

Improvement of a continuous-variable measurement-device-independent quantum key distribution system via quantum scissors

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪), Fan Jing(荆凡), Zhe-Kun Zhang(张哲坤), Jin Qi(齐锦), and Chen He(贺晨)

Citation: Chin. Phys. B, 2022, 31 (**9**): 090304. DOI: 10.1088/1674-1056/ac6dba
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Phase-matching quantum key distribution with light source monitoring

Wen-Ting Li(李文婷), Le Wang(王乐), Wei Li(李威), and Sheng-Mei Zhao(赵生妹)
Chin. Phys. B, 2022, 31 (**5**): 050310. DOI: 10.1088/1674-1056/ac4101

Measurement-device-independent quantum dialogue

Guo-Fang Shi(石国芳)
Chin. Phys. B, 2021, 30 (**10**): 100303. DOI: 10.1088/1674-1056/ac140a

Detection and quantification of entanglement with measurement-device-independent and universal entanglement witness

Zhi-Jin Ke(柯芝锦), Yi-Tao Wang(王轶韬), Shang Yu(俞上), Wei Liu(刘伟), Yu Meng(孟雨), Zhi-Peng Li(李志鹏), Hang Wang(汪航), Qiang Li(李强), Jin-Shi Xu(许金时), Ya Xiao(肖芽), Jian-Shun Tang(唐建顺), Chuan-Feng Li(李传锋), Guang-Can Guo(郭光灿)
Chin. Phys. B, 2020, 29 (**8**): 080301. DOI: 10.1088/1674-1056/ab9288

Performance analysis of continuous-variable measurement-device-independent quantum key distribution under diverse weather conditions

Shu-Jing Zhang(张淑静), Chen Xiao(肖晨), Chun Zhou(周淳), Xiang Wang(汪翔), Jian-Shu Yao(要建姝), Hai-Long Zhang(张海龙), Wan-Su Bao(鲍皖苏)
Chin. Phys. B, 2020, 29 (**2**): 020301. DOI: 10.1088/1674-1056/ab5efd

Measurement-device-independent quantum cryptographic conferencing with an untrusted source

Rui-Ke Chen(陈瑞柯), Wan-Su Bao(鲍皖苏), Yang Wang(汪洋), Hai-Ze Bao(包海泽), Chun Zhou(周淳), Mu-Sheng Jiang(江木生), Hong-Wei Li(李宏伟)
Chin. Phys. B, 2017, 26 (**1**): 010302. DOI: 10.1088/1674-1056/26/1/010302

Improvement of a continuous-variable measurement-device-independent quantum key distribution system via quantum scissors

Lingzhi Kong(孔令志), Weiqi Liu(刘维琪)†, Fan Jing(荆凡), Zhe-Kun Zhang(张哲坤), Jin Qi(齐锦), and Chen He(贺晨)‡

College of Information Science and Technology, Northwest University, Xi'an 710127, *China*

(Received 24 February 2022; revised manuscript received 22 April 2022; accepted manuscript online 7 May 2022)

We propose a new scheme to enhance the performance of the Gussian-modulated coherent-state continuous-variable measurement-device-independent quantum key distribution (CV-MDI-QKD) system via quantum scissors (QS) operation at Bob's side. As an non-deterministic amplifying setup, we firstly introduce the QS-enhanced CV-MDI-QKD protocol and then investigate the success probability of the QS operation in accordance with the equivalent one-way scheme. Afterwards, we investigate the effect of the QS operation on the proposed scheme and analyze the performance of the QS-enhanced CV-MDI-QKD system under the extreme asymmetric circumstance. Simulation results show that the QS operation can indeed improve the performance of the CV-MDI-QKD system considerably. QS-enhanced CV-MDI-QKD protocol outperforms the original CV-MDI-QKD protocol in both the maximum transmission distance and the secret key rate. Moreover, the better the performance of QS operation, the more significant the improvement of performance of the system.

Keywords: measurement-device-independent, quantum key distribution, quantum scissors, performance

PACS: 03.67.Hk, 03.67.Dd, 03.67.–a **DOI:** 10.1088/1674-1056/ac6dba

1. Introduction

Quantum key distribution (QKD) enables two distant legitimate parties, Alice and Bob, to share secret keys in the presence of eavesdropper (Eve). Based on the laws of Heisenberg's uncertainty principle and no-cloning theory, QKD can achieve unconditional secure communication through the untrusted channel in theory. Currently, the mainstream QKD protocols can be divided into discrete variable quantum key distribution (DVQKD) protocols[1–3] and continuous variable quantum key distribution (CVQKD) protocols.[4–9] The Gaussian-modulated coherent state (GMCS) CVQKD protocol,[10–12] which encodes information on the quadratures of coherent state and measures the quadratures via homodyne detector or heterodyne detector, has become the most favorable protocol. This protocol has been certified to be secure in both asymptotic case[13] and finite-size effect,[14] and its composable security has been established under collective attack. Furthermore, the GMCS CVQKD protocol has been successfully demonstrated in both labs and field tests.

However, theoretical security analyses of CVQKD protocol usually depend on some ideal theoretical hypothesis and models. Actually, practical CVQKD systems are usually deviated from ideal theoretical models. Devices applied in practical CVQKD systems may be imperfect,[15] such as laser source, beam splitters and detectors. Deviation between non-ideal devices and idealized models will open loopholes for Eve to eavesdrop encrypted information without being discovered. To defend side channel attacks,[16] some researchers put forward measurement-device-independent (MDI) QKD protocol.[17–21] Similarly, MDI-QKD protocols can be mainly divided into discrete variable (DV) MDI-QKD protocols[22] and continuous variable (CV) MDI-QKD protocols.[23–25] Compared to a DV-MDI-QKD system, the maximum transmission distance of the CV-MDI-QKD system is not satisfactory. Therefore, improvement of performance of the CV-MDI-QKD system has been a hot spot in recent years.

In order to improve performance of CV-MDI-QKD systems, some researchers have proposed various schemes, which can be mainly summarized as optical amplifier,[26–29] photon subtraction operation[30–34] and quantum catalysis operation.[35–37] Among the mentioned methods, photon subtraction and quantum catalysis can improve the system performance by enhancing the success probability of non-Gaussion operations, while optical amplifier improves the system performance by amplifying the amplitude of the coherent state. Among various amplifiers, the heralded noiseless linear amplifier (NLA)[38–41] outperforms the other linear amplifiers, since it will maintain the initial noise level while amplifying the amplitude of the coherent state. However, the implementation of NLA should be under strict assumption that the amplifier is ideally noiseless, and it is of challenge to apply it to a practical CV-MDI-QKD system.

Fortunately, quantum scissors (QS),[42–48] an non-deterministic amplifying setup which combines the input sig-

†Corresponding author. E-mail: vickylwq1991@nwu.edu.cn
‡Corresponding author. E-mail: chenhe@nwu.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

nal with a single photon, can be regarded as an ideal NLA under weak amplitude of input signal. In this paper, we propose a new scheme to improve the performance of a GMCS CV-MDI-QKD system by introducing QS operation at Bob's side. By amplifying the amplitude of the input state, the system performance can be improved considerably.[46] Simulation results show that the QS-enhanced CV-MDI-QKD protocol indeed outperforms the original CV-MDI-QKD protocol in both the secret key rate and the maximum transmission distance. Moreover, the better the performance of QS operation, the more significant the improvement of the performance of the system.

The rest of this paper is structured as follows. In Section 2, we investigate the proposed scheme of the GMCS CV-MDI-QKD protocol with QS operation in detail. Afterwards, the performance analysis of the new scheme is demonstrated in Section 3. Eventually, conclusions are drawn in Section 4.

2. The new scheme of CV-MDI QKD with quantum scissors

In this section, we firstly introduce the GMCS CV-MDI-QKD protocol with QS operation in detail. Afterwards, we investigate the QS operation in accordance with the equivalent one-way scheme, especially the success probability of the QS operation. Eventually, we perform simulation to demonstrate that success probability will be affected by some parameters.

2.1. The QS-enhanced GMCS CV-MDI-QKD protocol

Generally speaking, the prepare-and-measure (PM) scheme is usually applied for practical implementation, while the equivalent entanglement-based (EB) scheme is of great convenience for analysis. The EB scheme of the CV-MDI-QKD protocol with QS operation is drawn in Fig. 1, which is comprised of the following steps.

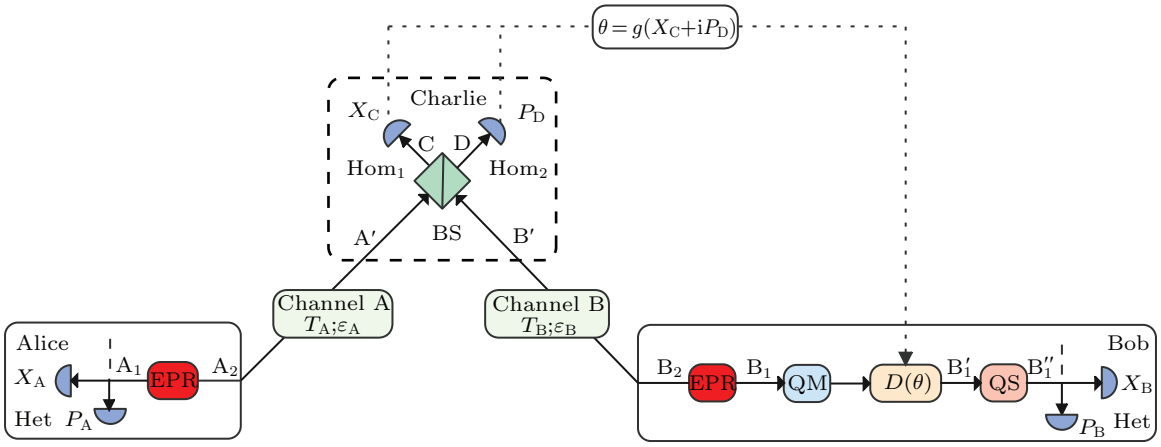


Fig. 1. The EB scheme of the GMCS CV-MDI-QKD protocol with QS operation. EPR: Einstein–Podolsky–Rosen state; BS: beam splitter; Hom: homodyne detector; Het: heterodyne detector; QM:quantum memory; $D(\theta)$: displacement operation; QS: quantum scissors operation.

Step 1 Alice prepares an EPR state with modulation variance V_A and retains mode A_1 to perform heterodyne detection, while the other mode A_2 is transmitted to the untrusted third party Chaile via the lossy channel A with transmittance T_A and excess noise ε_A. Similarly, Bob prepares another EPR state with modulation variance V_B and retains mode B_1, while the other mode B_2 is transmitted to the untrusted third party Chaile via the lossy channel B with transmittance T_B and excess noise ε_B. Thus the corresponding transmittance of the channels A and B can be expressed as

$$T_A = 10^{\frac{-\alpha L_{AC}}{10}}, \quad T_B = 10^{\frac{-\alpha L_{BC}}{10}}, \tag{1}$$

where $\alpha = 0.2$ dB/km represents the loss coefficient of the fiber channel, L_{AC} and L_{BC} depict the length of the channels A and B, respectively. As a result, the total transmission distance between Alice and Bob is $L_{AB} = L_{AC} + L_{BC}$.

Step 2 After being transmitted through the lossy channel, modes A' and B' are obtained. Then Charlie interferes them at the 50:50 beam splitter (BS) with output modes C and D. Afterwards, Charlie performs homodyne detection to measure the quadrature x of the mode C and the quadrature p of the mode D. As consequence, measurement results X_C and P_D are obtained and announced publicly by Charlie.

Step 3 The mode B_1 is stored in the quantum memory until Charlie announces the measurement result $\{X_C, P_D\}$ and returns $\theta = g(X_C + iP_D)$ to the displacement operation $D(\theta)$, where g depicts the gain of the displacement operation. When the mode B_1 is released from quantum memory, Bob performs $D(\theta)$ on the mode B_1, further obtains the mode B_1'. The mode B_1' is probabilistically amplified by the QS operation and the amplified mode B_1'' is obtained. Afterwards, Alice and Bob perform heterodyne detection on the modes A_1 and B_1'', respectively. Eventually, Alice and Bob obtain the final measurement results $\{X_A, P_A\}$ and $\{X_B, P_B\}$. It is noteworthy that the measurement results will be useful if and only if the QS setup works successfully.

Step 4 Alice and Bob accomplish the steps of parameter estimation, reverse reconciliation and privacy amplification

through a classical channel. Ultimately, Alice and Bob share the encrypted key.

2.2. The equivalent one-way model of the CV-MDI-QKD protocol with QS operation

In the proposed scheme, since the QS operation is an non-deterministic amplifying setup, the final secret key rate should be multiplied by the success probability P_{succ}. Therefore, it is of great significance to investigate the success probability P_{succ}. For simplicity, under the assumption that all operations at Bob's side are untrusted except the heterodyne detection, the EB scheme of the GMCS CV-MDI-QKD protocol can be converted into a specific one-way scheme using entanglement swapping, in which both Alice and Bob perform heterodyne detection on modes A_1 and B_1'', respectively, as drawn in Fig. 2. In what follows, we firstly give a brief introduction of QS operation and further investigate the success probability P_{succ} in detail.

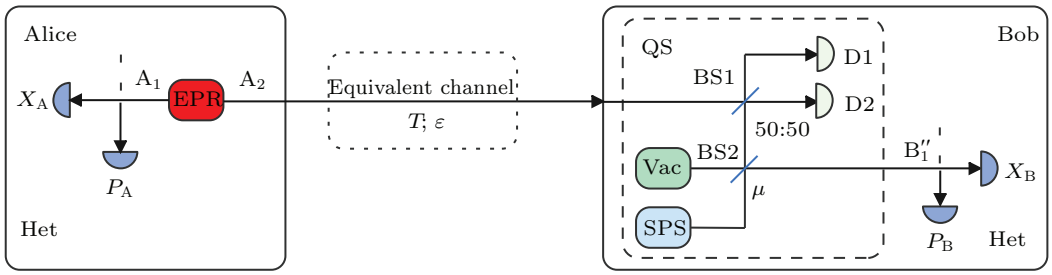


Fig. 2. Equivalent one-way scheme of GMCS CV-MDI-QKD with QS operation. Vac: vaccum states; SPS: single photon source; BS1: balanced beam splitter; BS2: unbalanced beam splitter with transmittance μ; D1 and D2: single photon detectors.

The schematic view of the QS operation is drawn in the dotted box in Fig. 2, which is composed of two single photon detectors and two beam splitters. The upper beam splitter is balanced with transmittance 50:50 whilst the lower beam splitter is unbalanced with transmittance μ. The two single photon detectors and the balanced beam splitter form a partial Bell-state measurement (BSM) module. In addition, the vacuum states and the single-photon source (SPS) are introduced here. For simplicity, it is usually supposed that the SPS is on-demand and ideal. Meanwhile, the detection efficiencies of the two single photon detectors are also supposed to be unity. When the single photon generated by SPS and the vacuum states passing the unbalanced beam splitter, an asymmetric entangled state is obtained and further drives the BSM module. Then the balanced BS1 couples the input signal from Alice with the asymmetric entangled state. Finally, the coupled state is transmitted to the single photon detectors D1 and D2. For an input state in the space spanned by the vacuum states and the single photon, the QS can offer an asymmetric teleportation functionality, whenever the BSM operation is successful, i.e., if and only if one of D1 and D2 detector clicks. It is worth noting that the QS operation is considered to be a failure under the case that both detectors click or neither clicks. The amplification gain of the QS operation is given by $k=\sqrt{(1-\mu)/\mu}$, then the success probability of the QS operation is expressed as[44]

$$P_{\text{succ}}=\frac{1}{k^2+1}\left[\frac{4(2F+1)k^2+3F}{(2F+1)^2}-\frac{k^2}{F}\right], \tag{2}$$

with

$$F=\frac{1}{2}+\frac{1}{4}T\left[2(\delta^2-1)+\frac{(1-T)\varepsilon}{T}\right], \tag{3}$$

where ε and T represent the equivalent excess noise and the equivalent transmittance, respectively, in the one-way scheme, and $\delta=\sqrt{\frac{V_{\text{A}}}{2}+1}$ is the parameter relevant to EPR state. The equivalent excess noise and transmittance in the one-way scheme can be given by[33]

$$\begin{aligned}\varepsilon &= 1+\frac{1}{T_{\text{A}}}\left[T_{\text{B}}(\chi_{\text{B}}-1)+T_{\text{A}}\chi_{\text{A}}\right.\\ &\quad\left.+\left(\frac{\sqrt{2(V_{\text{B}}-1)}}{g}-\sqrt{T_{\text{B}}(V_{\text{B}}+1)}\right)^2\right],\\ T &= \frac{g^2T_{\text{A}}}{2},\end{aligned} \tag{4}$$

where $\chi_{\text{A}}=\frac{1-T_{\text{A}}}{T_{\text{A}}}+\varepsilon_{\text{A}}$ and $\chi_{\text{B}}=\frac{1-T_{\text{B}}}{T_{\text{B}}}+\varepsilon_{\text{B}}$. In order to minimize the equivalent excess noise ε, g is usually set to satisfy $g^2=\sqrt{\frac{2(V_{\text{B}}-1)}{T_{\text{B}}(V_{\text{B}}+1)}}$. Consequently, the equivalent excess noise can be simplified to

$$\varepsilon=\varepsilon_{\text{A}}+\frac{1}{T_{\text{A}}}\left[T_{\text{B}}(\varepsilon_{\text{B}}-2)+2\right]. \tag{5}$$

From Eqs. (1)–(5), we can conclude that the success probability of the QS operation behaves as functions of the transmission distances L_{AC} and L_{BC}, the equivalent excess noise ε, the equivalent transmittance T, the transmittance μ of the BS2 and the modulation variance V_{A}. Among these parameters, T and ε are relevant to parameters L_{AC}, L_{BC}, ε_{A} and ε_{B}. As a result, the success probability can be expressed as a function $P_{\text{succ}}=P_{\text{succ}}(L_{\text{AC}},L_{\text{BC}},\varepsilon_{\text{A}},\varepsilon_{\text{B}},\mu,V_{\text{A}})$. For simplicity, we investigate the success probability under the extreme asymmetric circumstance that $L_{\text{AC}}\neq L_{\text{BC}}$ and $L_{\text{BC}}=0$. Therefore, the function can be simplified to $P_{\text{succ}}=P_{\text{succ}}(L_{\text{AC}},\varepsilon_{\text{A}},\varepsilon_{\text{B}},\mu,V_{\text{A}})$.

To demonstrate the effect of the transmittance μ, transmission distance L_{AC} and the excess noise ε_{A} (ε_{B}) and on the

success probability of the QS operation, we perform simulations as shown in Fig. 3. The success probability $P_{\rm succ}$ as a function of modulation variance $V_{\rm A}$ under different transmittance μ is plotted in Fig. 3(a). From top to bottom, the three curves depict the relationship between the success probability $P_{\rm succ}$ and modulation variance $V_{\rm A}$ with transmittance $\mu = 0.8$, $\mu = 0.7$ and $\mu = 0.6$, respectively. Obviously, the success probability $P_{\rm succ}$ increases with the increasing transmittance μ when other parameters are the same. Meanwhile, the success probability $P_{\rm succ}$ increases with the increasing modulation variance $V_{\rm A}$ within a certain range, while the success probability $P_{\rm succ}$ will decrease gradually when $V_{\rm A}$ exceeds a certain value. The certain value can be labeled as the optimal variance and the optimal variance decreases slightly with the increasing transmittance μ.

Afterwards, we investigate the relationship between the success probability $P_{\rm succ}$ and the modulation variance $V_{\rm A}$ with different transmission distance $L_{\rm AC}$, as drawn in Fig. 3(b). The success probability $P_{\rm succ}$ increases with the increasing modulation variance $V_{\rm A}$ within a certain range and decreases gradually when $V_{\rm A}$ exceeds the optimal variance. The optimal variance increases with the increasing transmission distance $L_{\rm AC}$. Meanwhile, we find that the success probability $P_{\rm succ}$ increases with the increasing transmission distance $L_{\rm AC}$ when the optimal variance is exceeded. Finally, the success probability $P_{\rm succ}$ as a function of modulation variance $V_{\rm A}$ for different excess noise $\varepsilon_{\rm A}$ ($\varepsilon_{\rm B}$) is plotted in Fig. 3(c). The success probability $P_{\rm succ}$ increases with the increasing modulation variance $V_{\rm A}$ within a certain range and decreases gradually when $V_{\rm A}$ exceeds the optimal variance. The optimal variance decreases as the excess noise increases. Meanwhile, the success probability $P_{\rm succ}$ changes slightly when the excess noise $\varepsilon_{\rm A}$ ($\varepsilon_{\rm B}$) fluctuates greatly, which implies that the effect of the excess noise on the success probability $P_{\rm succ}$ is much smaller than the transmittance μ and transmission distance $L_{\rm AC}$. In brief, the analysis of success probability $P_{\rm succ}$ of the QS operation is beneficial to select the appropriate parameters to obtain the optimal system performance.

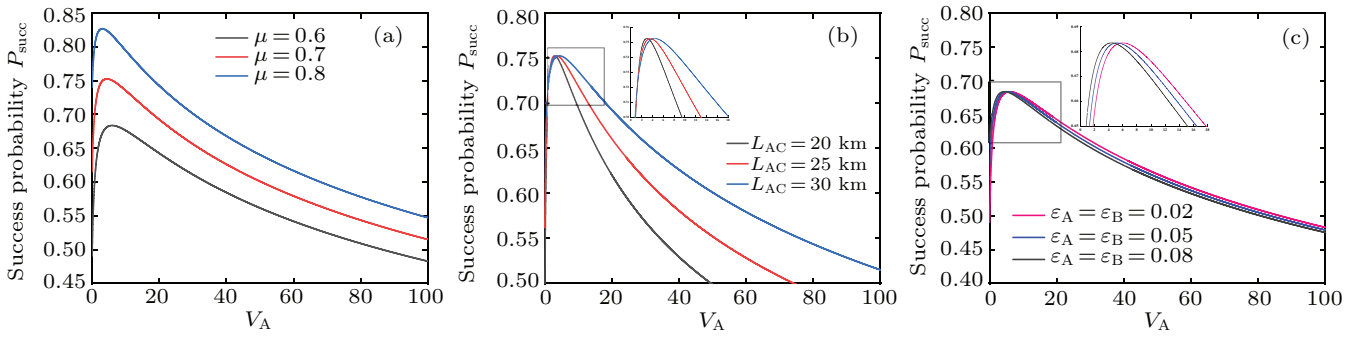


Fig. 3. (a) Success probability as a function of $V_{\rm A}$ with different transmittance μ. The excess noise $\varepsilon_{\rm A}$ ($\varepsilon_{\rm B}$) is fixed at 0.02 and the transmission distance $L_{\rm AC} = 30$ km. (b) Success probability as a function of $V_{\rm A}$ with different transmission distance $L_{\rm AC}$. The excess noise $\varepsilon_{\rm A}$ ($\varepsilon_{\rm B}$) is fixed at 0.02 and the transmittance $\mu = 0.6$. (c) Success probability as a function of $V_{\rm A}$ with different excess noise $\varepsilon_{\rm A}$ ($\varepsilon_{\rm B}$). The transmission distance $L_{\rm AC} = 30$ km and the transmittance $\mu = 0.6$.

3. Performance analysis of the new scheme

As aforementioned, the EB scheme of the QS-enhanced CV-MDI-QKD protocol can be converted into a specific one-way scheme under the assumption that all operations at Bob's side are untrusted except the heterodyne detection. In other words, the EB scheme is a specific case of the equivalent one-way scheme with more constraints on Eve. Therefore, the secret key rate of the equivalent one-way scheme should be a lower bound of the EB scheme. Assuming that the secret key rate of the equivalent one-way scheme and the EB scheme are K^* and $K_{\rm QS}$, respectively, we can further obtain $K_{\rm QS} \geq K^*$.[33] For the sake of simplicity, we use the lower bound of $K_{\rm QS}$ to depict the secret key rate of the QS-enhanced CV-MDI-QKD protocol under collective attack, that is,

$$K_{\rm QS} \geq P_{\rm succ}\left(\beta I_{\rm AB} - \chi_{\rm BE}\right), \tag{6}$$

where β is the efficiency of reverse reconciliation, $I_{\rm AB}$ represents the amount of mutual information between Alice and Bob, and $\chi_{\rm BE}$ is the amount of information constrained by Holevo bound that can be obtained by Eve from Bob.

When Bob performs QS operation successfully, the covariance matrix of $\gamma_{\rm A_1B_1''}$ can be written as

$$\gamma_{\rm A_1B_1''} = \begin{bmatrix} a\mathrm{II} & c\sigma_z \\ c\sigma_z & b\mathrm{II} \end{bmatrix}, \tag{7}$$

where $\mathrm{II} = \mathrm{diag}(1,1)$ and $\sigma_z = \mathrm{diag}(1,-1)$ with

$$a = \left(\frac{8\left[(\delta^2-1)T + (2F+1-(\delta^2-1)T)(k^2(2F+1)+2F)\right]}{(2F+1)^3} - \frac{k^2(2F-(\delta^2-1)T)}{F^2}\right)\frac{\delta^2}{P_{\rm succ}(k^2+1)} - 1,$$
$$b = \frac{4}{P_{\rm succ}(k^2+1)}\left(\frac{4\left[k^2(2F+1)+F\right]}{(2F+1)^2} - \frac{k^2}{F}\right) - 1, \quad c = \frac{8\delta\sqrt{\delta^2-1}}{P_{\rm succ}(k^2+1)(2F+1)^2}k\sqrt{T}. \tag{8}$$

Thus, the mutual information I_{AB} can be calculated by

$$I_{AB} = \log_2 \frac{a+1}{a+1-\frac{c^2}{b+1}}, \tag{9}$$

and for the gaussian-modulated coherent states, χ_{BE} can be simplified to

$$\chi_{BE} = G(\Lambda_1) + G(\Lambda_2) - G(\Lambda_3), \tag{10}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and the symplectic eigenvalues can be given by

$$\Lambda_{1,2} = \sqrt{\frac{(A \pm \sqrt{A^2 - 4B^2})}{2}}, \tag{11}$$

$$\Lambda_3 = a - \frac{c^2}{b+1}, \tag{12}$$

with $A = a^2 + b^2 - 2c^2$ and $B = ab - c^2$.

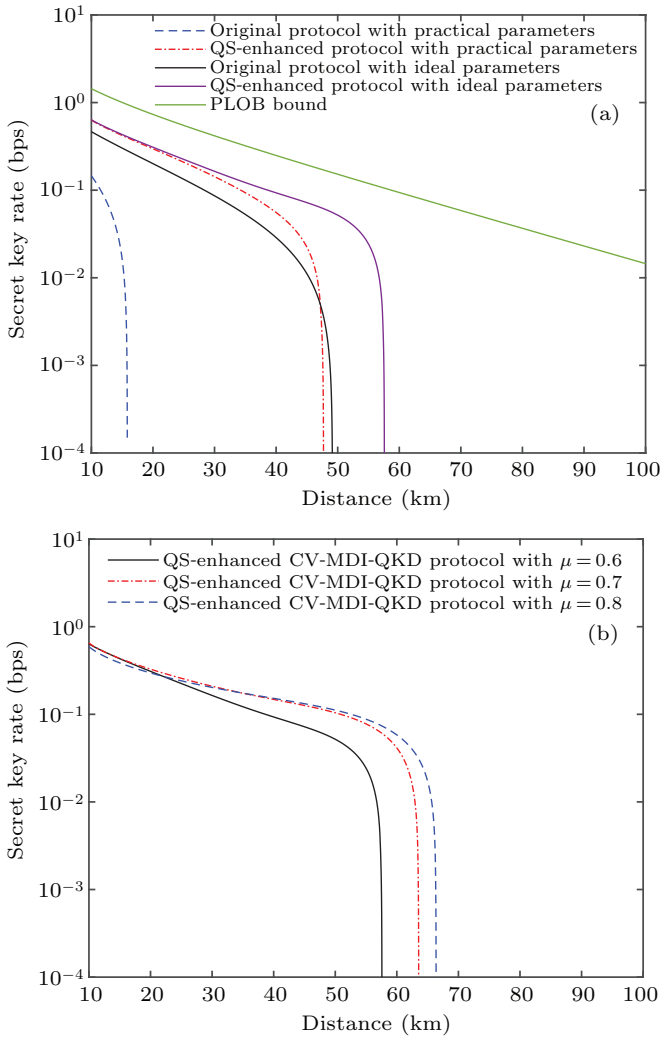


Fig. 4. (a) Performance comparison between the original CV-MDI-QKD protocol and the QS-enhanced CV-MDI-QKD protocol with transmittance $\mu = 0.6$ under practical parameters and ideal parameters, respectively. The practical parameters focus on the detection efficiency of homodyne detector $\eta = 0.97$, electronic noise of homodyne detector $v_{el} = 0.01$ and the ideal parameters focus on the detection efficiency of homodyne detector $\eta = 1$, electronic noise of homodyne detector $v_{el} = 0$. (b) The secret key rate as a function of transmission distance for different transmittance μ. Remaining parameters are similarly fixed: The excess noise $\varepsilon_A = \varepsilon_B = 0.01$, the modulation variance $V_A = 20$, and reconciliation efficiency $\beta = 0.98$.

In what follows, we analyze the performance of the GMCS CV-MDI-QKD system equipped with QS operation under the extreme asymmetric circumstance in detail. Firstly, to investigate the effect of the QS operation on the performance of the GMCS CV-MDI-QKD system, we perform the simulation of the original CV-MDI-QKD protocol[23,24] and the QS-enhanced CV-MDI-QKD protocol, respectively, as illustrated in Fig. 4(a). The blue curve represents the secret key rate of the original CV-MDI-QKD system versus the transmission distance with practical parameters. The red curve represents the secret key rate of the QS-enhanced CV-MDI-QKD system versus the transmission distance with practical parameters. The black curve depicts the relationship between the secret key rate of the original system and the transmission distance with ideal parameters. The purple curve depicts the relationship between the secret key rate of the system equipped with QS operation and the transmission distance with ideal parameters. The green curve is the PLOB bound,[49] which constrains the maximum secret key rate of the system with lossy channel. The results show that the QS-enhanced CV-MDI-QKD protocol outperforms the original CV-MDI-QKD protocol in both the secret key rate and the maximum transmission distance. In other words, QS operation at Bob's side can indeed improve the performance of the CV-MDI-QKD system significantly. In addition, compared to the system with an ideal homodyne detector at Charlie's side, the performance of the system with a practical homodyne detector which has finite detection efficiency and eletronic noise can be improved more considerably via the QS operation. In fact, the improvement of the performance can be attributed to the QS operation which truncates the input state to first order and simultaneously amplifies it by increasing the amplitude of the single photon component relative to the vacuum component.

Then from the schematic view of the QS operation, we can conclude that different transmittance μ corresponds to different QS operation, further leads to different degree of improvement of the performance. As aforementioned, the success probability P_{succ} increases as the transmittance μ increases. In other words, the performance of the QS operation will increase with the increasing transmittance μ. Therefore, we further perform the simulation to demonstrate the effect of the performance of QS operation on the improvement of the system, as plotted in Fig. 4(b). From left to right, curves represent the secret key rate as a function of transmission distance for transmittance $\mu = 0.6$, 0.7, 0.8, respectively. Simulation results indicate that the performance of the QS-enhanced system will improve more significantly with the increasing transmittance μ in both the secret key rate and the maximum transmission distance. In conclusion, the better the performance of QS operation, the more significant the improvement of the performance of the system.

4. Conclusion

In summary, we have proposed a new scheme to enhance the performance of the GMCS CV-MDI-QKD system by applying QS operation at Bob's side. In order to investigate the success probability of the QS operation and demonstrate the effect of the QS operation on the performance of the CV-MDI-QKD system, we perform simulations. The simulation results show that the transmittance of the unbalanced BS, the transmission distance, the excess noise and the modulation variance will all affect the success probability of the QS operation. Therefore, selecting suitable parameters is of great significance for obtaining the optimal performance. Subsequently, the performance analysis indicates that QS operation can indeed improve the performance significantly, in which the QS-enhanced CV-MDI-QKD protocol outperforms the original CV-MDI-QKD protocol in both the secret key rate and the maximum transmission distance. Meanwhile, the better the performance of QS operation, the more significant the improvement of performance of the system.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 62001383) and the Scientific Research Plan Project of Shaanxi Education Department (Natural Science Special Project) (Grant No. 19JK0847).

References

[1] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[2] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3
[3] Warke A, Behera B K and Panigrahi P K 2020 *Quantum Inf. Process.* **19** 407
[4] Ralph T C 1999 *Phys. Rev. A* **61** 010303
[5] Reid M D 2000 *Phys. Rev. A* **62** 062308
[6] Braunstein S L and Van Loock P 2005 *Rev. Mod. Phys.* **77** 513
[7] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[8] Cerf N J, Lévy M and Van Assche G 2001 *Phys. Rev. A* **63** 052311
[9] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[10] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[11] Chi Y M, Qi B, Zhu W, Qian L, Lo H K, Youn S H, Lvovsky A and Tian L 2011 *New J. Phys.* **13** 013003
[12] Zeng G H 2010 *Quantum Private Communication* (Beijing: Higher Education Press) pp. 260–309
[13] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502
[14] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[15] Xu F H, Ma X F, Zhang Q, Lo H K and Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
[16] Lo H K, Curty M and Tamaki K 2014 *Nat. Photonics* **8** 595
[17] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[18] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[19] Yin H L, Chen T Y, Yu Z W, Liu H, You L X, Zhou Y H, Chen S J, Mao Y Q, Huang M Q, Zhang W J, Chen H, Li M J, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X B and Pan J W 2016 *Phys. Rev. Lett.* **117** 190501
[20] Yin H L and Fu Y 2019 *Sci. Rep.* **9** 3045
[21] Yin H L, Zhu W and Fu Y 2019 *Sci. Rep.* **9** 49
[22] Xu F, Qi B, Liao Z and Lo H K 2013 *Appl. Phys. Lett.* **103** 061101
[23] Li Z Y, Zhang Y C, Xu F H, Peng X and Guo H 2014 *Phys. Rev. A* **89** 052301
[24] Ma X C, Sun S H, Jiang M S, Gui M and Liang L M 2014 *Phys. Rev. A* **89** 042335
[25] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein S L, Lloyd S, Gehring T, Jacobsen C S and Andersen U L 2015 *Nat. Photon.* **9** 397
[26] Li F, Zhao W and Guo Y 2018 *Int. J. Theor. Phys.* **57** 112
[27] Guo Y, Zhao W, Li F, Huang D, Liao Q and Xie C L 2017 *Commun. Theor. Phys.* **68** 191
[28] Zhou Y H, Qin S F, Shi W M and Yang Y G 2021 *Optik* **242** 166826
[29] Wu X D, Wang Y J, Huang D and Guo Y 2020 *Front. Phys.* **15** 31601
[30] Peng Q Q, Wu X D and Guo Y 2019 *Appl. Sci.* **9** 1333
[31] Zhao W, Ruan X C, Feng Y Y, Wang X X, Guo Y and Shi R H 2020 *Int. J. Theor. Phys.* **59** 2939
[32] Djordjevic I B 2019 *IEEE Access* **7** 147399
[33] Ma H X, Huang P, Bai D Y, Wang S Y, Bao W S and Zeng G H 2018 *Phys. Rev. A* **97** 042329
[34] Zhao Y J, Zhang Y C, Xu B J, Yu S and Guo H 2018 *Phys. Rev. A* **97** 042328
[35] Zhang S L and Zhang X D 2018 *Phys. Rev. A* **97** 043830
[36] Guo Y, Ye W, Zhong H and Liao Q 2019 *Phys. Rev. A* **99** 032327
[37] Ye W, Zhong H, Wu X D, Hu L Y and Guo Y 2020 *Quantum Inf. Process.* **19** 346
[38] Zhang Y C, Xu M Y, Han S L, Yu S and Gu W Y 2013 *Proceeding of* 2013 *IEEE 4th International Conference on Electronics Information and Emergency Communication*, November 15–17, 2013, Beijing, China, p. 9
[39] Jing F, Liu W Q, Kong L Z and He C 2021 *Entropy* **23** 1691
[40] Zhou J, Shi R H, Y Feng Y Y, Shi J J and Guo Y 2019 *J. Phys. A: Math. Theor.* **52** 245303
[41] Blandino R, Leverrier A, Barbieri M, Etesse J, Grangier P and Tualle-Brouri R 2012 *Phys. Rev. A* **86** 012327
[42] Ghalaii M, Ottaviani C, Kumar R, Pirandola S and Razavi M 2020 *IEEE J. Sel. Areas Commun.* **38** 506
[43] Li Y, Guo Y, Ruan X C and Zhao W 2021 *Int. J. Theor. Phys.* **60** 1949
[44] Ghalaii M, Ottaviani C, Kumar R, Pirandola S and Razavi M 2020 *IEEE J. Sel. Top. Quantum Electron.* **26** 6400212
[45] Ralph T C and Lund A P 2009 *AIP Conf. Proc.* **1110** 155
[46] Winnel M S, Hosseinidehaj N and Ralph T C 2020 *Phys. Rev. A* **102** 063715
[47] Ghalaii M, Kumar R and Razavi M 2017 *Proceeding of 2017 Conference on Lasers and Electro-Optics Europe & European Quantum Electronics Conference (CLEO/Europe-EQEC)*, June 25–29, 2017, Munich, Germany, p. 1
[48] Seshadreesan K P, Krovi H and Guha S 2020 *Phys. Rev. Res.* **2** 013310
[49] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 *Nat. Commun.* **8** 15043