

Improving source-in-the-middle continuous-variable quantum key distribution using a heralded hybrid linear amplifier

Lei-Xin Wu(伍磊鑫), Yan-Yan Feng(冯艳艳), and Jian Zhou(周健)
Citation: Chin. Phys. B, 2023, 32 (**7**): 070310. DOI: 10.1088/1674-1056/ac9b39
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

A new method of constructing adversarial examples for quantum variational circuits

Jinge Yan(颜金歌), Lili Yan(闫丽丽), and Shibin Zhang(张仕斌)
Chin. Phys. B, 2023, 32 (**7**): 070304. DOI: 10.1088/1674-1056/ac9b32

Faithful and efficient hyperentanglement purification for spatial-polarization-time-bin photon system

Fang-Fang Du(杜芳芳), Gang Fan(樊钢), Yi-Ming Wu(吴一鸣), and Bao-Cang Ren(任宝藏)
Chin. Phys. B, 2023, 32 (**6**): 060304. DOI: 10.1088/1674-1056/aca395

Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states

Yu-Qian He(贺宇千), Yun Mao(毛云), Hai Zhong(钟海), Duang Huang(黄端), Ying Guo(郭迎)
Chin. Phys. B, 2020, 29 (**5**): 050309. DOI: 10.1088/1674-1056/ab8216

Finite-size analysis of continuous-variable quantum key distribution with entanglement in the middle

Ying Guo(郭迎), Yu Su(苏玉), Jian Zhou(周健), Ling Zhang(张玲), Duan Huang(黄端)
Chin. Phys. B, 2019, 28 (**1**): 010305. DOI: 10.1088/1674-1056/28/1/010305

Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine

Hang Zhang(张航), Yu Mao(毛宇), Duan Huang(黄端), Ying Guo(郭迎), Xiaodong Wu(吴晓东), Ling Zhang(张玲)
Chin. Phys. B, 2018, 27 (**9**): 090307. DOI: 10.1088/1674-1056/27/9/090307

Improving source-in-the-middle continuous-variable quantum key distribution using a heralded hybrid linear amplifier

Lei-Xin Wu(伍磊鑫), Yan-Yan Feng(冯艳艳), and Jian Zhou(周健)†

College of Computer and Information Engineering, Central South University of Forestry and Technology, Changsha 410004, *China*

(Received 7 August 2022; revised manuscript received 4 October 2022; accepted manuscript online 19 October 2022)

A hybrid linear amplifier is inserted at the output of the source-in-the-middle distribution protocol to overcome the shortcomings of the transmission distance. The modified protocol aims to maintain a high key rate for long-distance transmission under high noise. It has the potential to significantly broaden the application range of the continuous variable quantum key distribution protocol. The effects of amplifier parameters and noise on the modified protocol are analyzed in detail with regard to applying it to a practical system. To make the simulation more realistic, the effect of finite size on the new protocol is taken into account. It will serve as a guideline for the future use of hybrid linear amplifiers. Different parameters can be adjusted to achieve the best performance for key rates of different quantum channels.

Keywords: hybrid linear amplifier, source-in-the-middle distribution, finite-size analysis

PACS: 03.67.–a, 03.67.Hk **DOI:** 10.1088/1674-1056/ac9b39

1. Introduction

Quantum key distribution (QKD)[1–5] enables the establishment of a secure key between two users (Alice and Bob)[6–9] in the presence of an eavesdropper,[10–14] which allows the two communicating parties to exchange and produce a random secure key to encrypt and decode messages.[15–19] Theoretically, the no-cloning theorem and uncertainty principle ensure the absolute security of quantum communication.[20,21] However, due to the interference of noise in the detector and channel, the eavesdroppers could acquire the information by attacking the quantum channel. For Alice and Bob, the signal leakage can be reduced by lowering the channel loss.[22] QKD is divided into discrete variable quantum key distribution (DVQKD) and continuous variable quantum key distribution (CVQKD). DVQKD uses single photons for quantum transport and has a long transmission distance. However, its ability to resist interference is poor. CVQKD offers the benefit of using commercially available telecom components and is more compatible with wave-length-division multiplexing (WDM).[23] However, it is not widely used, as the CVQKD protocol is fragile and cannot maintain high reconciliation efficiency in long distance transfer. As a result, increasing the transmission distance of CVQKD is imminent.[24–26]

Many new CVQKD distribution protocols have been proposed to overcome the disadvantages of transmission distance, such as the protocol involving placing the source between two users.[27–29] Unlike the traditional protocol (the Gaussian entanglement created by Alice, who is a trusted party to Bob), this protocol places the Gaussian entangled source in the middle of Alice and Bob, and uses an untrusted third party (likely Eve) to generate a secure string of keys. Direct reconciliation and reverse reconciliation are interchangeable in the new protocol. The results show that the coherent-state protocol outperforms the squeezed-state protocol in terms of noise resistance (3 dB). Also, the source-in-the-middle protocol, using the coherent state, has higher transmission efficiency and noise immunity than the traditional CVQKD protocol.[28] As a result, there is plenty of room for advancement via alternative means. Discrete modulation was adopted in Ref. [29] to enhance the protocol performance for source-in-the-middle distribution; the results are attractive, but the effective transmission distribution is always very limited under high noise.[29]

Moreover, adding the heralded hybrid linear amplifier (HLA), which is made of a tunable parameter heralded noiseless linear amplifier (NLA) and an optimal deterministic linear amplifier (DLA), to the end provides another way to extend the CVQKD transmission distance.[30–32] The HLA abandons determinism and employs the probabilistic approach to achieve high-fidelity cloning that surpasses the Gaussian unclonable limit.[30] On the one hand, the NLA can amplify the coherent state amplitude without introducing additional noise.[31] On the other hand, the DLA transforms the coherent state in a deterministic manner. Moreover, by tuning the parameters, the coherent state can be amplified with low noise and a high chance of success.[30–32] Besides, finite-size analysis can help to improve the security of quantum communication.[33–35] Although the finite-size analysis has a negative effect on the key rate, the simulation will be closer to the reality. Before the protocol begins, Alice and Bob have agreed on some of the parameters and reconciliation. The parameters are estimated to improve the security of the quantum channel.[33]

In this paper, we introduce the HLA at the output of the

†Corresponding author. E-mail: 13142153489@163.com

© 2023 Chinese Physical Society and IOP Publishing Ltd

channel to enhance the source-in-the-middle distribution protocol. Additionally, finite-size analysis is used to enhance the security of the protocol and bring the simulation closer to reality. The HLA addresses the transmission distance issues with the source-in-the-middle distribution. It is possible to transmit over long distances while keeping the key rate high. In the simulation section, we apply the protocol to a specific system, in which the impact of noise and each HLA parameter on this system will be investigated.

This paper is organized as follows: we describe the modified protocol in Section 2, the key rate of the modified protocol will be calculated in Section 3, the simulation is displayed in Section 4, and the concluding remarks are given in Section 5.

2. Entanglement-in-the-middle distribution with the HLA amplifier

The modified protocol is displayed in Fig. 1. A Gaussian entanglement source develops in the middle of Alice and Bob. The HLA is compensated at the output of Bob to address the transmission distance shortcomings of original protocols. Under the Gaussian collective attack of Eve, Alice and Bob use an unreliable third party to help them generate a secure key. We conclude from Ref. [28] that there is no impact on the protocol's security.

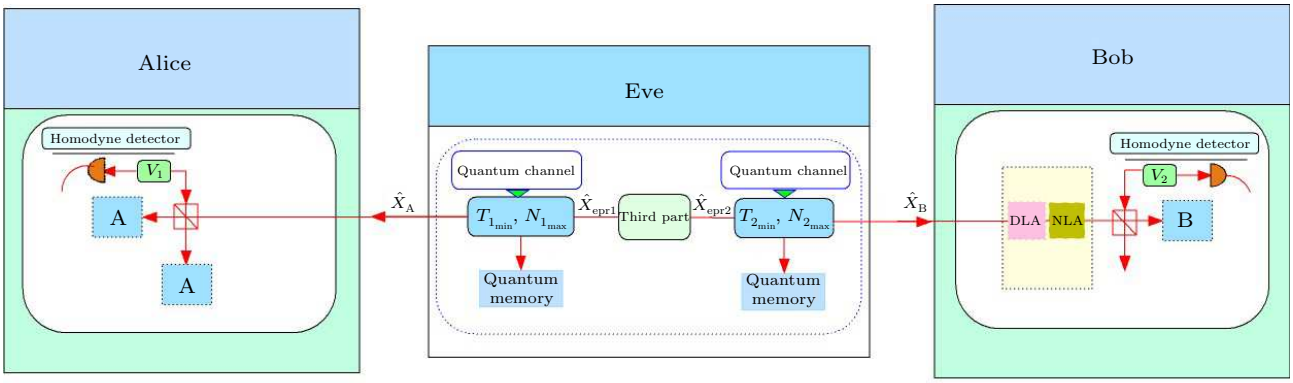


Fig. 1. A scheme of the entanglement-in-the-middle protocol with the HLA is detailed. An entanglement source is generated by a third party and transmitted to Alice and Bob by a quantum channel. The HLA amplifier is inserted at the output of Bob.

The two modes of EPR entangled pairs are created by third parties, where $\hat{X}_{\text{epr1}}$ is sent to Alice and $\hat{X}_{\text{epr2}}$ is sent to Bob, after traveling through the channel,

$$\hat{X}_{\text{epr1}} = \frac{X+P}{\sqrt{2}}, \tag{1}$$

$$\hat{X}_{\text{epr2}} = \frac{X-P}{\sqrt{2}}. \tag{2}$$

The protocol is strongly symmetric when the entanglement source is positioned in the middle of Alice and Bob[15]

$$V = V_1 = V_2, \quad T = T_1 = T_2, \quad N = N_1 = N_2. \tag{3}$$

Notably, the protocol switches to a conventional CVQKD protocol at $T = 1$, which allows Alice to generate entangled states and send them securely to Bob. Eve launches a collective Gaussian attack on the channel in the interim.

The HLA is demonstrated to scale the coherent state securely. It makes sense to use the HLA to enhance the source-in-the-middle protocol. The HLA is composed of a tunable NLA and a DLA, where the NLA is competent to the coherent state to g with probability $1/g^2$, and DLA is capable of expanding the coherent state by a factor of G. While a higher G increases the likelihood of success, it also brings more noise. This straightforward and efficient method accomplishes coherent state amplification close to the quantum noise limit. The original protocol will be improved with the HLA.

The HLA introduces additional noise

$$((\Delta N)^2)_{\text{out}} = 2G^2 - 1. \tag{4}$$

When the EPR entangled pair passes through the HLA, the signal is expanded to

$$\hat{b}_{\text{out}} = \sqrt{G}\hat{b}_{\text{in}} + \sqrt{G-1}\hat{b}_{\text{int}}. \tag{5}$$

The amplitude and phase are both increased to

$$\hat{x}_{\text{out}} = \sqrt{G}\hat{x}_{\text{in}} + \sqrt{G-1}\hat{x}_{\text{int}}, \quad \hat{y}_{\text{out}} = \sqrt{G}\hat{y}_{\text{in}} - \sqrt{G-1}\hat{y}_{\text{int}}. \tag{6}$$

The HLA can convert the parameter variance factor λ, channel transmittance T, and noise N into a new parameter variance factor ς, channel transmittance η, and noise N^g. They are related as follows:

$$\varsigma = \lambda\sqrt{\frac{(g^2-1)(N-2)T-2}{(g^2-1)NT-2}}, \tag{7}$$

$$\eta = \frac{g^2 T}{(g^2-1)T\left[(1/4)(g^2-1)(N-2)NT - N + 1\right] + 1}, \tag{8}$$

$$N^g = N + \frac{1}{2}(g^2-1)(2-N)NT. \tag{9}$$

The HLA takes a probabilistic approach to expand coherent states beyond the Gaussian unclonable limit, resulting in high-fidelity predictive cloning. The connection between the input

and output is

$$\rho_{\text{out}} = HTr_{\text{v}}\{D_G g_{\text{NLA}}^{\hat{n}} \rho_{\text{in}} \otimes |0\rangle\langle 0|_{\text{v}} g_{\text{NLA}}^{\hat{n}} D_G^{\dagger}\}. \tag{10}$$

The average values of the signals are amplified to

$$\hat{X}_{\text{out}} = Gg\hat{X}_{\text{in}}, \quad \hat{Y}_{\text{out}} = Gg\hat{Y}_{\text{in}}. \tag{11}$$

Since the HLA extends the transmission distance of the quantum and SNR, we intend to use it at Bob's end to address the shortcomings of the source-in-the-middle distribution. In fact, the HLA is very compatible with the original protocol and can improve its shortcomings, such as its inability to transmit over long distances and its low noise resistance. The modified protocol can be customized according to the actual transportation requirements. We will consider the use of direct reconciliation for homodyne detection and coherent states. Of course, it also involves the reverse reconciliation with heterodyne detection and squeezed states in this protocol.

3. Secure key rate of the modified protocol

The security keys that export the modified protocol will be distributed. To make the simulation more realistic, we take into account the finite size of the protocol. When deriving the key rate, we consider the direct reconciliation for homodyne detection and coherent states.

The secure key rate of the modified protocol is

$$K = \frac{1}{g^2} \cdot \frac{n}{N} \left[\beta S(A:B) - S_{\text{Qpe}}(A:E) - \Delta(n)\right], \tag{12}$$

where N signals are exchanged but only n is used to encode the signals, and $m = N - n$ is used for parameter estimation. Here, $S(A:B)$ expresses the information shared between Alice and Bob, and $S_{\text{Qpe}}(A:E)$ represents the information eavesdropped by Eve. The $\Delta(n)$ denotes the part of privacy amplification.

The following formula can be used to conduct the correlation of data between Alice and Bob

$$y = kx + b, \tag{13}$$

where

$$k = \sqrt{T}, \tag{14}$$

and b follows a normal distribution with a centered shape and an unidentified variance. The distribution is

$$M^2 = 1 + TN. \tag{15}$$

In Eqs. (14) and (15), k and M are determined parameters; thus, these parameters can be estimated.

Now the lower limit $k_{\min}$ for k and the upper limit $M_{\max}$ for M are acquired by

$$k_{\min} \approx \hat{k} - z_{\text{QPE}} \sqrt{\frac{\hat{\sigma}^2}{mV_A}}, \tag{16}$$

$$M_{\max}^2 \approx \hat{M}^2 + z_{\text{QPE}} \frac{\hat{\sigma}^2 \sqrt{2}}{\sqrt{m}}, \tag{17}$$

where m is the number of signals involved in the parameter estimation. According to Eqs. (4) and (5), we can obtain

$$T_{1,2_{\min}} \approx \left(\sqrt{T}_{1,2} - z_{\text{QPE}} \sqrt{\frac{1 + T_{1,2} N_{1,2}}{mV_A}}\right)^2, \tag{18}$$

$$N_{1,2_{\max}} \approx N_{1,2} + z_{\text{QPE}} \frac{(1 + T_{1,2} N_{1,2})\sqrt{2}}{T_{1,2}\sqrt{m}}. \tag{19}$$

The symmetry of the intermediate source protocol is not affected when the finite size is considered.

$$V = V_1 = V_2, \; T_{\min} = T_{1_{\min}} = T_{2_{\min}}, \; N_{\max} = N_{1_{\max}} = N_{2_{\max}}. \tag{20}$$

When the HLA is inserted by Bob's output, it is equivalent to a new EPR state being sent on a new Gaussian channel. Combined with finite-size analysis for parameters, the new EPR parameters $\hat{\varsigma}_2$, the channel transmission rate $\hat{\eta}_2$ and the extra noise $\hat{N}_2^g$ are provided by

$$\hat{\varsigma}_2 = \lambda \sqrt{\frac{(g^2-1)\left(\hat{N}_{2_{\max}} - 2\right)\hat{T}_{2_{\min}} - 2}{(g^2-1)\hat{N}_{2_{\max}}\hat{T}_{2_{\min}} - 2}}, \tag{21}$$

$$\hat{\eta}_2 = \frac{g^2 \hat{T}_{2_{\min}}}{(g^2-1)T_{1.2}\left[(1/4)(g^2-1)\left(\hat{N}_{2_{\max}} - 2\right)\hat{N}_{2_{\max}}\hat{T}_{2_{\min}} - N_{1.2} + 1\right] + 1}, \tag{22}$$

$$\hat{N}_2^g = N_{1.2} + \frac{1}{2}(g^2-1)(2 - \hat{N}_{2_{\max}})\hat{N}_{2_{\max}}\hat{T}_{2_{\min}}. \tag{23}$$

The new variance $\hat{V}_2$ is

$$\hat{V}_2 = (1 + \hat{\varsigma}_2^2)/(1 - \hat{\varsigma}_2^2). \tag{24}$$

Now, the formulae for computing $V(\varsigma_1)$, $V(\varsigma_2)$, and $V(\varsigma_3)$ are given by

$$V(\varsigma_1) = \hat{T}_{1_{\min}} V_1 + \left(1 - \hat{T}_{1_{\min}}\right) W_1 + \hat{T}_{1_{\min}} \hat{N}_{1_{\max}}, \tag{25}$$

$$V(\varsigma_2) = G(\hat{\eta}_2 \hat{V}_2 + (1 - \hat{\eta}_2) W_2 + \hat{\eta}_2 \hat{N}_2^g + \hat{\eta}_2 \hat{X}_{\text{h}}, \tag{26}$$

$$V(\varsigma_3) = \sqrt{G\hat{T}_{1_{\min}} \hat{\eta}_2 (V_1 \hat{V}_2 - 1)}. \tag{27}$$

When a flawless homodyne detection is run and the detector is free of noise,

$$\hat{X}_{\text{h}} = \frac{1 - \tau + v_{\text{el}}}{G\tau}. \tag{28}$$

Thus, Alice and Bob's covariance matrix can be found. The Z and I are the Pauli matrices.

$$\begin{pmatrix} \left(\hat{T}_{1_{\min}} V_1 + \left(1-\hat{T}_{1_{\min}}\right) W_1 + \hat{T}_{1_{\min}} \hat{N}_{1_{\max}}\right) I & \sqrt{G\hat{T}_{1_{\min}} \hat{\eta}_2 \left(V_1 \hat{V}_2 - 1\right)} Z \\ \sqrt{G\hat{T}_{1_{\min}} \hat{\eta}_2 \left(V_1 \hat{V}_2 - 1\right)} Z & \left(G\left(\hat{\eta}_2 \hat{V}_2 + (1-\hat{\eta}_2) W_2 + \hat{\eta}_2 \hat{N}_2^g + \hat{\eta}_2 \hat{X}_{\mathrm{h}}\right)\right) I \end{pmatrix}$$

Next, the mutual information $S(A:B)$ between Alice and Bob can be calculated,

$$S(A:B) = \frac{1}{2}\log_2\left(\frac{V(\varsigma_1)+1}{V(\varsigma_1)+1-(V(\varsigma_3)^2/V(\varsigma_2))}\right). \quad (29)$$

The information that Eve stole is

$$S_{\mathrm{Qpe}}(A:E) = S(AB) - S(BC|A), \quad (30)$$

where

$$S(AB) = G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2], \quad (31)$$

$$S(BC|A) = G\left[\frac{\lambda_3-1}{2}\right] + G\left[\frac{\lambda_4-1}{2}\right], \quad (32)$$

in which

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \quad (33)$$

$\lambda_{1.2}$ is obtained from Eq. (23)

$$\lambda_{1.2}^2 = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D^2}], \quad (34)$$

where

$$C = V^2(\varsigma_1) + V^2(\varsigma_2) - 2V^2(\varsigma_3),$$
$$D = V(\varsigma_1)V(\varsigma_2) - V^2(\varsigma_3). \quad (35)$$

$\lambda_{3.4}$ is obtained from Eq. (25)

$$\lambda_{3.4}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}]. \quad (36)$$

When performing homodyne detection to coherent states,

$$A = \frac{V(\varsigma_1) + V(\varsigma_2)D + C}{V(\varsigma_1)+1},$$
$$B = D(V(\varsigma_2)+D)/(V(\varsigma_1)+1). \quad (37)$$

The value of the privacy amplification $\Delta(n)$ is given by the following equation:

$$\Delta(n) = (2\dim H_x + 3)\sqrt{\log_2\left(\frac{2/\bar{Q}}{n}\right)} + \frac{2}{nQ}\log\left(\frac{1}{Q_{\mathrm{PA}}}\right). \quad (38)$$

Eventually, the secure key rate is derived.

4. Simulation

We concentrate on the nature of the modified protocol in this section. First, we conduct finite-size analysis of the protocol and compare the transmission distances of the original protocol and the protocol with HLA amplifiers. Based on the modified protocol's superiority in terms of the key rate, we apply it to a practical system. The effects of the system's critical parameters on the modified protocol are investigated. We investigate the impact of the protocol with the HLA in this section and analyze its finite-size impact. We assume that the protocol performs quantum key distribution in ideal circumstances. Although the key rate that considers the finite size is lower, the simulation results will be closer to reality. The reason for this is that, when the finite size is considered, not all bits are used to encode information, and some of them are used for channel estimation and will be discarded during reconciliation. Security is increased in the finite-size case. The key rate is lower than the conventional protocol when discrete modulation is used with the source-in-the-middle protocol (the reason for this may not be the use of optimal variance, which needs further exploration). Also, the source-in-the-middle protocol using the HLA has a much greater maximum transmission distance than it does. It is advantageous to use the protocol on a real system later. The linear hybrid amplifier has a significant effect on the source-in-the-middle of the key rate. As shown in Fig. 2, the key rate of the original protocol with finite-size analysis begins to decline drastically at 12 km, while the modified protocol can still communicate at a high key rate at 95 km. It is clear that the modified protocol offers superior transmission qualities. It demonstrates that the HLA can overcome the drawbacks of the traditional protocol's short transmission distance, and has strong compatibility with the source-in-the-middle distribution protocol. It shows that the HLA has a very significant influence on the source-in-the-middle distribution protocol. Compared to the unmodified protocol, it increases the quantum safe transmission distance by a factor of nearly seven. The modified protocol is applied to a system. As shown in Figs. 3–5, the effects of two critical amplifier parameters, G and g, as well as extra noise N, on the protocol's key rate are investigated. In fact, the transmission distance is sensitive to G and g within certain confidence intervals.

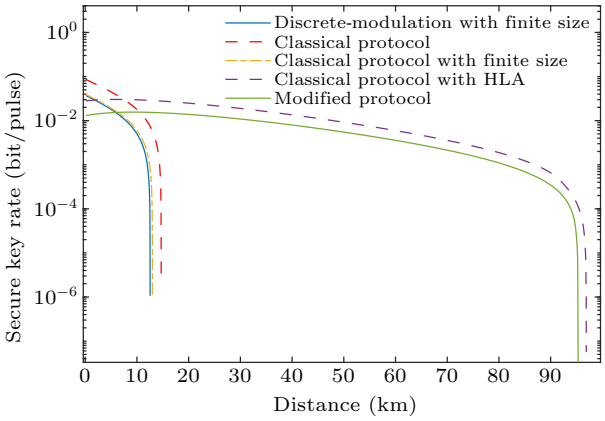


Fig. 2. The key rates of the modified and the original protocols with finite size are compared. The original protocol with finite size and discrete modulation with finite size are used as references.

To maximize the key rate in a certain case, we search for an optimal G within the legal region. We adjust the other parameters of the system: $z_{\mathrm{QPE}/2} = 6.5$, $m = n = N/2 = 10^8$, $\dim H_x = 2$, $\bar{Q} = 10^{-10}$. The finite size of T and N yields $T_{\min}$ and $N_{\max}$. The secure key is computed using the method described in Section 2. The relationship between them is roughly understood in Fig. 3(a), but it is not intuitive. As a result, we choose the longer distance (60 km, 75 km, 70 km) to investigate the association between the key rate and distance. If we choose a short distance (likely 10 km), it is meaningless, since the distance is the main factor affecting the key rate. In this case, the key rate is always large, whether or not an amplifier is plugged in. From Fig. 3(b), we find that when the transport distance is 65 km, we can compensate the key rate to a higher level by adjusting $G = 3$. When longer transport distances (65 km, 70 km) are required, a larger G is needed to maintain the communication. Of course, the value of G does not totally compensate for the negative effects of distance, and the key rate constantly drops gradually as the distance increases. Furthermore, when a particular data value G is reached, the key rate does not change much with G. We can find the optimal G in different systems of quantum communication using a similar method.

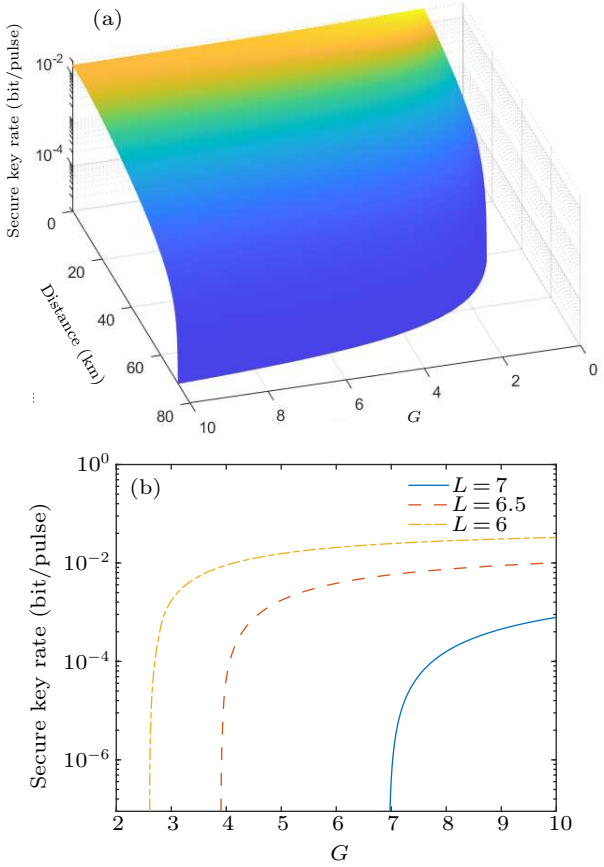


Fig. 3. We used three-dimensional surface plots and two-dimensional curve plots to investigate the effect of G on the system. Here, $g = 2.5$, $N = 0.06$ are the other parameters.

The g is another important parameter of the HLA. The HLA is composed of a DLA and an NLA, where G is a key parameter of the DLA and g is an important parameter of the NLA. Studying the effect of the g on the system is as important as studying G. In this system, the same method is used to find the optimal g. By analyzing Figs. 4(a) and 4(b), similarly, we can conclude that a larger g improves the performance of the quantum channel, both in terms of the key rate and transmission. The parameter g is very effective in the gain interval (2.5–3). Based on the desired length of the quantum channel, we can select the optimal parameters to achieve stable communication.

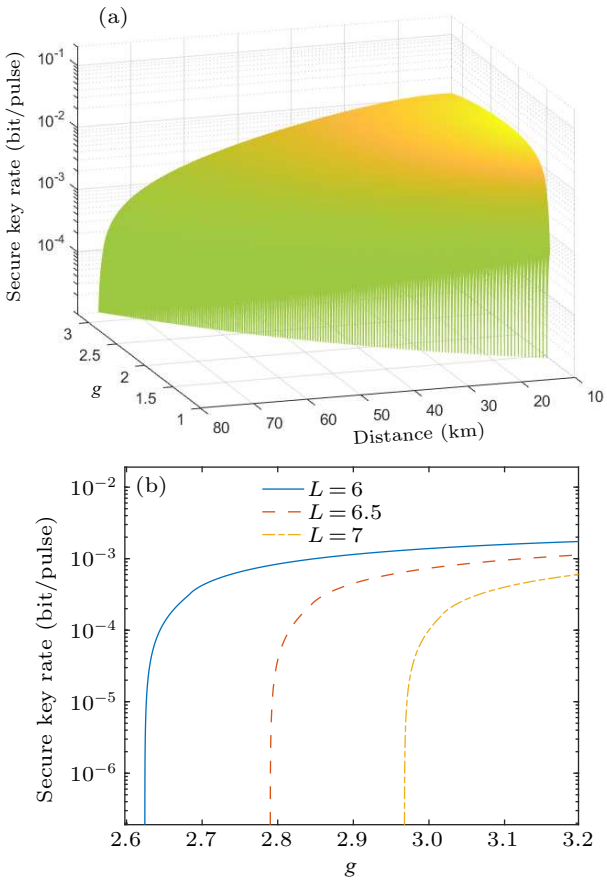


Fig. 4. The impact of g on the system is examined using two-dimensional curve plots and three-dimensional surface plots. The other parameters are $G = 2$, $N = 0.06$.

The ability to resist noise is tested in this system with $g = 3$, $G = 8$. In fact, the noise is dynamic rather than static in the quantum channel. Normal communication must be possible, even in the presence of maximum noise, to keep the channel secure; therefore, the effect of noise on the system must be investigated. The noise interval of the general channel is between 0.01 and 0.1. The additional noise is antagonistic to the channel in Fig. 5(a). In Fig. 5(b), if the noise upper bound is 0.04 dB, the system can achieve 90km communication, and when the noise rises to 0.08 dB, the distance of secure communication drops to 80 km.

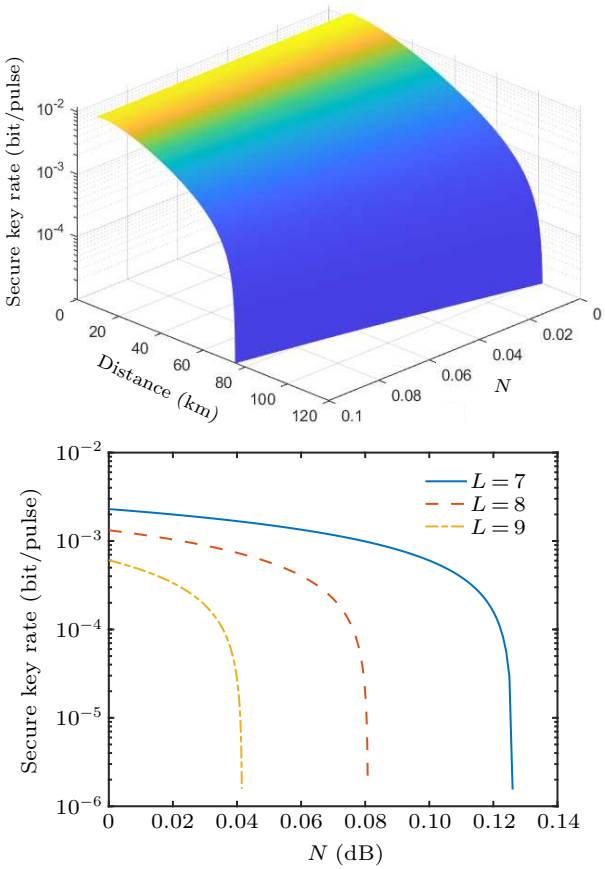


Fig. 5. How noise relates to the distance (a) and system key rate (b).

Even in 0.12 dB noise, it can still maintain a key rate of more than 10^4 (bit/pulse) in 70 km. The modified protocol has a high resistance to noise, and can be widely used in practice.

5. Conclusion

In this paper, we use the HLA to improve the source-in-the-middle distribution protocol. The shortcomings of the original protocol with regard to transmission distance have been overcome. The finite-size effect of the modified protocol has also been analyzed in the protocol. Compared with the original protocol, the modified protocol has better transmission, and can achieve 95 km transmission in ideal conditions. We specifically discuss the effect of the gain coefficient G, g on the key rate between the good simulation results of the protocol after inserting the HLA. To some extent, a larger G or g can improve the key rate for a given distance. However, the negative effect of distance on the key rate cannot be fully compensated, and the increases in the key rate with G, g is not significant up to a certain value. Also, the effect of noise on the modified protocol is discussed. The simulation results show that the modified protocol can transmit over long distances of 70 km under the noise conditions of 0.12 dB. It is excellent and broadens the application range of CVQKD significantly. In practical applications, we adjust the optimal G and g to apply HLA to different Gaussian channels to maximize the key rate and distance.

Acknowledgments

Project supported by the National Natural Science Foundation of China (Grant No. 62201620), the Outstanding Youth Program of Education Department of Hunan (Grant No. 21B0228), Changsha Municipal Natural Science Foundation (Grant No. kq2202293), Hunan Students' Platform for innovation and entrepreneurship training program (Grant No. S202210538069), and the Research Fund of Central South University of Forestry and Technology (Grant No. 1121001703).

References

[1] Ma H X, Bao W S and Li H W 2016 *Chin. Phys. B* **25** 080309
[2] Zhang Y Y, Bao W S, Li H W, Zhou C, Wang W and Jiang M S 2017 *Chin. Phys. Lett.* **34** 100302
[3] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Song X T, Li F Y, Wang D, Chen H, Han Y G, Huang J Z, Guo J F, Hao P L, Li M, Zhang C M, Liu D, Liang W Y, Miao C H, Wu P, Guo G C and Han Z F 2014 *Opt. Express* 2221739
[4] Li J J, Wang Y, Li H W, Peng P, Zhou C, Jiang M S, Ma H X, Feng L X and Bao W S 2017 *Chin. Phys. Lett.* **34** 100302
[5] Chen R K, Bao W S, Bao H Z, Zhou C and Jiang M S 2017 *Chin. Phys. Lett.* **34** 100302
[6] Nanrun Z, Guihua Z and Lihua G 2007 *American Journal of Cardiology* **95** 2
[7] Takeda S, Fuwa M and Loock P V 2014 *Phys. Rev. Lett.* 114
[8] Wu Y D and Zhou J 2016 *Phys Rev. A* **93** 022325
[9] Pu W, Wang X, Li Y 2018 *Entropy* **20** 157
[10] Liao S 2017 *Science* **356** 1140
[11] Xiao M, Cao Y R and Song X L 2017 *Chin. Phys. Lett.* **34** 100302
[12] Zhou J, Huang D and Guo Y 2018 *Phys Rev. A* **98** 042303
[13] Xu P, Bao W S, Li H W, Wang Y and Bao H Z 2017 *Chin. Phys. Lett.* **34** 100302
[14] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305
[15] Mao Y, Liu Q and Guo Y 2019 *Chin. Phys. Lett.* **36** 5
[16] Liu C Q, Zhu C H, Wang L H, Zhang L X and Pei C X 2016 *Chin. Phys. Lett.* **33** 100302
[17] Jouguet P, Kunz-Jacques, Sébastien and Leverrier A 2013 *Nat. Photon.* **7** 378
[18] Li Y M, Wang X Y and Bai Z L 2017 *Chin. Phys. B* **25** 102
[19] He Y, He Y M and Wei Y J 2017 *Phys. Rev. Lett.* 119
[20] Buzek V and Hillery M 1996 *Phys Rev. A* **54** 1844
[21] Oppenheim J and Wehner S 2010 *Science* **330** 1072
[22] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343
[23] Qi B, Zhu W and Qian L 2010 *New J. Phys.* **12** 2991
[24] Tang G Z, Sun S H and Li Y C 2019 *Chin. Phys. Lett.* **36** 100302
[25] Gan Y H, Wang Y, Bao W S, He R S, Zhou C and Jiang M S 2019 *Chin. Phys. Lett.* **36** 100302
[26] Xie C L, Guo T, Wang Y J, Huang D and Zhang L 2018 *Chin. Phys. Lett.* **35** 100302
[27] Guo Y, Liao Q and Wang Y 2017 *Phys. Rev. A.* **95** 032304
[28] Weedbrook C 2012 *Phys. Rev. A* **87** 1110
[29] Gong F, Jiang M and Wang T Y 2020 *Journal of Optoelectronics Laser*
[30] Zhou J, Shi R H and Feng Y Y 2019 *J. Phys. A: Math. Gen.* **52** 245303
[31] Xiang Y, Wang Y and Ruan X 2021 *Physica Scripta* **96** 065103
[32] Wang T, Yu S and Zhang Y C 2014 *Phys. Lett. A* **378** 2808
[33] Zhang J, Zhang Y C and Zheng Z 2020 *Opt. Express*
[34] Zhang X, Zhang Y and Zhao Y 2017 *Phys. Rev. A* **6** 042334
[35] Leverrier A and Grangier P 2010 *Phys. Rev. A* **81** 062314