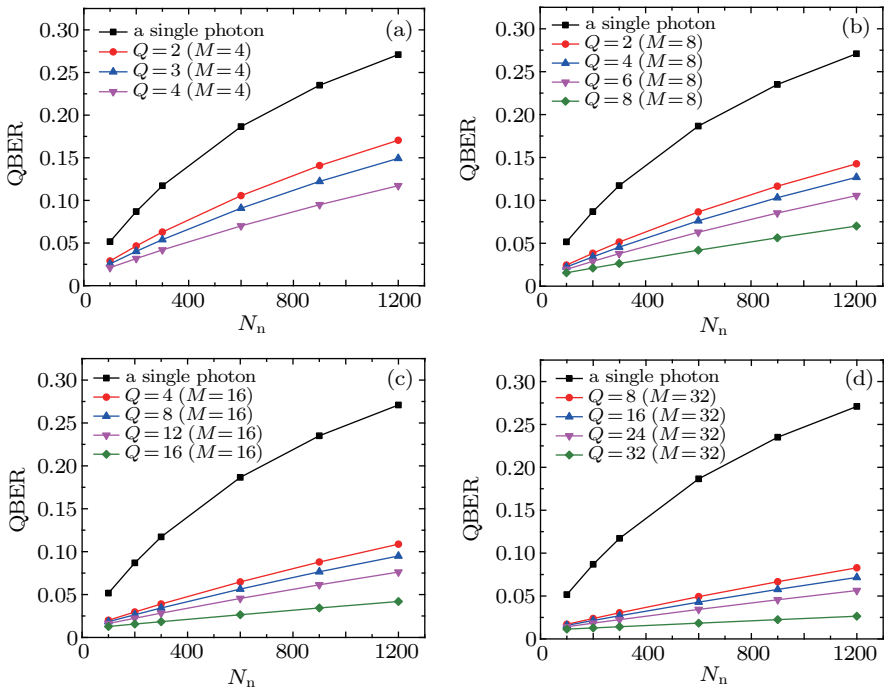


Fig. 2. (color online) The effects of partially entangled photons on the QBER with the number of photons (a) $M = 4$, (b) $M = 8$, (c) $M = 16$, (d) $M = 32$, together with a single photon scheme (black solid line).

The improvement of the key rate obtained from the partially entangled photons is shown in Fig. 3. Each subgraph of Fig. 3 has a similar downward trend: the key rate decreases with the increase of noise counts N_n, but the rate of decrease caused by the partially entangled photons ($Q < M$) is always less than that caused by a single photon and higher than that caused by M fully entangled photons ($Q = M$). That is to say, the increase of the degree of entanglement Q can further boost the final key rate. Besides, the enhancement in the number of photons also increases the key rate, for example, the key rate gap between a single photon and the fully entangled photons in Fig. 3(a) is less than that in Fig. 3(d).

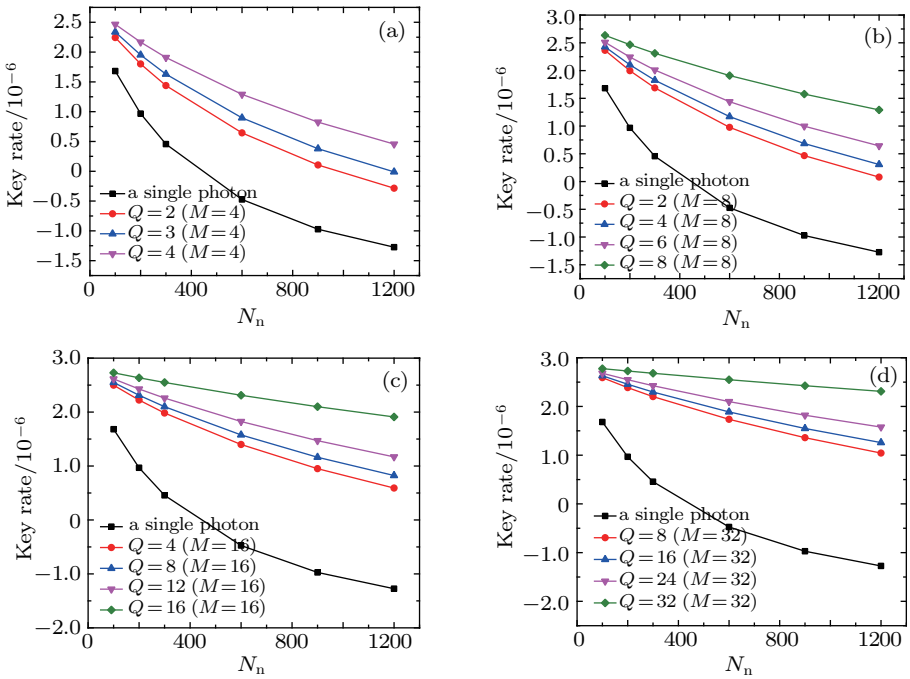


Fig. 3. (color online) The effects of partially entangled photons on the key rate with the number of photons (a) $M = 4$, (b) $M = 8$, (c) $M = 16$, (d) $M = 32$, together with a single photon scheme (black solid line).

3.2. QKD performance in lossy channel

Due to the presence of the atmosphere attenuation and background noises, losing one or more entangled photons is easy to happen.[28,37] This phenomenon can make the fully entangled photons scheme completely useless for the improvement of QKD performance. Since the loss of a single photon from a maximally entangled state would destroy the entanglement property, the gain in time-of-arrival accuracy afforded by the fully entangled photons scheme would become zero. Therefore, in the case of a lossy channel, the partial entanglement scheme, particularly the grouping entanglement scheme has become an effective alternative. According to Fig. 1, the improvement of QKD performance in terms of M grouping-entangled photons is presented in this section.

In G groups, if the lost photon comes from the jth group, only the jth group's photon arrival time needs to be discarded, the other TOA data may be retained and employed. On the contrary, all the TOA data need to be abandoned, if M photons are fully entangled. We use Eq. (13) to calculate the QBER and the final key rate in the presence of photon loss as

$$E_{\mu'} = e + \frac{kN_n f\Theta(G,\eta)\delta_{sys}}{2(N_s + kN_n f\Theta(G,\eta)\delta_{sys})}, \tag{19}$$

$$R_{\mu'} = S_{\mu'}\left\{\Delta_1^{\mu'}\left[1 - H(E_1^{\mu'})\right] - H\left(e + \frac{kN_n f\Theta(G,\eta)\sigma_{sys}}{2(N_s + kN_n f\Theta(G,\eta)\delta_{sys})}\right)\right\}. \tag{20}$$

To describe the effects of the grouping entanglement scheme on the QKD performance, the relationship among G, η, and $E_{\mu'}$ (key rate) is given in Fig. 4 (Fig. 5). The related parameters are $K = 4$, $\Delta\omega^2/\Delta\Omega^2 = 2$, and $\Delta\tau = 1/(2\sqrt{\Delta\omega^2 + \Delta\Omega^2})$.[31] It can been seen from Fig. 4 that the QBER decreases with the increase of channel quantum efficiency η when the number of groups G keeps stable. Because the increase in channel quantum efficiency means that the quantum loss declines, more and more entangled photons can be detected by Bob's receiver. Besides, the increase of the number of groups also contributes to the decline of QBER. With the increase of G, less and less TOA data would be affected by the photon loss, namely, less and less TOA data need to be discarded. Analogously, figure 5 depicts the improvement of the key rate obtained from Eq. (20). The key rate increases with the increase of quantum efficiency η under a certain G parameter. Moreover, the increase of G also accelerates the improvement of the key rate.

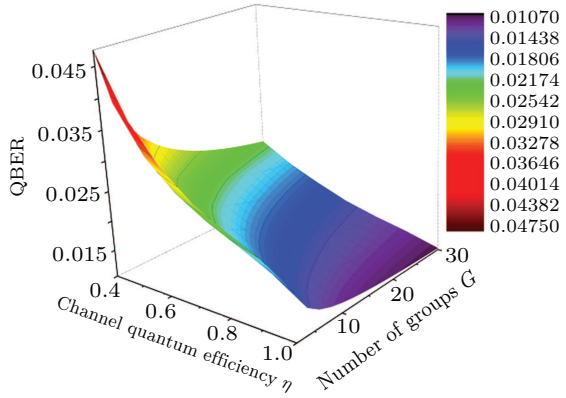


Fig. 4. QBER versus the number of groups G and the channel quantum efficiency η.

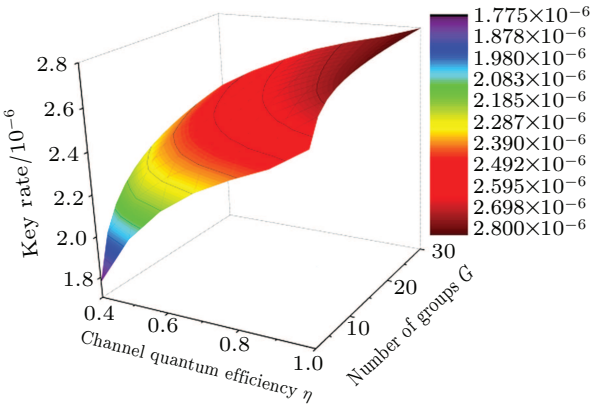


Fig. 5. The key rate versus the number of groups G and the channel quantum efficiency η.

4. Discussion

According to the above theoretical analysis and simulations, in reality, the partially entangled photons scheme, especially the grouping-entangled photons scheme can battle the effects of photon loss, enhance the robustness of QKD, and improve the QBER and key rate. It seems like an effective method to replace the conventional single-photon scheme, but it is not always the optimal choice under the practical circumstances. This optimal scheme stems from three different schemes: the grouping-entangled photons scheme, the fully entangled M-photon scheme, and the unentangled M-photon scheme. Moreover, it can bring the highest TOA accuracy and the greatest QKD performance compared to other unselected schemes. In this section, the selection strategy for the optimal scheme is presented.

In fact, the selection for the optimal scheme depends on the relationship between the channel quantum efficiency η and the number of photons M. For example, $\Delta t_{\eta_\mathrm{en}}(r)/\Delta t_{\eta_\mathrm{un}}(r) > 1$ shows that the M unentangled photons can bring a smaller time-of-arrival uncertainty than the M fully entangled photons, and $\Delta t_{\eta_\mathrm{un}}(r)/\Delta t_{\eta_G}(r) > 1$ shows that the grouping-entangled photons scheme can bring a better TOA accuracy. At this time, $\Delta t_{\eta_\mathrm{en}}(r) > \Delta t_{\eta_\mathrm{un}}(r) > \Delta t_{\eta_G}(r)$ indicates that the grouping-entangled photons scheme can obtain the highest TOA accuracy, so it is the optimal scheme. The other cases, which include $\Delta t_{\eta_\mathrm{un}}(r) > \Delta t_{\eta_G}(r) > \Delta t_{\eta_\mathrm{en}}(r)$, $\Delta t_{\eta_\mathrm{un}}(r) > \Delta t_{\eta_\mathrm{en}}(r) > \Delta t_{\eta_G}(r)$, and $\Delta t_{\eta_\mathrm{en}}(r) > \Delta t_{\eta_G}(r) > \Delta t_{\eta_\mathrm{un}}(r)$, are similar to this derivation process. With respect to this problem, Fig. 6 in Ref. [31] describes the results for selecting the optimal scheme in detail.

The gain in TOA accuracy can directly influence the system temporal precision of QKD, so we need to determine an optimal scheme that can bring the best QKD performance compared to other schemes. To show the effects of the relationship between η and M on the QKD performance, we insert Eqs. (11)–(13) into Eq. (15) successively, and calculate the respective QBER result. These three results are plotted together in Fig. 6.

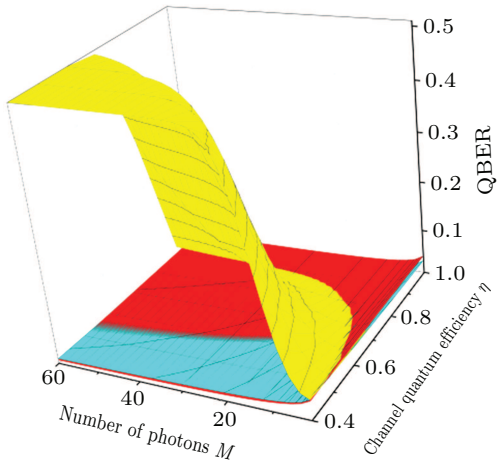


Fig. 6. Comparison of the QBER results that come from three different schemes. The yellow region is where the QBER may be obtained using M fully entangled photons. The QBER in the blue region is derived from M grouping-entangled photons. The red region is where the QBER is obtained through M unentangled photons.

In Fig. 6, the QBER obtained from M fully entangled photons is significantly higher than that from the other two methods when $\eta < 0.8$ and $M > 10$. The increase of M or the decrease of η means that more entangled photons are susceptible to the channel loss. According to the above descriptions, the fully entangled photons scheme is the most sensitive to the photon loss compared to the other schemes, so its QBER performance is the worst. On the contrary, the grouping-entangled photons can completely embody its ability of resisting the photon loss and retaining a part of TOA accuracy, so its QBER performance is better at this time. However, when $\eta < 0.6$, even if the grouping-entangled photons scheme also cannot fully achieve the entanglement function, the lowest QBER comes from the unentangled photons scheme. These discussions are specifically described in Fig. 7. In addition, as an alternative scheme of the fully entangled photons scheme, no matter which scheme is selected from the unentangled photons scheme and the grouping-entangled photons scheme, the QKD performance can be effectively improved compared to the conventional single-photon scheme.

This is because $\Delta t_{\eta_\mathrm{un}}(r)/\Delta t_{\eta}(r) < 1$ and $\Delta t_{\eta_G}(r)/\Delta t_{\eta}(r) < 1$ can guarantee the effectiveness of these two methods.

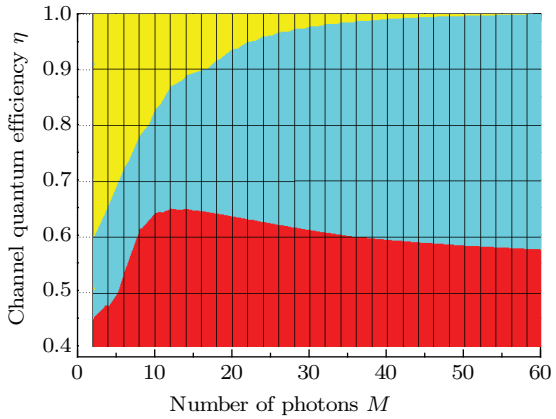


Fig. 7. The projection of Fig. 6 on the M–η plane when looking up along the negative half axis of the QBER axis. The red region indicates that M unentangled photons can bring the lowest QBER compared to the other two methods. The blue region represents that the lowest QBER comes from the grouping-entangled photons. The yellow region is where the lowest QBER is obtained through M fully entangled photons.

5. Conclusion

In this paper, we have used M fully entangled photons to achieve an enhancement in the time-of-arrival accuracy, which can decrease the width of the detection time window, increase the system temporal precision of QKD, and thereby improve the QBER and the final key rate. Most importantly, considering the adverse effects of photon loss on the entanglement in reality, we have employed M grouping-entangled photons to increase the robustness of QKD. In the case of a lossy channel, the selection for the optimal scheme has also been investigated, which comes from three alternative schemes presented in this paper. However, no matter which scheme is selected from the grouping-entangled photons scheme and the unentangled photons scheme, its QKD performance is always better than the results obtained from the conventional single-photon scheme.

References

[1] Schmitt-Manderbach T, Weier H, Fuerst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A and Weinfurter H 2007 *Phys. Rev. Lett.* **98** 010504

[2] Wang J Y, Yang B, Liao S K, et al. 2013 *Nat. Photon.* **7** 387

[3] Bourgoin J P, Higgins B L, Gigov N, Holloway C, Pugh C J, Kaiser S, Cranmer M and Jennewein T 2015 *Opt. Express* **23** 33437

[4] Gisin N and Thew R 2007 *Nat. Photon.* **1** 165

[5] Li C Y, Li X H, Deng F G and Zhou H Y 2008 *Chin. Phys. B* **17** 2352

[6] Zhao J J, Guo X M, Wang X Y, Wang N, Li Y M and Peng K C 2013 *Chin. Phys. Lett.* **30** 060302

[7] Miao E L, Han Z F, Gong S S, Zhang T, Diao D S and Guo G C 2005 *New J. Phys.* **7** 215

[8] Tomaello A, Bonato C, Deppo V D, Naletto G and Villoresi P 2011 *Adv. Space Res.* **47** 802

[9] Yearsley J M 2010 *Phys. Rev. A* **82** 012116

[10] Shen Q, Liao S K, Liu S B, Wang J H, Liu W Y, Peng C Z and An Q 2013 *IEEE Trans. Nucl. Sci.* **60** 3570

[11] Wang J C, Tian Z H, Jing J L and Fan H 2016 *Phys. Rev. D* **93** 065008

[12] Wu Q L, Han Z F, Miao E L, Liu Y, Dai Y M and Guo G C 2007 *Opt. Commun.* **275** 486

[13] Brida G, Degiovanni I P, Genovese M, Piacentini F, Traina P, Della-Frera A, Tosi A, Shehata A B, Scarcella C, Gulinatti A, Ghioni M, Polyakov S V, Migdall A and Giudice A 2012 *Appl. Phys. Lett.* **101** 221112

[14] Natarajan C M, Tanner M G and Hadfield R H 2012 *Supercond. Sci. Tech.* **25** 063001

[15] Ma H Q, Yang J H, Wei K J, Li R X and Zhu W 2014 *Chin. Phys. B* **23** 120308

[16] Wu J Y 2010 *IEEE Trans. Nucl. Sci.* **57** 1543

[17] Bayer E and Traxler M 2011 *IEEE Trans. Nucl. Sci.* **58** 1547

[18] Song J, An Q and Liu S B 2006 *IEEE Trans. Nucl. Sci.* **53** 236

[19] Wang J H, Liu S B, Shen Q, Li H and An Q 2010 *IEEE Trans. Nucl. Sci.* **57** 446

[20] Chen X B, Yang S, Su Y and Yang Y X 2012 *Phys. Scr.* **86** 055002

[21] Chen X B, Xu G, Su Y and Yang Y X 2014 *Quantum Inf. Comput.* **14** 589

[22] Chen X B, Su Y, Niu X X and Yang Y X 2014 *Quantum Inf. Process.* **13** 101

[23] Chen X B, Dou Z, Xu G, Wang C and Yang Y X 2014 *Quantum Inf. Process.* **13** 85

[24] Xu G, Chen X B, Dou Z, Yang Y X and Li Z P 2015 *Quantum Inf. Process.* **14** 2959

[25] Wang M M, Chen X B and Yang Y X 2013 *Sci. China-Phys. Mech. Astron.* **56** 1636

[26] Giovannetti V, Lloyd S and Maccone L 2001 *Nature* **412** 417

[27] Giovannetti V, Lloyd S and Maccone L 2004 *Science* **306** 1330

[28] Semenov A A and Vogel W 2010 *Phys. Rev. A* **81** 023835

[29] Usenko V C, Heim B, Peuntinger C, Wittmann C, Marquardt C, Leuchs G and Filip R 2012 *New J. Phys.* **14** 093048

[30] Bohmann M, Semenov A A, Sperling J and Vogel W 2016 *Phys. Rev. A* **94** 010302

[31] Giovannetti V, Lloyd S and Maccone L 2002 *Phys. Rev. A* **65** 022309

[32] Thew R T, Tanzilli S, Tittel W, Zbinden H and Gisin N 2002 *Phys. Rev. A* **66** 062304

[33] Chen N, Quan D X, Pei C X and Yang H 2015 *Chin. Phys. B* **24** 020304

[34] Wang X B 2005 *Phys. Rev. A* **72** 012322

[35] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326

[36] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[37] Chen X Y 2015 *Chin. Phys. Lett.* **32** 010301