Article

Lengthening Transmission Distance of Continuous Variable Quantum Key Distribution with Discrete Modulation through Photon Catalyzing

Zhengchun Zhou ^{1,†}, Shanhua Zou ^{1,2,*,†}, Tongcheng Huang ^{1,*} and Ying Guo ^{3,*} ¹ College of Information Engineering, Shaoyang University, Shaoyang 422000, China; 20156@hnsyu.edu.cn² Jiangsu Key Construction Laboratory of IoT Application Technology, Taihu University, Wuxi 214064, China³ School of Automation, Central South University, Changsha 410083, China

* Correspondence: 000037@wxu.edu.cn (S.Z.); 2587@hnsyu.edu.cn (T.H.); yingguo@csu.edu.cn (Y.G.)

† These authors contributed equally to this work.

Received: 18 September 2020; Accepted: 26 October 2020; Published: 3 November 2020

Abstract: Establishing global secure networks is a potential implementation of continuous-variable quantum key distribution (CVQKD) but it is also challenged with respect to long-distance transmission. The discrete modulation (DM) can make up for the shortage of transmission distance in that it 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 improving the transmission distance. We address a zero-photon-catalysis (ZPC)-based source preparation for enhancing the DM-CVQKD system. The statistical fluctuation is taken into account for the practical security analysis. Numerical simulations show that the ZPC-based source preparation can not only achieve the long-distance transmission, but also contributes to the reasonable increase of the secret key rate.

Keywords: continuous-variable; quantum key distribution; non-gaussian operation; quantum communications

1. Introduction

Quantum key distribution (QKD) [1–4] allows legal participants to share a secret key and enables theoretically information-secure communications [5–7]. Recently, it has spurred much interest, resulting in two 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 practically implemented with modern telecommunications, thus allowing for the exploitation of the heritage of integrability in existing optical communication system.

At present, there are several mainstream modulations in CVQKD, such as Gaussian modulation (GM) [11–15] and discrete modulation (DM) [16–20]. In the former, the transmitter generates the key bits in the quadratures of the Gaussian modulated optical field, while the receiver recovers the secret key using a coherent detector [13]. It is GM-CVQKD that could achieve the potential high secret key rate. Unfortunately, it is still limited to the transmission distance, compared with its DVQKD counterpart. A challenge is that the resulting reconciliation efficiency [14,15] is still low, which is unsuitable for long-distance transmission, whereas in the latter, one can solve this problem by using a DM source for CVQKD [16], where it generates nonorthogonal coherent states, taking advantage of the randomly measured quadrature for information encoding rather than exploiting the fixed quadrature in source preparation [17]. Consequently, it results in a merit of both high reconciliation efficiency and high tolerance against the excess noise [11–15] such that it can extend the transmission distance of the CVQKD

system [18]. Actually, GM-CVQKD is simpler for theoretical performance analysis than DM-CVQKD, and the secret key rates can approach the theoretical limits [17], whereas GM-CVQKD itself is always approximated by the DM sources, which may be taken into account for security analysis [18]. Moreover, as GM-CVQKD usually requires more resources in terms of randomness and classical post-processing resources, DM-CVQKD can offer further simplified implementation in experiments. While theoretics and experiments of DM-CVQKD have suggested that we can achieve the above-mentioned goal, there are still some potential challenges while promoting its performances.

Currently, photon catalysis (PC) [21–25], which is a non-Gaussian operation with n -photon state input/output in essence, has been utilized for security improvement attributed to the photon catalyzing operation, which increases the entanglement degree of the two-participant system by increasing the correlation between the transmitter and the receiver [21]. In a certain low-squeezing parameter, the entanglement of the two-mode squeezed vacuum (TMSV) state can be enhanced by increasing the catalysis photon number [22]. Due to equivalence of the entanglement-based (EB) CVQKD system and the prepare-and-measure (PM) CVQKD system [11–20], the PC-involved DM-CVQKD system may be implemented with existing optical technologies. Motivated by the above advantages, we propose an improved DM-CVQKD system through photon catalyzing. The DM scheme is employed for the source preparation because it can tolerate a lower signal-to-noise ratio (SNR) well, resulting in the long-distance transmission of the CVQKD system. Meanwhile, a zero-photon catalysis (ZPC) operation with zero-photon state input/output is adopted in the DM-involved source preparation at the transmitter. The ZPC-based CVQKD protocol has been proven to be beneficial for tolerating lower reconciliation efficiency [24,25] and extending the maximal transmission distance, thus promoting its practical implementations with underlying technology.

As for the performance analysis of the proposed DM-CVQKD system, we take into account the asymptotic case [17] where the secure key rate can be obtained via the covariance matrix approach. It is a theoretically calculated value without involving the finite-size effect. Unfortunately, the derived upper bound is difficult to obtain in practical implementations. Therefore, we have to consider the finite-size effects [26,27]. Though the secure key rate is still pessimistic, it approaches to the practical implementation. Its security analysis is based on the finite-size effects; hence, we can achieve the upper bound of the maximal transmission distance.

This paper is structured as follows. In Section 2, we propose the PC-based DM source for CVQKD, and then elaborate on the characteristics of the ZPC-based scheme for improving the DM-CVQKD system. In Section 3, we demonstrate the transmission distance improvement of the DM-CVQKD system via the ZPC-based source preparation scheme. Finally, we draw a conclusion in Section 4.

2. The DM Source Preparation via ZPC Operations

In what follows, we elaborate the ZPC-involved DM source preparation for performance improvement of the CVQKD system. To make the derivation self-contained, we suggest the ZPC-involved CVQKD system with the DM source preparation.

2.1. The CVQKD System with the DM Source Preparation

For the prepare-and-measure (PM) version of CVQKD that can be used for practical implementations, Alice randomly draws n quaternary or octal variables, each corresponding to a coherent state of $|\alpha_k^N\rangle = |\alpha e^{ik\pi/N}\rangle$, $\forall k \in \{1, 2, \dots, N\}$, where α is a real positive number related to the modulation variance of coherent state given by $V_A = 2\alpha^2$ [16–20]. For $N = 4$ and $N = 8$, we have the four-state DM source and the eight-state DM source, as shown in Figure 1 [28,29].

Alice generates n coherent states, which are sent through quantum channel characterized by transmission T and excess noise ε . Then, for the received state, Bob measures one of quadratures (i.e., $\hat{x}$ or $\hat{p}$) by homodyne detector.

Theoretical analysis of CVQKD is considered through using its equivalent entanglement-based (EB) version. The transmitter Alice starts with a pure bipartite state $|\Psi\rangle$ with variance $V = V_A + 1$.

Subsequently, she performs a projective measurement on the first half of this state, whereas the second half is sent to the receiver Bob. For the DM–CVQKD protocol, to apply the security analysis technique as the GM–CVQKD protocol [11–15], we therefore want to find a purification $|\Psi\rangle$ with a covariance matrix γ . This covariance matrix has the form given by [26,27]

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

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

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

with the parameters $\lambda_{0,2}$ and $\lambda_{1,3}$ given by $\lambda_{0,2} = \frac{1}{2}e^{-\alpha^2}(\cosh(\alpha^2) \pm \cos(\alpha^2))$ and $\lambda_{1,3} = \frac{1}{2}e^{-\alpha^2}(\sinh(\alpha^2) \pm \sin(\alpha^2))$ [24].

Figure 1. The discrete-modulation (DM)-based sources for four states (**left**) and eight states (**right**).

We note that the DM source has a positive effect on CVQKD. 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. However, it is difficult to distinguish Z_4 , Z_8 and Z_G for $V_A \leq 0.5$, as shown in Figure 2. Therefore, we attempt to derive the security bounds of DM–CVQKD referring to that of GM–CVQKD.

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

2.2. The ZPC-Based DM Source Preparation

It is known that ZPC, which is a non-Gaussian operation with zero-photon state input/output [21,22], can enhance the correlation of the two-participant entangled quantum system [25,28]. In what follows,

we suggest an improved CVQKD system with ZPC operation for the DM source preparation, as shown in Figure 3. In the auxiliary mode C, the zero-photon Fock state $|0\rangle$ is injected at one input port of beam splitter (BS) with transmittance τ , and quantum state $|\psi\rangle_{in}$ of the mode B is simultaneously injected at another input port. Subsequently, we detect the zero-photon Fock state $|0\rangle$ at one of the output ports of the BS using a photon number resolving detector (PNRD), resulting in the ZPC-enhanced quantum state $|\psi\rangle_{out}$ from another output port.

Figure 3. Schematic diagram of continuous-variable quantum key distribution (CVQKD) with zero-photon-catalysis (ZPC)-based DM source preparation.

Similar to the traditional photon subtraction operation [30–33], the ZPC operation can be used for performance improvement of CVQKD. In order to describe the ZPC-based DM source preparation, the ZPC operation can be described as [22,25]

$$\hat{O}_0 = (\sqrt{\tau})^{b^\dagger b}. \quad (3)$$

For an input $|\psi\rangle_{in}$, we have output $|\psi\rangle_{out}$ given by

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

where P_0 denotes the success probability of the operation given by $P_0 = e^{-(T-1)|\alpha_k|^2}$ as function of parameters V_A and τ , as shown in Figure 4. We find that the large V_A and τ result in the high success probability. Note that we have $|\psi\rangle_{out} = |\psi\rangle_{in}$ for $\tau = 1$, indicating that there is no ZPC effect.

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

In the PM version of CVQKD, 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

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

We note that the relationship of the transformed amplitudes can be written as $\tilde{\alpha}_k = \sqrt{\tau}\alpha_k$. After that, the catalyzed quantum state is sent to Bob through the Eve-controlled channel. Bob may perform either homodyne (Hom) or heterodyne (Het) detection on the resulting quantum state. Finally, Alice and Bob distill the shared secret key after they conduct the classical post-processing procedure. In the EB version of the CVQKD system, as shown in Figure 3, Alice prepares for $|\Psi\rangle_N$, and performs heterodyne detection (Het) on mode A. Mode B, which is performed with the ZPC operation, is sent to Bob. The role of the ZPC operation is for source-entanglement enhancement while promoting the mode transition between B and B_1 , resulting in the covariance matrix γ_{AB_1} of the catalyzed state ρ_{AB_1} given by

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

with the parameters

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

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

We note that we can obtain the effect of the ZPC operation on the DM source from the derived covariance matrix γ_{AB_1} . The parameter Z'_N , which can be calculated from modulation variances of the initially prepared coherent states, demonstrates the relation of the modes A and B_1 for source preparation. In what follows, we will show the effect of Z'_N on the performance of the CVQKD system.

In addition, there are the other similar operations, such as local Gaussian operation [34], photon subtraction and addition operations [35], which can be used for improving entanglement of a two-mode state. These operations, whether they are Gaussian or not, may be similarly employed for source preparation while considering performance improvement of the CVQKD system. However, due to the elegant structure of the ZPC operation that can be conventionally integrated with the practical quantum system, in this paper, we consider the ZPC-based DM source preparation for extending the maximal transmission distance of the CVQKD system.

3. Security Analysis

In this section, we demonstrate the effect of the DM source preparation on CVQKD in both asymptotic [32,33] and finite-size cases [33] with numeric simulation results. For the detailed derivation of the secret key rate of the CVQKD system in asymptotic and finite-size cases, please see Appendices A and B, respectively.

For the ZPC-based DM source preparation, we show the success probability of ZPC operation in Figure 4. We find that the success probability increases with the increased modulation variance, and simultaneously increases with the increased transmittance. In the security analysis, the transmittance τ is tunable to satisfy the optimality of the ZPC operation. 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. This is a feasible solution to improve the CVQKD system.

As usual, it is necessary to select an optimal modulation variance V_A for the performance improvement of CVQKD involving the ZPC operation. As shown in Figure 5, solid lines denote the secret key rate of the eight state CVQKD system, while dashed lines represent that of the four-state CVQKD system. In addition, we let $\beta = 90\%$, $\eta = 0.6$ and $v_{el} = 0.05$. We find that for $\varepsilon = 0.01$, the secret key rate

decreases as the transmission distance, while the inserted subgraph shows that the secret key rate decreases with the excess noise at the distance of 80km. Moreover, for $V_A = 0.5$ the secret key rate can reach the optimal value, and hence we let $V_A = 0.5$ in the subsequent simulations.

Figure 5. Asymptotic secret key rate of the CVQKD system with the ZPC-based DM source preparation for $\epsilon = 0.01$, where solid lines denote the eight-state DM source preparation, while dashed lines represent the four-state DM source preparation. The inserted subgraph shows that asymptotic secret key rate of the CVQKD system for $L = 80$ km.

In Figure 6a, we show the asymptotic secret key rate of the ZPC-based CVQKD system, where solid lines denote homodyne detection and dashed lines represent heterodyne detection. It seems that performances of homodyne and heterodyne detectors are almost similar, and thus we employ the homodyne detector in security analysis. The performance of the ZPC-based CVQKD is better than that of the traditional CVQKD whether it is four-state modulation or not.

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

The eight-state modulation scheme demonstrates better performance than the four-state modulation scheme in the traditional CVQKD system. However, after performing the ZPC operation, the performance of the ZPC-based four-state modulation scheme exceeds the eight-state modulation scheme. Therefore, the ZPC-based source preparation is an effective way to improve the DM-CVQKD system. We note

that the effect of the ZPC operation does not work over the whole transmission distance. In the short distance range, there are few catalytic effects. As shown in Figure 6b, the performance of the ZPC-based system is almost similar to that of the traditional system for $\tau = 1$. For the four-state DM source preparation, the ZPC effect occurs at the distance of $L = 60$ km, whereas for the eight-state DM source preparation, it occurs at $L = 30$ km.

Usually, one assumes that the quantum channel is given in an asymptotic regime. However, one does not know the quantum channel in advance in the finite-size scenario. Therefore, we take into account effect of the finite-size on the ZPC-based CVQKD. As shown in Figure 7, the proposed CVQKD system in finite-size scenario performs worse than that in the asymptotic limit. As the number N of the exchanged signals is increased, the corresponding curves approach to the asymptotic scenario. The reason is that the large number of the exchanged signals results in the perfect signals parameter estimation. However, it is infeasible to achieve the infinite number of the exchanged signals in practice. Nonetheless, it still has resulted in an improvement, compared with the traditional system in the finite-size regime, as shown in Figure 8.

Figure 7. Finite-size key rate of CVQKD involving the ZPC operation for $\varepsilon = 0.01$, where solid lines represent the eight-state DM source preparation and dotted lines represent the four-state DM source preparation, respectively.

Figure 8. Finite-size key rate of CVQKD involving the ZPC operation for $\varepsilon = 0.01$, where the (a) represents eight-state DM source preparation, and inset (b) represents four-state DM source preparation.

In addition, we show the effect of the ZPC-involved source on the tolerable excess noise of CVQKD, as shown in Figure 9. We find that CVQKD involving the ZPC-involved source performs better than the traditional system in terms of maximal transmission distance.

Figure 9. The maximal tolerable excess noise of CVQKD involving the ZPC operation (dotted lines and solid lines) for the traditional CVQKD (dotted lines) and the ZPC-based CVQKD (solid lines), where (a) represents eight-state DM source preparation, and inset (b) represents four-state DM source preparation.

Moreover, reconciliation efficiency is the other important parameter that has an effect on the performance of CVQKD. Figure 10 suggests the effect of the ZPC-based source on the secret key rate of CVQKD related to the reconciliation efficiency. We find that the ZPC-based source can tolerate low reconciliation efficiency. Therefore, the ZPC-based source preparation can reduce the requirements for reconciliation efficiency, thereby reducing costs of practical implementation of the high-rate long-distance quantum communications.

Figure 10. The secret key rate of the CVQKD system involving the ZPC operation with $L = 50$ km and $\varepsilon = 0.01$ for the traditional CVQKD system (dotted lines) and the ZPC-based CVQKD system (solid lines), where (a) represents eight-state DM source preparation, and inset (b) represents four-state DM source preparation.

4. Conclusions

We have suggested a ZPC-based source preparation scheme for improving the DM-CVQKD system in metropolitan areas. The PC operation, which is non-Gaussian, has been deployed for the source preparation at the transmitter. We consider the effect of the ZPC-based DM source on the performance of CVQKD. Numerical simulations show that the ZPC-involved DM source can extend the maximal transmission distance of the CVQKD system. Moreover, it can tolerate high excess noise and low reconciliation efficiency, compared with the traditional CVQKD system. Taking the finite-size effect into account, we obtain the tight bound of the maximal transmission distance, which can be experimentally achieved with state-of-the-art technologies.

Author Contributions: Writing—original draft preparation, Z.Z. and Y.G.; software, S.Z.; validation and formal analysis, T.H.; supervision, Y.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant No. 61871407).

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

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

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

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

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

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

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

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

$$\chi_{het} = \frac{1 + (1 - \eta) + 2v_{el}}{\eta}. \quad (\text{A4})$$

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

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

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

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

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

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

Consequently, we have

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

where A and B are parameters given by

$$A = \text{detfl}_A + \text{detfl}_{B_2} + 2\text{det}\epsilon_{AB_2}, B = \text{detfl}_{AB_2}. \quad (A9)$$

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

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

with the symplectic eigenvalues

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

For homodyne detection, we have

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

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

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

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

$$K_f = \frac{n}{N} (\beta I(x : y) - S_{e_{PE}}(y : E) - \Delta(n)), \quad (A14)$$

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

$$\Delta(n) = (2\text{dim}H_y + 3) \sqrt{\frac{\log_2(2/\bar{e})}{n}} + \frac{2}{n} \log_2(1/e_{PA}), \quad (A15)$$

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 $\dim \mathcal{H}_y = 2$. In addition, $\bar{e}$ is a smoothing parameter, and e_{PA} is the failure probability of the privacy amplification procedure. Both the smoothing parameter $\bar{e}$ and e_{PA} are intermediate parameters which should be optimized numerically. One needs to fix an overall security parameter e 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 e -security in a finite-size setting. The parameter e corresponds to the failure probability of the whole protocol, meaning that the protocol is assured to be performed as it is supposed to except with a probability at most e . The failure probability e can be computed from the various parameters as follows

$$e = e_{PE} + e_{EC} + \bar{e} + e_{PA}, \quad (\text{A16})$$

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

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

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

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

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

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

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

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [\[CrossRef\]](#)
2. Zhou, J.; Huang, D.; Guo, Y. Long-distance continuous-variable quantum key distribution using separable Gaussian states. *Phys. Rev. A* **2018**, *98*, 042303. [\[CrossRef\]](#)
3. Guo, Y.; Xie, C.; Huang, P.; Li, J.; Zhang, L.; Huang, D.; Zeng, G. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [\[CrossRef\]](#)
4. Liao, Q.; Wang, Y.; Huang, D.; Guo, Y. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. *Opt. Express* **2018**, *26*, 19907–19920. [\[CrossRef\]](#)
5. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photon* **2014**, *8*, 595. [\[CrossRef\]](#)
6. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802. [\[CrossRef\]](#)
7. Bang, J.Y.; Berger, M.S. Quantum mechanics and the generalized uncertainty principle. *Phys. Rev. D* **2006**, *74*, 125012. [\[CrossRef\]](#)
8. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [\[CrossRef\]](#)

9. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [\[CrossRef\]](#)
10. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lutkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* **2015**, *5*, 041010. [\[CrossRef\]](#)
11. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [\[CrossRef\]](#)
12. Grosshans, F.; van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238. [\[CrossRef\]](#)
13. Liao, Q.; Guo, Y.; Huang, D.; Huang, P.; Zeng, G. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection. *New J. Phys.* **2018**, 023015. [\[CrossRef\]](#)
14. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [\[CrossRef\]](#)
15. Ma, X.C.; Sun, S.H.; Jiang, M.S.; Gui, M.; Liang, L.M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 042335. [\[CrossRef\]](#)
16. Leverrier, A.; Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **2009**, *102*, 180504. [\[CrossRef\]](#)
17. Takeoka, M.; Guha, S.; Wilde, M.M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **2014**, *5*, 5235. [\[CrossRef\]](#)
18. Furrer, F.; Franz, T.; Berta, M.; Leverrier, A.; Scholz, V.B.; Tomamichel, M.; Werner, R.F. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **2012**, *109*, 100502. [\[CrossRef\]](#)
19. Leverrier, A.; Grangier, P. Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. *Phys. Rev. A* **2011**, *83*, 042312. [\[CrossRef\]](#)
20. Mao, Y.; Wang, Y.; Huang, W.; Zhong, H.; Qin, H.; Guo, Y.; Huang, D. Detecting quantum attacks: a machine learning based defense strategy for practical continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083073. [\[CrossRef\]](#)
21. Guo, Y.; Ye, W.; Zhong, H.; Liao, Q. Continuous-variable quantum key distribution with non-Gaussian quantum catalysis. *Phys. Rev. A* **2019**, *99*, 032327. [\[CrossRef\]](#)
22. Ye, W.; Zhong, H.; Liao, Q.; Huang, D.; Hu, L.; Guo, Y. Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis. *Opt. Express* **2019**, *27*, 17186–17198. [\[CrossRef\]](#)
23. Xu, X. Enhancing quantum entanglement and quantum teleportation for two-mode squeezed vacuum state by local quantum-optical catalysis. *Phys. Rev. A* **2015**, *92*, 012318. [\[CrossRef\]](#)
24. Guo, Y.; Ding, J.Z.; Mao, Y.; Ye, W.; Liao, Q.; Huang, D. Quantum catalysis-based discrete modulation continuous variable quantum key distribution with eight states. *Phys. Lett. A* **2020**, *384*, 126340. [\[CrossRef\]](#)
25. Ye, W.; Guo, Y.; Xia, Y.; Zbinden, H.; Zhang, H.; Ding, J.Z.; Hu, L.Y. Discrete modulation continuous-variable quantum key distribution based on quantum catalysis. *Acta Phys. Sinica* **2020**, *69*, 060301. [\[CrossRef\]](#)
26. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343.
27. Guo, Y.; Li, R.J.; Liao, Q.; Zhou, J.; Huang, D. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier. *Phys. Lett. A* **2018**, *382*, 372–381. [\[CrossRef\]](#)
28. Mao, Y.; Wang, Y.; Huang, W.; Qin, H.; Huang, D.; Guo, Y. Hidden-Markov-model-based calibration-attack recognition for continuous-variable quantum key distribution. *Phys. Rev. A* **2020**, *101*, 062320. [\[CrossRef\]](#)
29. Wang, Y.; Mao, Y.; Huang, W.; Huang, D.; Guo, Y. Optical frequency comb-based multichannel parallel continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 25314–25329. [\[CrossRef\]](#)
30. Li, Z.; Zhang, Y.; Wang, X.; Xu, B.; Peng, X.; Guo, H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *93*, 012310. [\[CrossRef\]](#) [\[PubMed\]](#)
31. He, Y.Q.; Mao, Y.; Zhong, H.; Huang, D.; Guo, Y. Hybrid linear amplifier-involved detection for continuous variable quantum key distribution with thermal states. *Chin. Phys. B* **2020**, *29*, 050309. [\[CrossRef\]](#)
32. Guo, Y.; Liao, Q.; Wang, Y.; Huang, D.; Huang, P.; Zeng, G. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [\[CrossRef\]](#)

33. Wu, X.; Wang, Y.; Zhong, H.; Ye, W.; Huang, D.; Guo, Y. Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis. *Quantum Infor. Process.* **2020**, *19*, 234. [[CrossRef](#)]
34. Ryu, J.; Lim, J.; Lee, C.; Lee, J. Nonlocality for continuous variable system with local symplectic operation. *J. Mod. Opt.* **2010**, *57*, 1550–1554. [[CrossRef](#)]
35. Lee, S.-Y.; Ji, S.-W.; Kim, H.-J.; Nha, H. Enhancing quantum entanglement for continuous variables by a coherent superposition of photon subtraction and addition. *Phys. Rev. A* **2011**, *84*, 012302. [[CrossRef](#)]

Publisher’s Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).