Article

Discrete modulation source enhancement for continuous variable quantum key distribution through photon catalyzing

Zhengchun Zhou[1,2], Shanhua Zou[1], Yun Mao[1],Tongcheng Huang[2], Ying Guo[1,2,*]

[1] School of Automation, Central South University, Changsha 410083, China
[2] College of Information Engineering, Shaoyang University, Shaoyang 422000, China
* Correspondence: yingguo@csu.edu.cn;

Abstract: Establishing global high-rate secure communications is a potential application of continuous-variable quantum key distribution (CVQKD) but also challenging for long-distance transmissions in metropolitan areas. The discrete modulation(DM) can make up for the shortage of transmission distance that has a unique advantage against all side-channel attacks, however its further performance improvement requires source preparation in the presence of noise and loss. Here, we consider the effects of photon catalysis (PC) on the DM-involved source preparation for lengthening the maximal transmission distance of the CVQKD system. We address a zero-photon catalysis (ZPC)-based source preparation for enhancing the DM-CVQKD system. The statistical fluctuation due to the finite length of data is taken into account for the practical security analysis. Numerical simulations show that the ZPC-based DM-CVQKD system can not only achieve the extended maximal transmission distance, but also contributes to the reasonable increase of the secret key rate. This approach enables the DM-CVQKD to tolerate lower reconciliation efficiency, which may promote the practical implementation solutions compatible with classical optical communications using state-of-the-art technology.

Keywords: Photon catalyzing; Discrete modulation; Continuous-variable; Quantum key distribution; Quantum communications

1. Introduction

Quantum key distribution (QKD) [1–4] that allows two legal parties to distill a common secret key, enables information-theoretically secure communications, despite the potential presence of a ferocious eavesdropper. The security is guaranteed by fundamental laws of quantum physics [5–7]. To this end, it has spurred lots of interest over the last decades, giving birth to two main approaches, i.e., discrete-variable (DV) QKD [8,9] and continuous- variable (CV) QKD [10–20]. A possible breakthrough may come from the practical implementation of CVQKD, which has an advantage of being implemented with standard telecommunication components, and thus allowing to exploit the heritage of integrability in existing optical communication system in terms of high speed components and space qualification.

At present, there are several mainstream modulations in CVQKD, such as Gaussian modulated(GM) CVQKD [11–15] and discretely modulated(DM) CVQKD [16–20]. In the former, the transmitter encodes key bits in the quadratures ($\hat{x}$ and $\hat{p}$) of optical field with Gaussian modulation, while the receiver can restore the secret key through high-speed and high-efficiency coherent detector [13]. It is GM-CVQKD that could potentially achieve higher secret key rate, however it seems limited to the shortening distance, compared with its DVQKD counterpart. The problem is that the reconciliation

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

efficiency is still low for GM-CVQKD in the long-distance transmission. Whereas in the later, one can solve this problem by using discrete modulation for CVQKD [16]. In DM-CVQKD it generates nonorthogonal coherent states and takes advantage of the sign of the measured quadrature of each state for encoding information rather than exploits the fixed quadrature $\hat{x}$ or $\hat{p}$ itself [17]. Consequently, it has a merit of both high reconciliation efficiency in the long-distance transmission and high tolerance against the excess noise generated by the quantum channel so that it could extend the maximal transmission distance of the CVQKD system [18]. While theoretics and experiments of the DM-CVQKD system have been shown recently that this goal is achievable, we still face a great challenge in promoting its performances.

Currently, photon catalysis (PC) [21–24], which is a kind of non-Gaussian operations in essence, has been demonstrated to extend the transmission distance of the CVQKD system due to the fact that a suitable photon catalyzing operation would increase the entanglement degree of the entangled system and thereby increase the correlation between two output modes of the states [21]. Since the entanglement-based (EB) CVQKD is equivalent to the prepare-and-measure (PM) one, this operation can be implemented in practical protocols using coherent states with existing technologies. Motivated by the above advantages, in this paper, we propose an enhanced DM-CVQKD system through photon catalyzing for source preparation. The DM-CVQKD protocol is adopted as the fundamental communication protocol since it can well tolerate lower SNR, resulting in the long-distance transmission. Meanwhile, a zero-photon catalysis (ZPC) operation is deployed for the DM-involved source preparation at the transmitter, where it is not only used for splitting the incoming signal, but also improving the performance of the CVQKD system. The ZPC-based DM-CVQKD protocol has been proven to be beneficial for tolerating lower reconciliation efficiency and hence extending the maximal transmission distance, thus promoting its practical implementations with underlying technology.

As for the security analysis of the ZPC-based DM-CVQKD system, we consider the asymptotic case [17] and the finite-size regime [25,26]. In the asymptotic case, the secure key rate can be achieved with the covariance matrix of whole quantum system. However, it is a theoretically computed value that ignores the finite size effect of raw keys, and its upper bound cannot be achieved in realistic implementations. In order to solve this problem, the finite-size effects was taken into account [25]. Though the secure key rate is still pessimistic, but it approaches to the practice. It is the security enhancement based on uncertainty of the finite-size effect, and hence one can obtain the tightest bound of the maximal transmission distance, which is more practical than that obtained in asymptotic limit.

This paper is structured as follows. In Sec. 2, we propose the PC-involved DM source preparation for CVQKD, and then elaborate the characteristics of the ZPC-based scheme for performance improvement of the CVQKD system. In Sec. 3, we demonstrate the performance of the ZPC-based CVQKD system with numeric simulation and performance analysis. Finally conclusions are drawn in Sec. 4

2. The ZPC-involved DM source preparation for CVQKD

In this section, we elaborate the PC-involved DM source preparation form performance improvement of the CVQKD system. To make the derivation self-contained, we describe the DM-CVQKD protocol, and then proposed the PC-involved DM source preparation scheme.

2.1. The DM-CVQKD protocol

In the prepare and measure(PM) version of the CVQKD protocol that can be used in practice, Alice randomly draws n quaternary or octal variables, each corresponding to a coherent state of of $\left|\alpha_k^N\right\rangle = \left|\alpha e^{ik\pi/N}\right\rangle, k \in \{1, 2, \cdots, N\}$, where α is a real positive number related to the modulation variance of coherent state as $V_A = 2\alpha^2$. For example, we have the four-state scheme and the eight-state scheme in Fig. 1.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

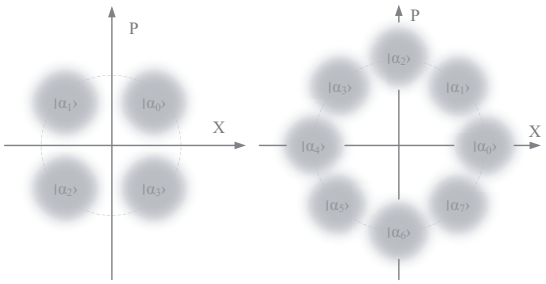


Figure 1. The DM source preparation for four states (left) and eight states (right).

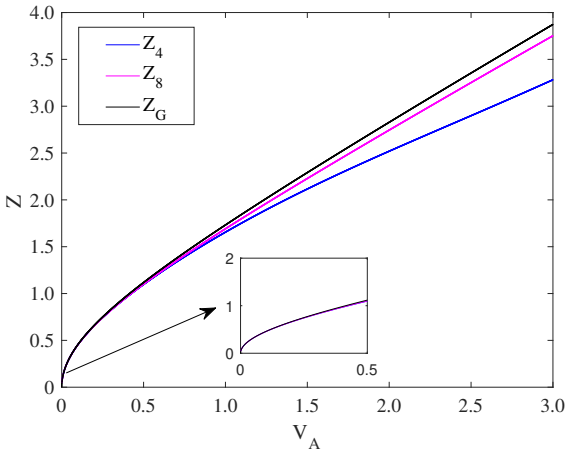


Figure 2. The correlation comparison of Z_4, Z_8 and Z_G.

Alice then prepares the n coherent states and sends them to Bob, which is characterized by its transmission T and excess noise ε. Then, for each state received, Bob measures arbitrary one of the two quadratures $\hat{x}$ or $\hat{p}$ by homodyne detector or both quadratures by heterodyne detector.

The security of the DM-CVQKD protocol is analyzed through using its entanglement-based(EB) version, which is equivalent to the PM version and is convenient for security analysis. In the EB version, Alice starts with a pure bipartite state $|\Psi\rangle$ with variance $V = V_A + 1$, and performs a projective measurement on the first half of this state. Subsequently, the second half is sent to Bob. For the DM-CVQKD protocol, to apply the same type of proof technique as the GM-CVQKD protocol, we therefore want to find a purification $|\Psi\rangle$ with a covariance matrix γ. This covariance matrix has the form given by

$$\gamma_N = \begin{pmatrix} (V_A+1)\mathbb{I} & Z_N\sigma_z \\ Z_N\sigma_z & (V_A+1)\mathbb{I} \end{pmatrix}, \tag{1}$$

where $\mathbb{I} = \mathrm{diag}(1,1)$ and $\sigma_z = \mathrm{diag}(1,-1)$. For example, taking $N = 4$ into account, we have the four-state scheme given by

$$Z_4 = V_A \sum_{k=0}^{3} \frac{\lambda_{k-1}^{3/2}}{\sqrt{\lambda_k}}, \tag{2}$$

where $\lambda_{0,2} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) \pm \cos(\alpha^2))$ and $\lambda_{1,3} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) \pm \sin(\alpha^2))$.

It should be noted that the DM source has a positive effect on the performance of the CVQKD system. For example, we have $Z_4 \leq Z_8 \leq Z_G$ for $N = 4$ and $N = 8$ in the DM-CVQKD protocol, where $Z_G = \sqrt{V_A^2 + 2V_A}$ represents the GM-CVQKD protocol. But it is still difficult to distinguish Z_4, Z_8 and Z_G for $V_A \leq 0.5$, as shown in Fig.2, due to the fact that the mutual information of the DM-CVQKD between Bob and Eve is similar to that of the GM-CVQKDl. Therefore, we attempt to get the security bounds of the DM-CVQKD referring to that of the GM-CVQKD.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

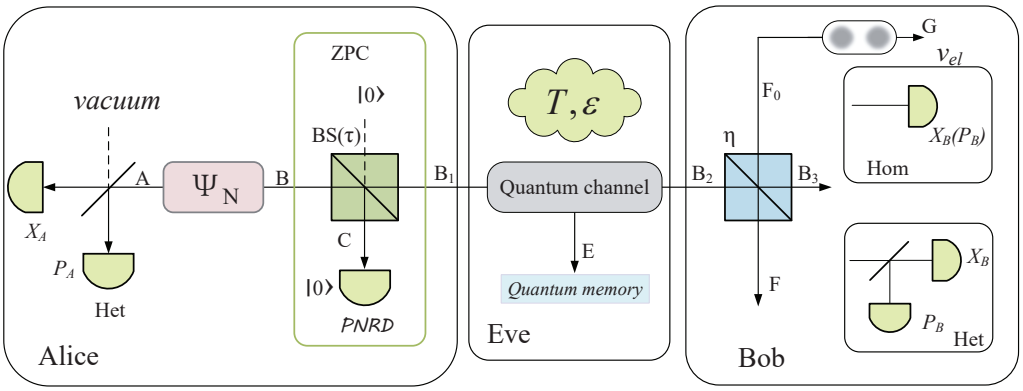


Figure 3. Schematic diagram of the ZPC-based DM-CVQKD protocol, where the green box represents zero-photon catalysis operation. Het: heterodyne detection, Hom: homodyne detection, $BS(\tau)$: beam splitter with transmittance τ, PNRD: photon number resolving detector, T: transmission effciency, ε: excess noise, η: detection efficiency, v_{el}: electronic noise.

2.2. The ZPC-involved DM source preparation

It is known that zero-photon catalysis(ZPC), which is actually seen as a noiseless attenuation, can enhance the performance of the practical quantum system [21]. In what follows, we suggest the ZPC-based CVQKD system, as shown in Fig. 3. In the auxiliary mode C, the zero-photon Fock state $|0\rangle$ is injected at one of the input ports of the beam splitter (BS) with transmittance τ, and quantum state $|\psi\rangle_{in}$ of the mode B is simultaneously injected at another input port of the BS. Subsequently, we detect the zero-photon Fock state $|0\rangle$ at one of the output ports of the BS by an ideal photon number resolving detector (PNRD), resulting in the ZPC-involved quantum state $|\psi\rangle_{out}$ from another output port.

Similar to the traditional photon subtraction operation [27–30], the ZPC-based source preparation can be used to promote the conversion of the target set, which can prevent the loss of information without photon subtraction. In order to describe the ZPC-based source preparation, the ZPC operation can be described as

$$\hat{O}_0 = \mathrm{Tr}[\mathrm{B}(\varnothing)\,|0\rangle\,\mathrm{C}\,\langle 0|] = (\sqrt{\varnothing})^{\mathrm{b}^\dagger \mathrm{b}}, \tag{3}$$

where $\mathrm{B}(\varnothing) = \hat{\mathrm{N}}\{\exp[(\sqrt{\varnothing}-1)(\mathrm{b}^\dagger\mathrm{b}+\mathrm{c}^\dagger\mathrm{c})+(\mathrm{c}^\dagger\mathrm{b}-\mathrm{c}\mathrm{b}^\dagger)(1-\sqrt{\varnothing})]\}$ and $\hat{\mathrm{N}}$ represents a normally ordering of operator [22]. Therefore, for an input state $|\psi\rangle_{in}$ in mode B, the output state $|\psi\rangle_{out}$ can be expressed as

$$|\psi\rangle_{out} = \frac{\hat{O}_0}{\sqrt{P_0}}\,|\psi\rangle_{in}\,, \tag{4}$$

where P_0 represents the success probability for achieving ZPC operation given by $P_0 = e^{(T-1)|\alpha_k|^2}$, as shown in Fig. 4. Note that we have $|\psi\rangle_{out} = |\psi\rangle_{in}$ for $\tau = 1$, indicating that there is no ZPC effect.

In the PM version of the ZPC-based DM-CVQKD system, Alice randomly draws n quaternary or octal variables, each corresponding to a coherent state of $|\alpha_k^N\rangle$. Subsequently, Alice performs the ZPC operation on these n coherent states, which is modeled (BS) with transmittance τ, resulting in the catalyzed state

$$|\tilde{\alpha}_k\rangle = \frac{e^{(\tau-1)|\alpha|^2}}{\sqrt{P_0}}\,|\sqrt{\tau}\alpha_k\rangle\,. \tag{5}$$

We note that the relationship of the quantum state amplitude change can be written as $\tilde{\alpha}_k = \sqrt{\tau}\alpha_k$. After that the catalyzed quantum state is transmitted to Bob via the Eve-controlled channel which is characterized by excess noise ε and transmission T. Bob can perform either homodyne or heterodyne detector on the received quantum state, to measure arbitrary one of the two quadratures $\hat{x}$ or $\hat{p}$ (or both quadratures), where Bob's detection efficiency is modeled by a BS with transmittance η and electronic

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

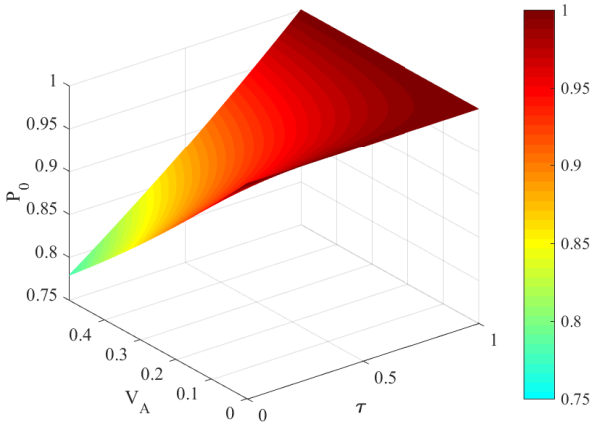


Figure 4. Success probabilities of ZPC with transmittances τ and modulation variance V_A.

noise v_{el} is introduced during this process. Finally, after conducting post-processing procedure, Bob shares the same key string with Alice.

In the EB version of the ZPC-based DM-CVQKD system, as shown in Fig. 3, Alice prepares the entangled state $|\Psi\rangle_N$, and performs heterodyne detection on the first half (mode A) of this state. The second half (mode B), which is performed with the ZPC operation, is sent to Bob through quantum channel controlled by Eve. The role of the ZPC operation is for source enhancement while promoting the mode transition between B and B_1, and hence the covariance matrix γ_{AB_1} of the catalyzed state ρ_{AB_1} can be derived as

$$\gamma_{AB_1} = \begin{pmatrix} (\tau V_A + 1)\mathbb{I} & Z'_N \sigma_z \\ Z'_N \sigma_z & (\tau V_A + 1)\mathbb{I} \end{pmatrix}, \tag{6}$$

with the parameters

$$Z'_N = \tau V_A \sum_{k=0}^{N-1} \frac{\tilde{\lambda}_{N-1}^{3/2}}{\sqrt{\tilde{\lambda}_k}}, \tag{7}$$

where the calculation of $\tilde{\lambda}_k$ is similar to that of λ_k in Eq.(2), but note that α is replaced by $\sqrt{\tau}\alpha$.

3. Security analysis

In this section, we show the effect of the ZPC-involved DM source preparation on the performance of CVQKD system in both asymptotic and finite-size cases with numeric simulation results. The detailed derivation of secret key rate is shown in Appendix A and Appendix B.

For the ZPC-involved DM source preparation, we demonstrate the success probability of ZPC operation as a function of transmittance τ and modulation variance V_A in Fig. 4. The success probability decreases with the increased modulation variance, whereas increases with the increased transmittance. In the security analysis, the transmittance τ can be optimized to ensure the optimality of the ZPC operation. As shown in Fig. 4, taking $V_A \leq 0.5$ into account, no matter what the value of V_A is, the success probability can remain more than 0.75, which indicates that it is a feasible solution to improve the performance of the CVQKD system by using the ZPC-involved DM source preparation.

As we know that an optimal modulation variance V_A is necessary for the DM source enhancement of the CVQKD system. As shown in Fig. 5, solid lines denote the performance of the ZPC-based eight-state CVQKD, while dashed lines represent the ZPC-based four-state CVQKD protocol, and their secret key rates change as V_A changes. The global simulation parameters are as follows: reconciliation efficiency is $\beta = 90\%$, quantum efficiency of Bob's detection is $\eta = 0.6$ and electronic noise is $v_{el} = 0.05$. We find that for the given $\varepsilon = 0.01$, as transmission distance is extended, the secret key rate is lowered, while the inserted subgraph shows that the secret key rate decreases with the increase of excess noise

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

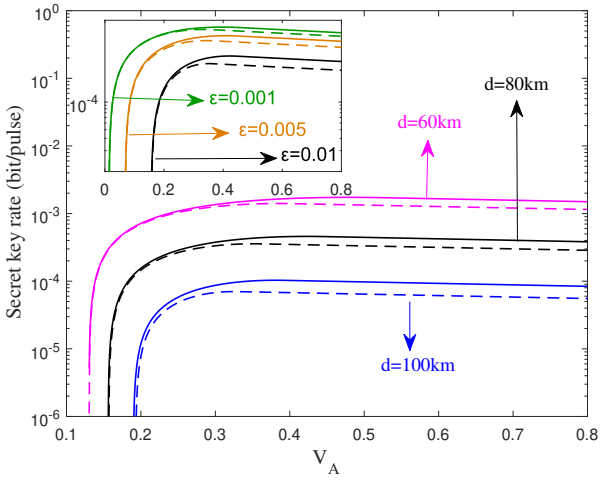
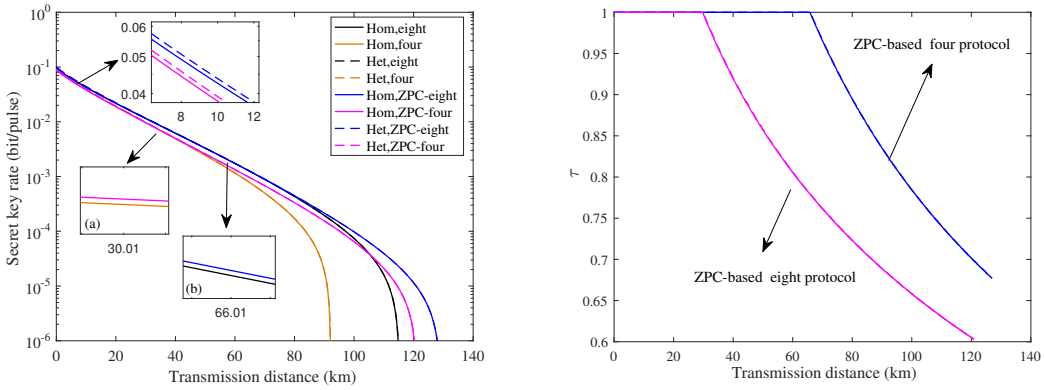


Figure 5. Asymptotic secret key rate as a function of modulation variance V_A in different transmission distance with $\varepsilon = 0.01$, where solid lines denote the performance of the ZPC-based eight-state CVQKD, while dashed lines represent the ZPC-based four-state CVQKD protocol.The inserted subgraph shows that asymptotic secret key rate as a function of modulation variance V_A in different excess noise with $L = 80km$.

ε for the given transmission distance 80km. Moreover all curves have a public interval including 0.5 where the secret key rate can reach the highest value. Therefore, in the subsequent numerical simulations, we take $V_A = 0.5$ into account.



(a) (b)

Figure 6. (a) Asymptotic secret key rate of the ZPC-based DM-CVQKD as a function of transmission distance with $\varepsilon = 0.01$, where solid lines denote homodyne detection, while dashed lines heterodyne detection. (b) Corresponding to (a), the transmittance τ varies with the transmission distance.

In Fig. 6(a), we show that asymptotic secret key rate of the ZPC-based DM-CVQKD system as a function of transmission distance, where solid lines denote homodyne detection, while dashed lines represent heterodyne detection. We find that the performances of homodyne detection and heterodyne detection are almost similar, and thus we employ homodyne detection for the security analysis. Moreover, the ZPC-based DM-CVQKD outperforms the original DM-CVQKD in terms of maximum transmission distance whether it is four-state or eight-state modulation. The eight-state modulation demonstrates better performance than the four-state modulation, but after performing the ZPC operation, the performance of the ZPC-involved four-state modulation exceeds the original eight-state modulation in terms of maximum transmission distance of the CVQKD system, which manifests that the ZPC-involved source preparation is an effective way to improve performance of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

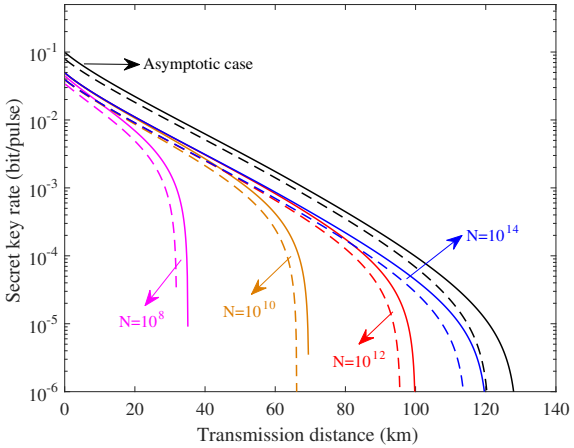


Figure 7. Finite-size secret key rate of the proposed ZPC-based DM-CVQKD scheme as a function of transmission distance with excess noise $\varepsilon = 0.01$, where the solid lines represent the ZPC-based eight-state modulation protocol, and the dotted lines represent the ZPC- based four-state modulation protocol.

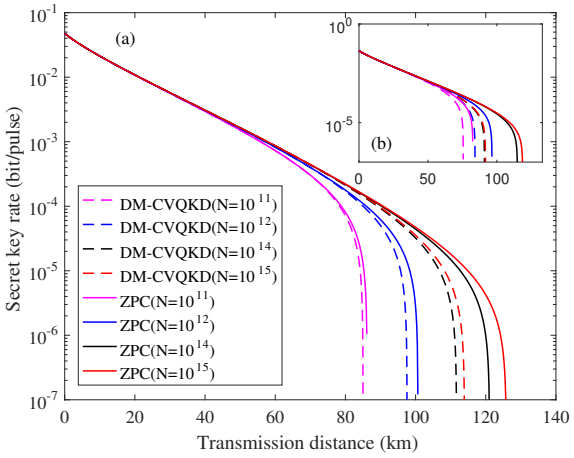


Figure 8. The secret key rate of the ZPC-based DM-CVQKD system with $\varepsilon = 0.01$ in the finite-size regime, where the (a) represents eight-state modulation, and inset (b) represents four-state modulation.

DM-CVQKD. We note that the effect of the ZPC operation does not work over the whole transmission distance. In the short distance range, there is few catalytic effect. For example, taking $\tau = 1$, the performance of the ZPC-based DM-CVQKD is almost the same as the original DM-CVQKD, as shown in Fig. 6(b). For the four-state DM source, the ZPC effect occurs at $L = 30km$, whereas for the eight-state DM source, it occurs at $L = 60km$.

Traditionally, in the asymptotic regime, one can make an assumption that quantum channel is perfectly known, before the transmission is even performed, while one actually does not know the characteristics of quantum channel in advance in finite-size scenario. Therefore, finite-size effect needs to be taken into consideration. As shown in Fig. 7, the performance of the ZPC-based DM-CVQKD system finite-size scenario is worse than that obtained in the asymptotic limit. As the number of exchanged signals N increases, the curves become closer to the curve of the asymptotic scenario. The reason is that the bigger number of exchanged signals is, the more signals parameter estimation can be used and hence the parameter estimation approaches to be perfection. However, it is impossible for number of exchanged signals to reach infinity in practice. But it still has a large improvement when comparing with the original DM-CVQKD system in the finite-size regime, as shown in Fig. 8. It can

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

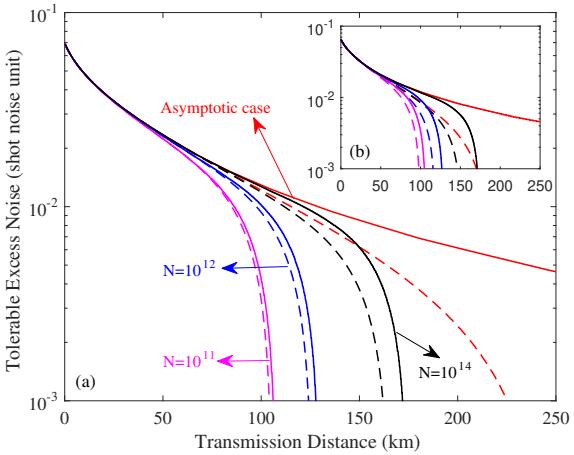


Figure 9. The maximal tolerable excess noise of the ZPC-based DM-CVQKD system (dotted lines and solid lines) as a function of the transmission distance for the original DM-CVQKD(dotted lines) and the ZPC-based DM-CVQKD(solid lines), where the (a) represents eight-state modulation, and inset (b) represents four-state modulation.

even partially compensate for the short transmission distance of the original DM-CVQKD caused by the small number of exchanged signals N.

In addition, we show the effect of the ZPC-involved DM source on the tolerable excess noise of the CVQKD system. As shown in Fig. 9, we illustrate the tolerable excess noise as a function of transmission distance for the optimalized T. We find that over a long distance, the performance of the ZPC-based DM-CVQKD system exceeds that of the original DM-CVQKD system in terms of maximum tolerable excess noise.

Moreover, it is known that reconciliation efficiency is an important factor affecting the secret key rate of the CVQKD system. In Fig. 10, we show the effect of the ZPC-involved source on the secret key rate of the DM-CVQKD system as a function of the reconciliation efficiency. We find that that ZPC-based DM-CVQKD system can tolerate lower reconciliation efficiency than the original DM-CVQKD protocol when the same secret key rate is achieved. Therefore, the ZPC-based DM-CVQKD system can reduce the requirements for reconciliation efficiency, thereby reducing costs for practical implementation of the high-rate long-distance metropolitan quantum communications.

4. Conclusion

We have proposed a ZPC-involved DM source preparation scheme for performance improvement of the CVQKD system in metropolitan areas. The photon catalysis operation, which is a non-Gaussian operation, has been deployed for the DM source preparation enhancement at the transmitter. We consider the effect of the ZPC-involved DM scheme, which is actually seen as a noiseless attenuation in essence and can be implemented with the-state-of-art experimental technologies. Security analysis shows that the ZPC-involved DM source preparation scheme can extend the maximal transmission distance of the CVQKD system. Moreover, numerical simulations show that the ZPC-based DM-CVQKD protocol can tolerate higher excess noise and tolerate lower reconciliation efficiency when achieving the same secret key rate, and thus outperforms the original DM-CVQKD protocols. Taking the finite-size effect into account we achieve the tightest bound of the maximal transmission distance, which is more practical than that obtained in asymptotic limit.

Author Contributions: Conceptualization,writing–original draft preparation, Z.Z. and Y.G.; software, S.Z; validation and formal analysis, T.H. and Y.M.; supervision, G.Y.;

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61972529, 61871407).

Conflicts of Interest: The authors declare no conflict of interest.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

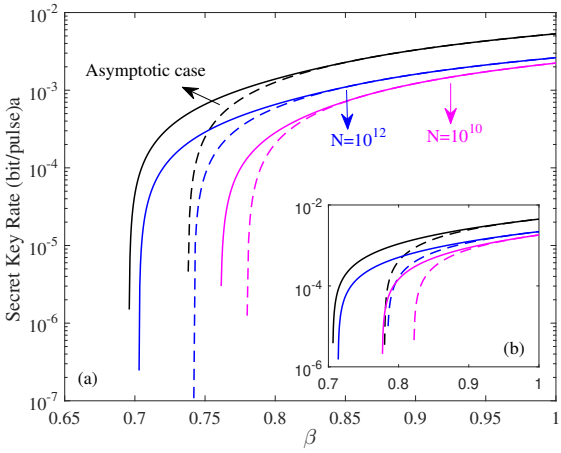


Figure 10. The secret key rate of the ZPC-based DM-CVQKD system as a function of the reconciliation efficiency with $L = 50km$ and $\varepsilon = 0.01$ for the original DM-CVQKD(dotted lines) and the ZPC-based DM-CVQKD(solid lines), where the (a) represents eight-state modulation, and inset (b) represents four-state modulation.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum Key Distribution
CVQKD	Continuous-variable Quantum Key Distribution
DVQKD	Discrete-variable Quantum Key Distribution
EPR	Einstein-Podolsky-Rosen
PP	Plug-and-paly
PS	Photon subtraction
EB	Entanglement-based
PM	Prepare-and-measurement
TMSV	Two-mode squeezed vacuum

Appendix A. Calculation of asymptotic secret key rate

We assume that Eve performs the Gaussian collective attack to achieve the useful results, and the information obtained is limited to the Holevo range $S(E:y)$. The definition of secret key rate in the case of reverse reconciliation under collective attacks can be given by

$$K_a = P_0(\beta I(x:y) - S(E:y)), \tag{A1}$$

where β is the reconciliation efficiency, $I(x:y)$ is the Shannon mutual information between Alice and Bob, and $S(E:y)$ is the Holevo bound of the mutual information between Eve and Bob. The mutual information $I(x:y)$ for homodyne detection is derived as

$$I(x:y) = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}}, \tag{A2}$$

where χ_{tot} represents the total noise given by $\chi_{tot} = \chi_{line} + \chi_{hom(het)}/T$ and χ_{line} represents the total channel-added noise given by $\chi_{line} = 1/T + \varepsilon - 1$. The transmission efficiency T is calculated as $T = 10^{-\mu L/10}$, where $\mu = 0.2$ dB/km is the loss coefficient for the standard optical fibers and L is the length of the fiber optics. For homodyne detection, the detection-added noise referred to Bob's input can be given by

$$\chi_{hom} = \frac{(1-\eta) + v_{el}}{\eta}. \tag{A3}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

Note that in the case of heterodyne detection, we have,

$$\chi_{het} = \frac{1 + (1-\eta) + 2\nu_{el}}{\eta}. \tag{A4}$$

After Bob applies homodyne or heterodyne measurement, Eve purifies the whole system so that the mutual information between Eve and Bob can be expressed as

$$\begin{aligned} S_(E:y) &= S(E) - S(E|y) \\ &= S(xy) - S(x|y), \end{aligned} \tag{A5}$$

where the first term $S(xy)$ is a function of the symplectic eigenvalues $\lambda_{1,2}$ of γ_{AB_2} , which is given by

$$S(xy) = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right), \tag{A6}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$ and $\lambda_{1,2}$ are symplectic eigenvalues of covariance matrix

$$\gamma_{AB_2} = \begin{bmatrix} (\tau V_A + 1)\mathbb{I} & \sqrt{T}Z'_N\sigma_z \\ \sqrt{T}Z'_N\sigma_z & T(\tau V_A + 1 + \chi_{line})\mathbb{I} \end{bmatrix}. \tag{A7}$$

Consequently, we have

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left(A \pm \sqrt{A^2 - 4B}\right)}, \tag{A8}$$

where A and B are parameters given by

$$A = \text{detfl}_\text{A} + \text{detfl}_{\text{B}_2} + 2\text{detœ}_{\text{AB}_2}, \text{B} = \text{detfl}_{\text{AB}_2}. \tag{A9}$$

The second term $S(x|y)$ is a function of the symplectic eigenvalues $\lambda_{3,4}$ of the convariance matrix of Alice's mode after Bob performs homodyne(heterodyne) detection, which is given by

$$S(x|y) = G\left(\frac{\lambda_3 - 1}{2}\right) + G\left(\frac{\lambda_4 - 1}{2}\right), \tag{A10}$$

with the symplectic eigenvalues

$$\lambda_{3,4} = \sqrt{\frac{1}{2}\left(C \pm \sqrt{C^2 - 4D}\right)}. \tag{A11}$$

For homodyne detection, we have

$$\begin{aligned} C_{hom} &= \frac{A\chi_{hom} + V\sqrt{B} + T'}{T(V + \chi_{tot})}, \\ D_{hom} &= \sqrt{B}\frac{V + \sqrt{B}\chi_{hom}}{T(V + \chi_{tot})}, \end{aligned} \tag{A12}$$

with $T' = T(V + \chi_{line})$. For heterodyne detection, we have

$$\begin{aligned} C_{het} &= \frac{A\chi_{het}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T') + 2TZ_8^2}{T^2(V + \chi_{tot})^2}, \\ D_{het} &= \left(\frac{V + \sqrt{B}\chi_{het}}{T(V + \chi_{tot})}\right)^2. \end{aligned} \tag{A13}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2020 doi:10.20944/preprints202009.0224.v1

Appendix B. Secret key rate in the finite-size scenario

In the following, let the notation N represent the total number of signals exchanged by Alice and Bob during the protocol. The x and y represent the classical data of Alice and Bob after they have measured their quantum states, and E refers to the quantum state of the eavesdropper. In the case of the CVQKD system, the secret key rate obtained for a finite size analysis can be given by

$$K_f = \frac{n}{N}\left(\beta I(x:y) - S_{\epsilon_{PE}}(y:E) - \Delta(n)\right), \tag{A14}$$

where $\frac{n}{N}$ represents n signals are used for the establishment of the key, out of the N signals exchanged. The notation $S_{\epsilon_{PE}}(y:E)$ is defined as the maximum of the Holevo information compatible with the statistics except with probability ϵ_{PE}, where ϵ_{PE} is the failure probability of parameter estimation. The parameter $\Delta(n)$ is related to the security of the privacy amplification given by

$$\Delta(n) = (2\mathrm{dim}\mathrm{H_y} + 3)\sqrt{\frac{\log_2(2/\bar{\mathrm{ffl}})}{\mathrm{n}}} + \frac{2}{\mathrm{n}}\log_2(1/\mathrm{ffl_{PA}}), \tag{A15}$$

where $\mathcal{H}_Y$ is the Hilbert space corresponding to the variable y used in the raw key. Since the raw key is usually encoded on binary bits, we have $\mathrm{dimH_y} = 2$. In addition, $\bar{\epsilon}$ is a smoothing parameter, and ϵ_{PA} is the failure probability of the privacy amplification procedure. Both the smoothing parameter $\bar{\epsilon}$ and ϵ_{PA} are intermediate parameters which should be optimized numerically. One needs to fix an overall security parameter ϵ for the performance analysis of the CVQKD system. Compared with the unconditional security in the case of asymptotic scenario, the CVQKD system is limited to ϵ-security in a finite-size setting. The parameter ϵ corresponds to the failure probability of the whole protocol, meaning that the protocol is assured to performed as it is supposed to except with a probability at most ϵ. The failure probability ϵ can be computed from the various parameters as follows

$$\epsilon = \epsilon_{PE} + \epsilon_{EC} + \bar{\epsilon} + \epsilon_{PA}, \tag{A16}$$

where ϵ_{EC} is the probability that the reconciliation fails. The above-mentioned error probabilities can be set to $\epsilon \approx \epsilon_{PE} = \epsilon_{EC} = \bar{\epsilon} = \epsilon_{PA} = 10^{-10}$.

In the finite-size scenario, $S_{\epsilon_{PE}}(y:E)$ needs to be calculated in parameter estimation procedure where one can find a covariance matrix $\gamma_{AB_{2_{\epsilon_{PE}}}}$, which minimizes the secret key rate with a probability of at least $1-\epsilon_{PE}$. The estimation of $\gamma_{AB_{2_{\epsilon_{PE}}}}$ can be calculated by $m = N - n$ couples of correlated variables $(x_i, y_i)_{i=1,\cdots,m}$ in the following form

$$\gamma_{AB_1\epsilon_{PE}} = \begin{bmatrix} (\tau V_A + 1)\mathbb{I} & t_{min} Z'_N \sigma_z \\ t_{min} Z'_N \sigma_z & (t_{min}^2 \tau V_A + \sigma_{max}^2)\mathbb{I} \end{bmatrix}, \tag{A17}$$

where t_{min} and σ_{max}^2 correspond respectively to the minimal value of t and the maximal value of σ^2 compatible with the sampled data, except with probability $\epsilon_{PE}/2$. With the maximum-likelihood estimators, we have

$$\begin{aligned} t_{min} &\approx \sqrt{T} - z_{\epsilon_{PE}/2}\sqrt{\frac{1+T\varepsilon}{mV_A}}, \\ \sigma_{max}^2 &\approx 1 + T\varepsilon + z_{\epsilon_{PE}/2}\frac{(1+T\varepsilon)\sqrt{2}}{\sqrt{m}}, \end{aligned} \tag{A18}$$

where $z_{\epsilon_{PE}/2}$ is such that $1 - \mathrm{erf}(\mathrm{z_{ffl_{PE}}}/\sqrt{2}) = \mathrm{ffl_{PE}}/2$ and erf is the error function given by

$$erf(x) = \frac{2}{\sqrt{\pi}}\int_0^x e^{-t^2}\, dt. \tag{A19}$$

References

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. C. Weedbrook, S. Pirandola, R. García-Patrón, N .J .Cerf, T .C .Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys, **84**(2), 621 (2012).
3. Law, and Jim, Acm Sigsoft Software Engineering Notes, **26**(4), 91 (2001).
4. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys, **81**(3), 1301 (2009).
5. H. K. Lo, M. Curty, and K. Tamaki, Nat. Photon, **8**(8), 595 (2014).
6. W. K. Wootters, and W. H. Zurek, Nature, **299**(5886), 802(1982).
7. J. Y. Bang, and M. S. Berger, Phys. Rev. D, **74**(12), 125012 (2006).
8. P. W. Shor, and J. Preskill, Phys. Rev. Lett, **85**(2), 441 (2000).
9. H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett, **108**(13), 130503 (2012).
10. D. B. S. Soh, C. Brif, P. J Coles, N. Lutkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X, **5**(4), 041010(2015).
11. F. Grosshans, and P. Grangier, Phys. Rev. Lett, **88**, 057902 (2002).
12. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature, **421**(6920), 238 (2003).
13. F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, and H. Hübel, Advanced Quantum Technologies, **1**(1), 1800011 (2018).
14. S. L. Braunstein, and P. Van Loock, Rev. Mod. phys, **77**(2), 513 (2005).
15. X. C. Ma, S. H. Sun, M. S. Jiang, M. Gui, and L. M. Liang, Phys. Rev. A, **89**(4), 0423359(2014).
16. A. Leverrier, and P. Grangier, Phys. Rev. Lett, **102**(18), 180504 (2009).
17. A. Leverrier, and P. Grangier, arXiv: Quantum Physics (2010).
18. A. Becir, F. A. A. El-Orany, and M. R. B. Wahiddin, Int. J. Quantum. Inf, **10**(01), 1250004 (2012).
19. A. Leverrier, and P. Grangier, Phys. Rev. A, **83**(4), 042312 (2011).
20. H. Zhang, G. Q. He, and J. Fang, Phys. Rev. A, **86**(2), 022338 (2012).
21. Y. Guo, W. Ye, H. Zhong, and Q. Liao, Phys. Rev. A, **99**(3), 032327 (2019).
22. W. Ye, H. Zhong, Q. Liao, D. Huang, L. Hu, and Y. Guo, Opt. Express, **27**(12), 17186-17198 (2019).
23. Y. Guo, J. Z. Ding, Y. Mao, W. Ye, Q. Liao, and D. Huang, Phys. Lett. A **384**(12), 126340 (2020).
24. W. Ye, H. Zhong, X. D. Wu, L. Y. Hu, and Y. Guo, arXiv: Quantum Physics (2019).
25. A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A, **81**(6), 062343 (2010).
26. Y. Guo, R. J. Li, Q. Liao, J. Zhou, and D. Huang, Phys. Lett. A, **382**(6), 372-381 (2018).
27. Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, and H. Guo, Phys. Rev. A, **93**(1), 012310 (2016).
28. P. Huang, G. He, J. Fang, and G. Zeng, Phys. Rev. A, **87**(1), 012317 (2013).
29. Y. Guo, Q. Liao, Y. Wang, D. Huang, P. Huang, and G. Zeng, Phys. Rev. A, **95**(3), 032304 (2017).
30. Q. Liao,Y. Guo, D. Huang, P. Huang, and G. Zeng, New. J. Phys, **20**(2), 023015 (2018).