Continuous Variable Quantum Secret Sharing with Security Enhancement in Practical Quantum Communications

Yun Mao 1,2,†, Yiwu Zhu 2,†, Yijun Wang 2,* and Ying Guo 2,3,*

1 School of Information Engineering, Shaoyang University, Shaoyang 422000, China
2 School of Automation, Central South University, Changsha 410083, China
3 School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: xxywyj@csu.edu.cn (Y.W.); guoying@bupt.edu.cn (Y.G.)
† These authors contributed equally to this work.

Abstract: Quantum communications can be conveniently implemented by two participants, but quantum secret key sharing (QSS) through multi-participant communication seems difficult in practice. In this paper, we propose a multi-participant QSS scheme with the local local oscillator (LLO) in continuous variable (CV) quantum communications. It allows an honest participant called a dealer to share a secret key with the others, making it possible to establish a secret key if and only if all participants gather together. The LLO scheme, which eliminates the need for the local oscillator (LO) to be propagated in insecure channels, can be used to avoid the potential LO attack in the traditional CVQSS scheme. Numerical simulation shows that the performance of the LLO-based CVQSS can be improved in terms of the maximal transmission distance even if it is performed with the partially trusted noise.

Keywords: quantum secret sharing; quantum communications; quantum cryptography

MSC: 81P94; 81P45

1. Introduction

Continuous variable quantum communications, which has the advantage of compatibility and convenience in signal preparations [1,2], has been proposed for secure communications with two participants. With the popularization of networks, however, the demand for multi-participant quantum communication increases. In order to establish a multi-participant approach to network, we consider implementations of quantum secret sharing (QSS) [3–5], where the secret message or information is divided into many pieces and sent to all users who participate in sharing information. The legal users can recover the initial message only if they cooperate together.

The traditional QSS was the discrete variable (DV) QSS [3–5] since it uses the single-photon for the signal single-photon source and single-photon detector for detection. Whereas, for CVQSS, it employs continuous light for the signal source and uses either a homodyne detector or heterodyne detector for detection. There is an advantage since it can be carried out by using the existing optical communication technology, resulting in good compatibility and usability [6]. After CVQSS was suggested in feasible implementations [7,8], lots of schemes on CVQSS have been proposed, which involve the detection of eavesdroppers, the modulation of coherent states, and so on [9,10]. However, there are few studies on security enhancement that are related to the key distribution in quantum communications.

Motivated by structure characteristics of the CV quantum communication systems [11], the propagation of local oscillator (LO) between the sender and the receiver is a necessary factor for security assurance [12,13]. Taking into account the performance improvement [14,15], we consider the local local oscillator (LLO)-based CVQSS. Different from
the previous CVQSS that involves the LO used to avoid the practical security problems of coherent detection [12], the proposed CVQSS can be implemented with the LLO-based detection scheme, aiming at security enhancement. Consequently, it provides an advantage because the LLO can be used to eliminate the potential dangers through insecure channels, such as the wavelength attack, the LO fluctuation attack, and the LO polarization attack [16,17]. However, when the LLO scheme is implemented in CVQSS for a large number of users, the performance of the system becomes worse. Fortunately, we can make the part of phase noise regarded as reliable to improve the performance, where the trusted part of phase noise is overestimated [18]. As the dealer needs to establish quantum communication links with all legal users, we can achieve security enhancement while making use of the partially trusted noises.

This paper is organized as follows. In Section 2, we suggest an approach to the implementation of the LLO-based CVQSS. In Section 3, we demonstrate the security analysis of the CVQSS system. Moreover, we perform numerical simulations to prove its feasibility in practical implementation, which includes the number of users, the maximal transmission distance and the secure key rate. Finally, the conclusion is drawn in Section 4.

2. The LLO-Based CVQSS

In the QSS scheme, each legal user $U_i$ can send the discretely modulated coherent states (DMCS), denoted by $u_i \in \{(x_i, p_i) : |x_i + ip_i\rangle\}$ for $i \in \mathbb{Z}_n = \{1, 2, \ldots, n\}$, to the dealer, and then recover the secret in cooperation by using the highly asymmetric beam splitter (HABS). The QSS scheme can be designed as follows.

Step 1. The user who is the farthest from the dealer can be arranged as the first user $U_1$, as shown in Figure 1. For all legal users $U = \{U_i : i \in \mathbb{Z}_n\}$, the user who is nearest to $U_i$ but has not been selected as $U_{i+1}$ for $i \in \mathbb{Z}_n$. In this way, we define the order of $n$ participants.

Step 2. $U_1$ prepares $u_1$ with phase reference, where both the signal and the phase reference are synchronously generated by using the same laser [11]. Then, $U_1$ sends them to $U_2$. Subsequently, $U_2$ prepares $u_2$ with phase reference and couples them to the same mode as $U_1$ has. Finally, $U_n$ sends the final mode to the dealer.

Step 3. Repeat the above steps to ensure all participants hold sufficient raw data. In order to estimate $T_i$, the dealer requests all participants to announce the corresponding data in a random subset of raw data. After that, they discard the disclosed data.

![Figure 1. The LLO-based QSS with discretely modulated coherent states.](image)

Because the displacement of each user is $(x_i, p_i)$, the resulting signal which is received by the dealer can be expressed as $(x_d, p_d)$ with

$$x_d = \sum_{i=1}^{n} \sqrt{T_i} x_i, \quad p_d = \sum_{i=1}^{n} \sqrt{T_i} p_i,$$

where $T_i$ is the $i$-th channel transmittance established between $U_i$ and the dealer.

Step 3. Repeat the above steps to ensure all participants hold sufficient raw data. In order to estimate $T_i$, the dealer requests all participants to announce the corresponding data in a random subset of raw data. After that, they discard the disclosed data.
Step 4. All users $U_i$ achieve the key $K$ according to the calculation $K = \bigoplus_{i=1}^{n} K_i$, where $K_i$ is the deviation of $u_i$.

Assuming that $U_i$ is honest, the dealer chooses a random subset of remaining raw data while asking all users $U$ except $U_i$ to announce their raw data, respectively. Following the resulting data, the measurements will be updated as

$$
x_{ri} = x_d - \sum_{j\neq i}^{n} \sqrt{T_j} x_j, \quad p_{ri} = p_d - \sum_{j\neq i}^{n} \sqrt{T_j} p_j,$$

for $i, j \in \mathbb{Z}_n$. When establishing the link $T_i$ between the dealer and $U_i$, we can achieve the secret key rate $R_i$. Subsequently, a lower bound of the final secret key rate $R$ of CVQSS can be expressed as $R = \min\{R_i : i \in \mathbb{Z}_n\}$ [19].

When considering the characteristics of $R$ for the LLO-based CVQSS, we take into account the effect of the phase noise given by [20]

$$\xi_{\text{phase}} = 2V_A \left(1 - e^{-\frac{V_{\text{est}}^2}{2}}\right),$$

where $V_A$ denotes the modulation variance, $V_{\text{est}}$ is the variance of the phase noise given by $V_{\text{est}} = \text{var}(\theta_S - \hat{\theta}_S)$ with the real phase rotation value $\theta_S$ and the estimated value $\hat{\theta}_S$. The analysis and extrapolation of $V_{\text{est}}$ are detailed in Appendix A, where the relations of the trusted phase noise, the total channel added noise, the total detection added noise and the total added noise has been derived in details.

3. Performance Analysis

3.1. Derivation of the Secret Key Rate

We have achieved the secret key rate $R$ of the LLO-based QSS system for $U_i$. The secret key rate can be obtained from the longest transmission distance when each user $U_i$ has an equal amount of noise $\xi_{\text{tot}}$, including the phase noise $\xi_{\text{phase}}^{0}$ and $\xi_{\text{rest}}$ [19]. Without loss of generality, Alice is the farthest user $U_1$ and Bob is the dealer. The rest of $n - 1$ users are assumed to be dishonestly located with an equal interval. Then, the secret key rate $R$ can be calculated as [21]

$$R = \beta I_{AB} - \chi_{BE},$$

where $\beta$ denotes the traditional reconciliation efficiency, $I_{AB}$ is Alice and Bob’s mutual information, and $\chi_{BE}$ is Eve and Bob’s Holevo bound.

Assuming that the transmittance of HABS approaches one, the channel transmittance of the $i$-th participant $U_i$ is calculated as

$$T_i = 10^{-\frac{\delta l_i}{10}},$$

where $l_i$ denotes the transmission distance between $U_i$ and the dealer, and $\delta$ is the attenuation coefficient of the fiber link. The excess noise of $U_i$, referring to the channel input, can be calculated by [6]

$$\xi_i = \frac{T_i}{T_1} (\xi_{\text{rest}}^{0} + \xi_{\text{phase}}^{0})$$

$$= \frac{T_i}{T_1} (\xi_{\text{rest}} + \xi_{\text{error}} - \frac{\xi_{\text{error}} T_1}{T_1}),$$

where $\xi_{\text{rest}} = \xi_{\text{rest}}^{0} + \xi_{\text{AM}} + \xi_{\text{LE}} + \xi_{\text{ADC}}$ [19]. Combined with the results in Appendix A, the channel-added noise, the total channel-added noise, the total detection-added noise and the total added noise can be derived as
We note that the derivation of the parameter $\kappa_{15}$, the maximal transmission distance approaches 10 km. While deriving the secure key with an increased number of legal users. When the number of users is selected more than $D = \left( V + \sqrt{B} \chi_{\text{het}} / T (V + \chi_{\text{tot}}) \right)^2$, the effect of noise and influence brought by other $n-1$ untrusted users become disastrous when the number of users $U$ is increased.

Consequently, Alice and Bob’s mutual information $I_{AB}$ can be derived as

$$I_{AB} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}},$$

where $V = 1 + V_A$. The Holevo bound $\chi_{BE}$ is given by

$$\chi_{BE} = S(\rho_E) - \int d\chi_{\left(\rho_{E}^{x,B,p_B}\right)} S\left(\rho_{E}^{x,B,p_B}\right),$$

where $(\chi_{x}, \rho_{B})$ is Bob’s results with the probability density $P(\chi_{x}, \rho_{B})$, $\rho_{E}^{x,B,p_B}$ denotes the eavesdropper’s state based on Bob’s measurements, and $S$ represents the von Neumann entropy. Followed by the derivation in Appendix A, we assume that the loss and noise of Bob’s detector are all trusted, and then we obtain

$$\chi_{BE} = \sum_{j=1}^{2} \mathcal{G}\left(\frac{\lambda_{j} - \frac{1}{2}}{2}\right) - \sum_{j=3}^{8} \mathcal{G}\left(\frac{\lambda_{j} - \frac{1}{2}}{2}\right),$$

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$, and $\{\lambda_{k} : k \in \{1, 2, 3, 4\}\}$ can be described as

$$\lambda^2_{1,2} = \frac{1}{2} \left[ A \pm \sqrt{A^2 - 4B} \right], \quad \lambda^2_{3,4} = \frac{1}{2} \left[ C \pm \sqrt{C^2 - 4D} \right],$$

involving the parameters $A, B, C$ and $D$ given by

$$A = V^2 + T^2 \left( V + \chi_{\text{line}}^T \right)^2 - 2T\kappa_1^2, \quad B = T^2 \left( V^2 + V \chi_{\text{line}}^T - \kappa_2^2 \right)^2, \quad C = \frac{1}{T^2 (V + \chi_{\text{tot}})} \left\{ A (\chi_{\text{het}}^T)^2 + B + 1 + 2\chi_{\text{het}}^T \left[ V\sqrt{B} + T(V + \chi_{\text{tot}}) + 2T\kappa_4^2 \right] \right\}, \quad D = \left( V + \sqrt{B} \chi_{\text{het}} / T (V + \chi_{\text{tot}}) \right)^2, \quad \lambda_5 = 1.$$
Figure 2. Asymptotic secret key rate of the LLO-based CVQSS. The dashed lines denote the situation of conventional phase noise and the solid lines denote the partially trusted phase noise.

Meanwhile, for the given number of legal users $U$, the maximal transmission distance can be lengthened when taking into account the partially trusted noise. The reason is that the tolerance of the traditional phase noise is lower than that of the partially trusted noise. Taking $n = 2$ as an example, the maximal transmission distance is slightly less than 40 km. However, it reaches more than 50 km for the trusted noise, which means it delivers a performance improvement. With the traditional phase noise, the implementation of the LLO-based CVQSS will result in limits in terms of the secret key rate and the maximal transmission distance. A slight excess noise will become a great impact on the performance because the system is sensitive to the excess noise, as shown in Figure 3. This improvement is more pronounced with the large number of users $U$. It seems that the proposed scheme is very sensitive to the number of users $U$. Therefore, three factors, which include the secret key rate, the maximal transmission distance and the number of legal users, should be determined to illustrate the security of the LLO-based CVQSS. For example, while designing a scheme with long-distance transmission and high-rate secret keys, the number of legal users $U$ has to be sacrificed.

Figure 3. The excess noise (solid lines) and the partially trusted phase noise for $n \in \{2, 5, 10, 15\}$.

4. Conclusions

We have proposed an approach to the LLO-based CVQSS with security enhancement, which can be further improved by making the partial phase noise be trusted. We prove the security of the CVQSS system while considering effects of the external eavesdroppers and dishonest users. Numerical simulations demonstrate the performance of the LLO-based CVQSS system when taking into account the effect of the number of legal users. When we
take the suitable numbers of legal participants, the performance of the LLO-based CVQSS can be furthermore improved in terms of the secret key rate, which is compared with the traditional one. Moreover, we find that the performance of the system can be improved by making full use of the partially trusted phase noise. It leaves an optimization space for multi-participant secret sharing in practical networks.

**Author Contributions:** Conceptualization, Y.M.; writing—original draft preparation, Y.Z.; writing—review, Y.W.; writing—editing, Y.G. All authors have read and agree to the published version of the manuscript.

**Funding:** This work was supported by the National Natural Science Foundation of China (Grant No. 61871407), and the Special Funds for the Construction of an Innovative Province in Hunan (Grant No. 2022GK2016).

**Data Availability Statement:** All data generated or analyzed during this study are included in this published article.

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

**Appendix A. The Phase Noise**

The parameter $V_{\text{error}}$ denotes the variance generated by the error between the real phase rotation value $\theta_R$ and estimated value $\hat{\theta}_R$ given by

$$V_{\text{error}} = \text{var}(\theta_R - \hat{\theta}_R) = \frac{\chi + 1}{E_R^2}, \quad (A1)$$

where $\chi$ is the total noise of phase reference can be calculated by

$$\chi = \frac{1}{T} - 1 + \varepsilon_0 + \frac{2 - \mu + 2v_{\text{el}}}{T\mu}. \quad (A2)$$

The first three items mentioned above are the components of channel-added noise in quantum communications, and the last item denotes the heterodyne detector noise. The parameter $V_{\text{drift}}$ represents the variance of the relative phase drift between two lasers for $\Delta T$, which can be described as

$$V_{\text{drift}} = 2\pi(\Delta v_A + \Delta v_B)\Delta T \quad (A3)$$

where $\Delta v_A$ and $\Delta v_B$ correspond to the line widths of the two free-running lasers. The parameter $V_{\text{channel}}$ represents the variance of the noise resulting from the accumulated drift of phase of the signal pulse. Therefore, when $V_{\text{est}}$ approaches 0, the phase noise can be approximated as

$$\xi_{\text{phase}} = V_A(V_{\text{drift}} + V_{\text{channel}} + V_{\text{error}}) = \xi_{\text{drift}} + \xi_{\text{channel}} + \xi_{\text{error}}. \quad (A4)$$

Furthermore, we consider the characteristics of the trusted noise after calibration. The excess noise $\xi$ is a component element of the channel added noise, which is part of the total added noise, and hence it can be described as

$$\xi = \xi_{\text{phase}} + \xi_{\text{rest}}. \quad (A5)$$

Then the total channel added noise $\chi_{\text{line}}$ can be given by

$$\chi_{\text{line}} = 1/T - 1 + \xi. \quad (A6)$$

The total detection added noise $\chi_{\text{het}}$ can be calculated as

$$\chi_{\text{het}} = (2 - \mu + 2v_{\text{el}})/\mu. \quad (A7)$$
Combined with the noise calculation method, the total noise can be derived as

\[ \chi_{\text{tot}} = \chi_{\text{line}} + \frac{\chi_{\text{het}}}{T}. \]  

(A8)

In what follows, we try to distinguish the trusted and untrusted parts among them. We assume \( \chi_{\text{het}} \) is the trusted noise based on a well calibration of \( \mu \) and \( v_{el} \). Meanwhile, since the part of the phase noise \( \xi_{\text{error}} \) can be perfectly controlled and calibrated by Bob, it can be regarded as the trusted noise [18,22].

Based on (A8), we achieve the total phase noise of reference given by

\[ \chi = \chi^u + \frac{\chi^T}{T}, \]  

(A9)

where

\[ \chi^u = \frac{1}{T} - 1 + \varepsilon_0 \]  

and

\[ \chi^T = \frac{2 - \mu + 2v_{el}}{\mu}. \]  

(A10)

Combined with (A1), (A2), (A4) and (A9), the measurement noise of phase reference can calculated as

\[ \xi_{\text{error}} = \xi^u_{\text{error}} + \frac{\xi^T_{\text{error}}}{T}, \]  

(A11)

where

\[ \xi^u_{\text{error}} = V_A \left( \frac{\chi^u + 1}{E_R^2} \right) = V_A \left( \frac{1 + TE_0}{TE_0^2} \right), \]  

(A12)

Appendix B. The Secret Key Rate

In the EB version, DMCS with QPSK modulation can be defined as [24]

\[ |\Psi_4}\rangle = \sum_{k=0}^{3} \sqrt{\lambda_k} |\phi_{k}^4\rangle |\phi_{k}^4\rangle = \frac{1}{2} \sum_{k=0}^{3} |\psi_{k}^4\rangle |\alpha_{k}^4\rangle, \]  

(A13)

where the state \( |\psi_{k}^4\rangle \) for \( k \in Z_4 \), can be given by

\[ |\psi_{k}^4\rangle = \frac{1}{2} \sum_{m=0}^{3} e^{i(1+2k)m\pi/4} |\phi_{m}^4\rangle. \]  

(A14)

The state \( |\phi_{m}^4\rangle \) for \( m \in Z_4 \), can be described as

\[ |\phi_{k}^4\rangle = \frac{e^{-a^2/2}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} (-1)^n \frac{a^{4n+k}}{\sqrt{(4n+k)!}} |4n+k\rangle \]  

(A15)

with \( \lambda_{0,2} \) and \( \lambda_{1,3} \) given by

\[ \lambda_{0,2} = \frac{1}{2} e^{-a^2} \left[ \cosh (a^2) \pm \cos (a^2) \right], \quad \lambda_{1,3} = \frac{1}{2} e^{-a^2} \left[ \sinh (a^2) \pm \sin (a^2) \right]. \]  

(A16)

Therefore, the mixture state \( \rho_4 \) can be defined as

\[ \rho_4 = \text{Tr}(|\Psi_4\rangle \langle \Psi_4|) = \sum_{k=0}^{3} \lambda_k |\phi_{k}^4\rangle \langle \phi_{k}^4|. \]  

(A17)
Let $A$ and $B$ describe two output modes of state $|\Psi_4\rangle$, whereas $\hat{a}$ and $\hat{b}$ denote the respective annihilation operators corresponding to $A$ and $B$. We can achieve the covariance matrix, denoted by $\Gamma_{AB}^4$, of $|\Psi_4\rangle$. Namely, we obtain

$$\Gamma_{AB}^4 = \begin{pmatrix} X \mathbb{I} & \kappa_4 \sigma_z \\ \kappa_4 \sigma_z & Y \mathbb{I} \end{pmatrix},$$

where $\mathbb{I}$ and $\sigma_z$ represent the respective diagonal matrices diag(1,1) and diag(1,−1), and $X$, $Y$, and $Z_4$ are parameters given by

$$X = \langle \Psi_4 | 1 + 2a^\dagger a | \Psi_4 \rangle = 1 + 2a^2,$$

$$Y = \langle \Psi_4 | 1 + 2b^\dagger b | \Psi_4 \rangle = 1 + 2a^2,$$

$$\kappa_4 = \langle \Psi_4 | ab + a^\dagger b^\dagger | \Psi_4 \rangle = 2a^2 \sum_{k=0}^3 \lambda_k^{3/2} \lambda_k^{-1/2}.$$

References

