Simultaneous Classical Communication and Quantum Key Distribution Based on Plug-and-Play Configuration with an Optical Amplifier

Xiaodong Wu ¹, Yijun Wang ¹, Qin Liao ¹, Hai Zhong ¹ and Ying Guo ¹,², *

¹ School of Automation, Central South University, Changsha 410083, China; wuxiaodong2019@163.com (X.W.); llqqlq@csu.edu.cn (Q.L.); zhonghai@csu.edu.cn (H.Z.)
² Jiangsu Key Construction Laboratory of IoT Application Technology, Wuxi Taihu University, Wuxi 214064, China
* Correspondence: csuyijun@163.com (Y.W.); yingguo@csu.edu.cn (Y.G.)

Received: 28 January 2019; Accepted: 26 March 2019; Published: 27 March 2019

Abstract: We propose a simultaneous classical communication and quantum key distribution (SCCQ) protocol based on plug-and-play configuration with an optical amplifier. Such a protocol could be attractive in practice since the single plug-and-play system is taken advantage of for multiple purposes. The plug-and-play scheme waives the necessity of using two independent frequency-locked laser sources to perform coherent detection, thus the phase noise existing in our protocol is small which can be tolerated by the SCCQ protocol. To further improve its capabilities, we place an optical amplifier inside Alice’s apparatus. Simulation results show that the modified protocol can well improve the secret key rate compared with the original protocol whether in asymptotic limit or finite-size regime.

Keywords: simultaneous; classical communication; quantum key distribution; plug-and-play configuration; optical amplifier

1. Introduction

Quantum key distribution (QKD) is one of the most active areas in quantum information science, which promises to generate a secure key between two authenticated parties (Alice and Bob) over insecure quantum and classical channels [1–4]. The security of a key is guaranteed by the fundamental laws of quantum mechanics [5,6]. Generally speaking, there are two main approaches for the implementation of QKD, namely, discrete-variable (DV) QKD [7] and continuous-variable (CV) QKD [8–11]. Different from the DVQKD, in CVQKD, there is no requirement to use expensive single-photon detectors. Instead, the key bits are encoded in the quadrature variables (X and P) of the optical field, and the secret key bits are decoded through high-efficiency homodyne or heterodyne detection techniques [12–15].

At present, the CVQKD protocol, especially for the Gaussian-modulated coherent-state (GMCS) scheme, has been demonstrated over 100-km telecom fiber through controlling excess noise [16] and designing high-efficiency error correction codes [17–19]. From a practical point of view, the hardware needed in the implementation of the GMCS QKD is amazingly similar to that needed in classical coherent optical communication [20]. On the basis of this similarity, it is viable to take advantage of the same communication facility for both QKD and classical communication.

Recently, a simultaneous classical communication and quantum key distribution (SCCQ) scheme was proposed [21,22]. In this scheme, the Gaussian distributed random numbers for GMCS QKD and bits for classical communication are encoded on the same weak coherent pulse and decoded through
the same coherent receiver, which provides a more cost-effective solution in practice. However, a major obstacle to the SCCQ scheme is that it can only tolerate a very small amount of phase noise [21]. This problem could lead to poor performance and thus obstruct its further development.

In this paper, we propose a SCCQ protocol based on plug-and-play configuration with an optical amplifier. Different from the GMCS QKD protocols using a true local oscillator (LO) [23–25], the plug-and-play CVQKD scheme waives the necessity of using two independent frequency-locked laser sources and automatically compensating the polarization drifts [26]. Since the LO and signal pulses are generated from the same laser source, we can obtain a small phase noise which can be tolerated by the SCCQ protocol in the framework of plug-and-play configuration. To further improve its capabilities, we insert an optical amplifier (OA) at the output of the quantum channel [27–29]. The modified protocol (SCCQ protocol based on plug-and-play configuration with an OA) can well increase the secret key rate by compensating the imperfection of Alice’s detector with only little cost in transmission distance. Here, both the asymptotic limit and the finite-size regime are taken into consideration.

This paper is structured as follows. In Section 2, we first introduce the plug-and-play dual-phase modulated coherent states (DPMCS) scheme, then present the model of SCCQ protocol based on plug-and-play configuration and the proposed modified protocol. In Section 3, we perform the noise analysis and show numeric simulations in view of practical system parameters. Finally, conclusions are drawn in Section 4. Detailed calculation of equations is shown in the Appendix.

2. Protocol Description

In this section, we first introduce the plug-and-play DPMCS protocol. Then, we present the model of SCCQ protocol based on the plug-and-play configuration and its modified protocol (with OA). To simplify the analysis, we adopt the binary phase-shift keying (BPSK) modulation for the classical communication and the GMCS for QKD protocol in this paper.

2.1. The Plug-and-Play DPMCS Protocol

The prepare-and-measurement scheme of plug-and-play DPMCS protocol is illustrated in Figure 1. The source of light is sent from Alice to Bob, then Bob performs the dual-phase-modulation work after receiving the light. During the modulated process, random numbers drawn from a random number generator are utilized to modulate the amplitude and phase quadrature (X and P quadrature). This is really different from previous one-way CV-QKD protocols where the symmetrical Gaussian modulation is performed at Alice’s side. When Bob completes the modulation work, the dual-quadrature modulated coherent-state is directly reflected to Alice with the help of Faraday mirrors. After passing through the untrusted channel characterized by transmittance $T$ and excess noise $\xi$, Alice receives the modulated signal. Then, she performs homodyne detection to measure the incoming mode. After this, Alice can obtain the list of data which is correlated with the list of Bob. Note that this correction is important in generating a secret key through error reconciliation and privacy amplification. Here, the classical source mentioned above is controlled by Fred [26]. Besides, the untrusted source noise is characterized by taking advantage of a phase-insensitive amplifier (PIA) with a gain of $g$. In such a practical scheme, the detector used by Alice features an electronic noise $\nu_{el}$ and an efficiency $\eta$. Therefore, the detector-added noise referred to Alice’s input can be expressed as $\chi_{hom} = [(1 - \eta) + \nu_{el}] / \eta$. 
Figure 1. The prepared-and-measure scheme of plug-and-play dual-phase modulated coherent states (DPMCS) protocol. (a) Gaussian modulation scheme by using two phase modulators. PIA, phase insensitive amplifier; RNG, random number generator; PM, phase modulator; FM, Faraday mirror.

2.2. SCCQ Protocol Based on Plug-and-Play Configuration

In the BPSK modulation scheme, the bit value $k_B$ is encoded by $|e^{-ik_B \pi} \rangle$, where $\alpha$ is a real number. While, in plug-and-play DPMCS protocol, Bob prepares coherent state $|x_B + ip_B \rangle$ and transmits it to Alice. Here $x_B$ and $p_B$ are assumed to be Gaussian random numbers with zero mean and a variance of $\sqrt{V_B}$, where $N_0$ represents the shot-noise variance. The SCCQ protocol based on plug-and-play configuration is straightforward and combines these two communication schemes. Namely, as shown in Figure 2, both the classical bit $k_B$ and Gaussian random numbers $\{x_B, p_B\}$ are encoded on a coherent state $(x_B + e^{-ik_B \pi}) + i(p_B + e^{-ik_B \pi})$. It is remarkable that in the plug-and-play DPMCS protocol, Alice performs homodyne detection to measure either the $X$ or $P$ quadrature of each incoming signal. In order to obtain deterministic classical communication, the same classical bit $k_B$ should be encoded on both $X$ and $P$ quadratures.

Figure 2. Simultaneous classical communication and quantum key distribution (SCCQ) protocol based on plug-and-play configuration. The probability distributions of $X$-quadrature measurement is shown at Alice’s side.

Suppose Alice measures the $X$ quadrature ($P$ quadrature) and obtains the measurement result $x_h$ ($p_h$). The sign of $x_h$ ($p_h$) can be utilized to determine a classical bit $k_B$. In other words, the value of $k_B$ is assigned as 0 if $x_h > 0$ and the value of $k_B$ is assigned as 1 if $x_h < 0$. Note that according to the overall transmittance $T_\eta$ and the value of $k_B$, Alice’s measurement result can be rescaled and displaced to generate a secure key, which is given by

$$x_A = \frac{x_h}{\sqrt{T_\eta}} + (2k_B - 1)\alpha,$$
$$p_A = \frac{p_h}{\sqrt{T_\eta}} + (2k_B - 1)\alpha. \quad (1)$$

On the basis of the raw keys $\{x_B, x_A\}$ and $\{p_B, p_A\}$, Alice and Bob can distill a secure key by proceeding with classical data postprocessing, as in the case of traditional GMCS QKD.
The prepare-and-measurement (PM) version of our protocol shown above is equivalent to the entanglement-based (EB) version. In the EB scheme, Fred prepares a three-mode entanglement state $|\Phi_{ABF}\rangle$. Bob keeps one mode ($B$) with variance $V = V_B + 1$ and measures it by using a heterodyne detector. The other mode ($A_0$) is sent to Alice through an untrusted quantum channel. At Alice’s side, a beam splitter with transmission $\eta$ is taken advantage of to model her detector inefficiency, while an EPR state of variance $\nu_{el}$ is utilized to model its electronics. For the homodyne detection case, we have $\nu_{el} = \eta \chi_{hom} (1 - \eta) = 1 + \nu_{el} (1 - \eta)$. Finally, to distill the secret key, Alice and Bob perform information reconciliation and privacy amplification procedures. Here, we mainly consider the reverse reconciliation since it has been proved to provide a great advantage in performance of QKD schemes [11].

2.3. Addition of an Optical Amplifier

In practice, because of some inherent imperfection inevitably existing in Alice’s detection apparatus, the ideal detection process cannot be achieved. Therefore, we can only obtain a lower secret key rate than expected. In order to improve the performance of our protocol, here, an optical amplifier is applied to compensate for the detectors’ imperfections. In the following, two types of amplifiers are considered, namely, the phase-sensitive amplifier (PSA) and phase-insensitive amplifier (PIA).

**Phase-sensitive amplifier.** The PSA can be deemed as a degenerate amplifier which allows ideally noiseless amplification of a chosen quadrature. We use a matrix $\Xi_{PSA}$ to describe its properties, which is given by

$$
\Xi_{PSA} = \begin{pmatrix}
\sqrt{G} & 0 \\
0 & \frac{1}{\sqrt{G}}
\end{pmatrix},
$$

where $G$ represents the gain of amplification and $G \geq 1$.

**Phase-insensitive amplifier.** The PIA can be regarded as a non-degenerate amplifier, which is able to amplify both quadratures symmetrically. Different from the PSA, the amplification process of the PIA is related to the inherent noise. The transform of the PIA can be modeled as

$$
\Xi_{PIA} = \begin{pmatrix}
\sqrt{g} I_2 & \sqrt{g-1} \sigma_z \\
\sqrt{g} \sigma_z & \sqrt{g-1} I_2
\end{pmatrix},
$$

The inherent noise of the PIA can be given by

$$
\Xi_{noise} = \begin{pmatrix}
\frac{N_s I_2}{\sqrt{N_s^2 - 1} \sigma_z} & \frac{N_s^2 - 1}{N_s I_2} \sigma_z \\
\frac{N_s}{\sqrt{N_s^2 - 1} \sigma_z} & \frac{N_s^2}{N_s I_2}
\end{pmatrix},
$$

where $g$ is the gain of the PIA and $N_s$ stands for variance of noise. We have introduced the PIA in the above analysis. Different from the PSA which is inserted into the output of the quantum channel in our protocol, the PIA is placed at the channel to characterize the untrusted source noise. That is to say the gain $g$ of the PIA can be used to weight the source noise in the plug-and-play scheme.

As illustrated in Figure 3, after the amplification process, mode $A_3$ is measured using Alice’s detector. A beam splitter with transmission $\eta$ is taken advantage of to model her detector inefficiency. Besides, an EPR state of variance $\nu_{el}$ is utilized to model its electronics. It is worth mentioning that we adopt homodyne detection in our scheme, thus it is suitable for us to choose the PSA to compensate for Alice’s apparatus imperfection [27,28]. Then, the modified parameter $\chi_{hom}^{PSA}$ for this case is given by

$$
\chi_{hom}^{PSA} = \frac{(1 - \eta) + \nu_{el}}{G \eta}.
$$

Consequently, we can achieve the modified secure key rate $\hat{K}$ by substituting $\chi_{hom}^{PSA}$ for $\chi_{hom}$ in homodyne detection case.
3. Performance Analysis and Discussion

The noises which originated from the practical system have important effects on the performance of the SCCQ protocol. In this section, we first introduce the noise model which we adopt in this paper and present the computation of the BER in BPSK modulation scheme. Then, we show and discuss the simulation results.

3.1. Noise Model of SCCQ Protocol Based on Plug-and-Play Configuration

Note that the main noise sources analyzed here are (1) the detector noise assumed as $v_{el}$, (2) the vacuum noise, (3) the excess noise due to the untrusted sources denoted by $\zeta_u$, (4) excess noise $\xi_{RB}$ caused by Rayleigh backscattering photons, (5) the Gaussian modulation for QKD with a variance of $V_B$. All the noises mentioned above are defined in the shot-noise unit.

Now let’s calculate the BER of the BPSK modulation scheme, which is expressed by [21]

$$BER = \frac{1}{2} erfc\left( \frac{\sqrt{T\eta \alpha}}{\sqrt{2N_0(V_B T \eta + v_{el} + 1)}} \right),$$

where $erfc(x)$ represents the complementary error function. In order to make the value of BER small enough in the classical channel, namely, obtain a BER of $10^{-9}$, the displacement $\alpha$ is required as

$$\alpha = 4.24\sqrt{\frac{V_B T \eta + v_{el} + 1}{\sqrt{2T\eta}}}.$$  

The numerical simulations of the required displacement $\alpha$ as a function of the transmission distance and modulation variance $V_B$ are illustrated in Figure 4. It shows that the longer transmission distance needs a larger displacement $\alpha$ for a typical modulation variance $V_B$ in the range of 1 to 20.
The untrusted source noise $\zeta_s$ is deemed to be one of the most important excess noises in the plug-and-play configuration. It can be expressed as $\zeta_s = (g - 1) + (g - 1) V_I$, where $g$ is a gain of a PIA and $V_I$ is the noise variance of a vacuum state $(X_I, P_I)$. That is to say, the untrusted source noise $\zeta_s$ can be weighted by parameter $g$.

The other excess noise we need to consider here is $\zeta_{RB}$, which is caused by Rayleigh backscattering photons. Since the reflected light in the plug-and-play configuration is of the same frequency as the initial laser source, we cannot use the “in-band” photon to filter or attenuate it. The excess noise $\zeta_{RB}$ is given by

$$\zeta_{RB} = \frac{2\langle N_{RB}\rangle}{\eta_T},$$

where $\langle N_{RB}\rangle$ is Rayleigh backscattering photons. Then, the backscattered photons $\langle N_{RB}\rangle$ per second $\Delta_B$ is expressed as [30]

$$\Delta_B = \frac{\omega(1 - 10^{-2\gamma L/10})V_BR}{2\eta_T},$$

where $\omega$ stands for the the Rayleigh backscattering coefficient, $\eta_B$ represents the insertion loss inside Bob (round-trip), $R$ represents the system repetition rate, $\gamma$ is a fiber loss, and $L$ is the length of an infinite fiber used as a QKD link. Under the assumption that the electronic integral time of Alice’s homodyne detector is $\sigma t$, the excess noise $\zeta_{RB}$ can be rewritten as

$$\zeta_{RB} = \frac{2\Delta_B \eta_T \sigma t}{\eta_B T} = \frac{\omega(1 - 10^{-2\gamma L/10})V_BR \sigma t}{\eta_B 10^{-2\gamma L/10}}.$$

Note that Equation (10) shows the excess noise which is caused by the quantum channel, namely, here $\zeta_{RB}$ can be used to represent $\xi$.

In the following, we perform an analysis of the effect of phase noise, which commonly exists in a coherent communication system. The excess noise caused by the phase instability is given by

$$\zeta_p = \frac{\sigma^2 \phi}{N_0},$$

where $\phi$ represents the phase-noise variance. Here Equation (11) is derived with the assumption of $\alpha^2 \geq (V_B + 1)N_0$ [21]. It is worth mentioning that the excess noise $\phi$ not only contains the phase noise between the signal and the LO but also the other modulation errors.

On the basis of the above analysis, the overall excess noise outside Alice’s system can be defined as

$$\zeta_t = \zeta_s + \zeta_{RB} + \zeta_p.$$

Note that excess noises $\zeta_s$ and $\zeta_{RB}$ are independent of $\alpha$.

3.2. Simulation Results

In Figure 5, we conduct numerical simulations of the asymptotic secret key rate as a function of transmission distance in different imperfect source scenarios. Note that $g = 1$ means no source noise case. We adopt the optimal value of modulation $V_B$ in the analysis (see Appendix A). Here, the solid lines in Figure 5 stand for the case of the original protocol ($G = 1$), while the dashed lines represent the case of the modified protocol (a protocol with homodyne detection and a PSA, $G = 3$). On the one hand, we observed that for each imperfect source scenario, the secret key rate is well improved within a relatively long distance by utilizing an optical preamplifier. On the other hand, we also found that the maximum secure distance of the modified protocol is slightly shorter compared with the original protocol. That is to say, by utilizing the optical amplifier, the secret key rate of the modified protocol increases in a large range of distance with a slight cost of the maximum transmission distance. It is remarkable that the PLOB bound has been plotted in Figure 5, which illustrates the ultimate limit...
of point-to-point QKD [31]. Here, we should note that the phase noise in our protocol is very small since the LO and signal pulses are generated from the same laser source in the plug-and-play scheme. Therefore, we can achieve the phase noise $\zeta_p = 10^{-6}$. Detailed calculation of the asymptotic secret key rate is shown in Appendix B.

![Figure 5. Comparison of secret key rate between the modified protocol (homodyne detection with phase-sensitive amplifier (PSA)) and the original protocol (without PSA) under different imperfect source scenarios. Solid lines represent the original protocol (G = 1) while the dashed lines represent the modified protocol (G = 3). From left to right, the green curves correspond to $g = 1.015$, the black curves correspond to $g = 1.01$, the red curves correspond to $g = 1.005$, and the blue curves correspond to $g = 1$ (no source noise). The simulation parameters are $V_B = 4$, $\zeta_p = 10^{-6}$, $\zeta_{RB} = 0.02$, $\eta = 0.5$, $\nu_{id} = 0.1$.](image)

In addition, it is necessary to consider the finite-size effect since the length of secret key is impossibly unlimited in practice. Different from the asymptotic case, in the finite-size scenario, the characteristics of the quantum channel cannot be known before the transmission is performed. The reason is that a portion of the exchanged signals needs to be taken advantage of for parameter estimation instead of generating the secret key. We conduct numerical simulations of the finite-size secret key rate in different imperfect source scenarios, as shown in Figure 6. The solid lines in Figure 6 stand for the case of the original protocol ($G = 1$), while the dashed lines represent the case of the modified protocol ($G = 3$). From left to right, the green curves, the black curves, and the red curves correspond to the finite-size scenario of block length $N = 10^6$, $10^8$, and $10^{10}$, respectively, and the blue curves represent the asymptotic scenario. Here, Figure 6a–d show the proposed protocol with $g = 1$ (no source noise), $g = 1.005$, $g = 1.01$, and $g = 1.015$. We observe that the performance of the asymptotic scenario is better than that of the finite-size scenario whether the PSA is placed at Alice’s detection apparatus or not. Furthermore, the curves of the finite-size scenario are more and more close to the curve of asymptotic case with the increased number of exchanged signals $N$. That is to say that the more exchanged signals we have, the more the signal parameter estimation step can be utilized, and thus the parameter estimation is approaching perfection. Interestingly, for each imperfect source scenario, the finite-size secret key rate of the modified protocol is well improved without the price of reducing the maximum transmission distance, especially for the small-length block, compared with the original protocol, which is different from the asymptotic case. Detailed calculation of finite-size secret key rate is shown in Appendix C.
Figure 6. Finite-size secret key rate of SCCQ protocol based on plug-and-play configuration with PSA as a function of transmission distance under different imperfect source scenarios. Solid lines represent the original protocol ($G = 1$) while the dashed lines represent the modified protocol ($G = 3$). From left to right, the green curves, the black curves, and the red curves correspond to finite-size scenario of block length $N = 10^6$, $10^8$, and $10^{10}$, respectively, and the blue curves represent the asymptotic scenario. (a) The parameter $g = 1$ (no source noise). (b) The parameter $g = 1.005$. (c) The parameter $g = 1.01$. (d) The parameter $g = 1.015$. Other parameters are set to be the same as Figure 5.

4. Conclusions

We propose a SCCQ protocol based on plug-and-play configuration with an optical amplifier. Benefiting from the plug-and-play scheme where a real local LO is generated from the same laser of quantum signal at Alice’s side, the phase noise existing in our protocol is very small, which can be tolerated by the SCCQ protocol. Therefore, our research may bring the SCCQ technology into real life and thus reduce the cost of QKD effectively. To further improve its capabilities, we inserted an optical amplifier inside Alice’s apparatus. The simulation results show that the secret key rate is greatly enhanced in a large range of distances for each imperfect source scenario in both asymptotic limit and finite-size regime compared with the original protocol.

Author Contributions: Y.W. and Y.G. gave the general idea of the study, designed the conception of the study and performed critical revision of the manuscript. X.W. accomplished the formula derivation and numerical simulations and drafted the article. Q.L. provided feasible advices and critical revision of the manuscript. All authors have read and approved the final manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (Grant Nos. 61572529, 61871407, 61872390, 61801522), and the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 18KJB510045).

Conflicts of Interest: The authors declare no conflict of interest.
Appendix A. Parameter Optimization

To maximize the performance of our protocol, we need to find an optimal Bob’s modulation $V_B$. As illustrated in Figures A1–A3, different values of $g$, $d$, and $G$ are, respectively, set to find a public optimal $V_B$. From Figure A1, we observe that as the value of parameter $g$ increases (the source noise increases), the optimal interval becomes gradually compressed. In addition, the secret key rate also decreases as a result of the increase in parameter $g$. Fortunately, there exists a public interval where we can obtain a public optimal modulation $V_B$ for all curves in Figure A1. Namely, we have $V_B = 4$. Note that in this case, the parameters $d$ and $G$ are fixed to legitimate values.

Figure A1. SCCQ protocol based on plug-and-play configuration using homodyne detection with a practical detector, $d = 50$, $G = 1$.

Figure A2. SCCQ protocol based on plug-and-play configuration using homodyne detection with a practical detector, $g = 1.005$, $G = 1$.

Figure A3. SCCQ protocol based on plug-and-play configuration using homodyne detection with a practical detector, $g = 1.005$, $d = 40$. 
The plot of Figure A2 illustrates the relationship between secret key rate and modulation $V_B$ under different values of distance $d$. We find that the peak value of secret key rate can be obtained when Bob’s modulation is about 4. In other words, the optimal value of $V_B$ in this case is 4.

Furthermore, Figure A3 shows the relationship between secret key rate and modulation $V_B$ with different gains of the amplifiers. Here, the optimal value of Bob’s modulation $V_B$ is still about 4. That is to say that we achieve the same conclusion (optimal $V_B = 4$) as above.

In view of above analysis, we can achieve the optimal value of modulation $V_B$, namely, $V_B = 4$, which is deemed as a constant in our protocol.

Appendix B. Calculation of Asymptotic Secret Key Rate

Here, we calculate the asymptotic secret key rate with reverse reconciliation under the optimal collective attack, which is given by

$$K_{\text{asy}} = f I(A:B) - \chi_{AE}, \quad (A1)$$

where $f$ is the reconciliation efficiency, $I(A:B)$ represents the Shannon mutual information shared by Alice and Bob, and $\chi_{AE}$ represents the Holevo bound of the information between Eve and Alice.

The mutual information shared by Alice and Bob $I(A:B)$ is expressed as

$$I(A:B) = \frac{1}{2} \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}. \quad (A2)$$

The Holevo bound of the information between Eve and Alice $\chi_{AE}$ can be calculated by [26,27]

$$\chi_{AE} = \sum_{i=1}^{2} G(\nu_i - \frac{1}{2}) - \sum_{i=3}^{5} G(\nu_i - \frac{1}{2}), \quad (A3)$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2x$, and the symplectic eigenvalues $\nu_{1,2,3,4,5}$ are given by

$$\nu_{1,2} = \frac{1}{2} [A \pm \sqrt{A^2 - 4B}], \quad (A4)$$

where

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2, \quad (A5)$$

$$B = T^2(V \chi_{\text{line}} + 1)^2, \quad (A6)$$

$$\nu_{3,4} = \frac{1}{2} [C \pm \sqrt{C^2 - 4D}], \quad (A7)$$

where

$$C = \frac{AX_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})}, \quad (A8)$$

$$D = \frac{\sqrt{B}(V + \sqrt{B}X_{\text{hom}})}{T(V + \chi_{\text{tot}})}, \quad (A9)$$

$$\nu_5 = 1. \quad (A10)$$

Note that in the above equations, $V = V_B + 1$, the total channel-added noise $\chi_{\text{line}} = \frac{1}{T} - 1 + \zeta_t$ and the total noise referred to the channel input $\chi_{\text{tot}} = \chi_{\text{line}} + \frac{X_{\text{hom}}}{T}$. 
Appendix C. Secret Key Rate in the Finite-Size Scenario

For the proposed protocol, the finite-size secret key rate is expressed as [33,34]

\[ K_{\text{fini}} = \frac{n}{N} [fI(A : B) - \chi_{\epsilon_{\text{PE}}}(A : E) - \Delta(n)], \quad (A11) \]

where \( f \) and \( I(A : B) \) are as the same as the aforementioned definitions. Here, \( N \) stands for the total exchanged signals and \( n \) stands for the number of signals which is taken advantage of to derive QKD. The remaining signals \( r = N - n \) are utilized to estimate the parameter. \( \epsilon_{\text{PE}} \) represents the failure probability of parameter estimation and \( \chi_{\epsilon_{\text{PE}}}(A : E) \) represents the maximum of the Holevo information compatible with the statistics except with probability \( \epsilon_{\text{PE}} \). \( \Delta(n) \) is related to the security of the privacy amplification, which is given by

\[ \Delta(n) = (2\dim H_A + 3) \left( \sqrt{\frac{\log_2(2/e)}{n}} + \frac{2}{n} \log_2(1/\epsilon_{\text{PB}}) \right), \quad (A12) \]

where \( e \) and \( \epsilon_{\text{PB}} \) stand for the smoothing parameter and the failure probability of privacy amplification, respectively. In addition, \( H_A \) represents the Hilbert space corresponding to the Alice’s raw key. In our protocol, binary bits are taken advantage of to encode the raw key, thus we have \( \dim H_A = 2 \).

In the finite-size scenario, the covariance matrix \( \Gamma_{\epsilon_{\text{PE}}} \) needs to be calculated \( \chi_{\epsilon_{\text{PE}}}(A : E) \). Besides, \( \Gamma_{\epsilon_{\text{PE}}} \) minimizes the secret key rate with a probability of at least \( 1 - \epsilon_{\text{PE}} \). Here, \( r \) couples of correlated variables \( (x_i, y_i)_{i=1...r} \) are sampled to derive the covariance matrix \( \Gamma_{\epsilon_{\text{PE}}} \). Then, a normal model is used for these correlated variables, which is given by

\[ y = tx + z, \quad (A13) \]

where \( t = \sqrt{T} \) and \( z \) follow a centered normal distribution with variance \( \tilde{\psi}^2 = 1 + T \tilde{\xi}_t \). On the basis of Equation (A13), Alice and Bob’s data can be linked. The covariance matrix \( \Gamma_{\epsilon_{\text{PE}}} \) is given by

\[ \Gamma_{\epsilon_{\text{PE}}} = \begin{pmatrix} (V_B + 1)I_2 & t_{\text{min}}Z\tilde{\psi} \cr t_{\text{min}}Z\tilde{\psi} & (t_{\text{min}}^2V_B + \tilde{\psi}^2)I_2 \end{pmatrix}, \quad (A14) \]

where \( t_{\text{min}} \) and \( \tilde{\psi}_{\text{max}}^2 \) represent the minimum of \( t \) and maximum of \( \tilde{\psi}^2 \) compatible with sampled couples except with probability \( \epsilon_{\text{PE}}/2 \), and \( Z = \sqrt{V_B^2 + 2V_B} \). Here, we denote the Maximum-likelihood estimators as \( \hat{t} \) and \( \hat{\tilde{\psi}}^2 \), which can be, respectively, expressed by

\[ \hat{t} = \frac{\sum_{i=1}^r x_i y_i}{\sum_{i=1}^r x_i^2} \quad \text{and} \quad \hat{\tilde{\psi}}^2 = \frac{1}{r} \sum_{i=1}^r (y_i - \hat{t}x_i)^2. \quad (A15) \]

According to this, \( t_{\text{min}} \) (the minimum of \( t \)) and \( \tilde{\psi}_{\text{max}}^2 \) (the maximum of \( \tilde{\psi}^2 \)) can be derived by

\[ t_{\text{min}} \approx \hat{t} - \frac{\tilde{\psi}_{\text{max}}}{2} \sqrt{\frac{\hat{\tilde{\psi}}^2}{rV_B}}, \]

\[ \tilde{\psi}_{\text{max}}^2 \approx \hat{\tilde{\psi}}^2 + \frac{\tilde{\psi}_{\text{max}}}{2} \sqrt{\frac{\hat{\tilde{\psi}}^2}{r}}, \quad (A16) \]

where \( \tilde{\psi}_{\text{max}}/\sqrt{2} \) is such that \( 1 - \text{erf}(\tilde{\psi}_{\text{max}}/\sqrt{2})/2 = \epsilon/2 \), and \( \text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt \) stands for error function. In order to theoretically analyze our protocol, the expected values of \( \hat{t} \) and \( \hat{\tilde{\psi}}^2 \) are, respectively, given by
\[ E[\hat{t}] = \sqrt{T}, \]
\[ E[\hat{\psi}^2] = 1 + T\zeta_t. \] (A17)

Then, we can calculate \( t_{\text{min}} \) and \( \psi_{\text{max}}^2 \) as follows:

\[
t_{\text{min}} \approx \sqrt{T} - z_{\epsilon_{PE}}/2 \sqrt{1 + T\zeta_t}/\sqrt{V_B},
\]
\[
\psi_{\text{max}}^2 \approx 1 + T\zeta_t + z_{\epsilon_{PE}}/2 \sqrt{2(1 + T\zeta_t)}/\sqrt{r}. \] (A18)

The optimal value for the error probabilities can be taken as being

\[ \epsilon = \epsilon_{PE} = \epsilon_{PB} = 10^{-10}. \] (A19)

Then, the secret key rate in the finite-size scenario can be calculated by taking advantage of the derived bounds \( t_{\text{min}} \) and \( \psi_{\text{max}}^2 \).

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. Rev. Mod. Phys. 2002, 74, 145. [CrossRef]
2. Lo, H.-K.; Curty, M.; Tamaki, K. Secure Quantum Key Distribution. Nat. Photon. 2014, 8, 595. [CrossRef]
3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The Security of Practical Quantum Key Distribution. Rev. Mod. Phys. 2009, 81, 1301. [CrossRef]
4. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. Rev. Mod. Phys. 2012, 84, 621. [CrossRef]
5. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 2000, 85, 441. [CrossRef]
6. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. Science 1999, 283, 2050. [CrossRef] [PubMed]
7. Takeda, S.; Fuwa, M.; Van, L.P.; Furusawa, A. Entanglement Swapping between Discrete and Continuous Variables. Phys. Rev. Lett. 2015, 114, 100501. [CrossRef]
8. Huang, D.; Lin, D.; Wang, C.; Liu, W.Q.; Peng, J.Y.; Fang, S.H.; Huang, P.; Zeng, G.H. Continuous-variable quantum key distribution with 1 Mbps secure key rate. Opt. Express 2015, 23, 17511. [CrossRef] [PubMed]
9. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. High-rate measurement-device-independent quantum cryptography. Nat. Photon. 2015, 9, 397. [CrossRef]
10. Huang, D.; Huang, P.; Li, H.; Wang, T.; Zhou, Y.; Zeng, G. Field demonstration of a continuous-variable quantum key distribution network. Opt. Lett. 2016, 41, 3511. [CrossRef]
11. Grosshans, F.; Van A.G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. Nature 2003, 421, 238. [CrossRef] [PubMed]
12. Wu, X.D.; Liao, Q.; Huang, D.; Wu, X.H.; Guo, Y. Balancing four-state continuous-variable quantum key distribution with linear optics cloning machine. Chin. Phys. B 2017, 26, 110304. [CrossRef]
13. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 2002, 88, 057902. [CrossRef]
14. Huang, P.; Fang, J.; Zeng, G. State-discrimination attack on discretely modulated continuous-variable quantum key distribution. Phys. Rev. A 2014, 89, 042330. [CrossRef]
15. Guo, Y.; Liao, Q.; Wang, Y.J.; Huang, D.; Huang, P.; Zeng, G.H. 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]
16. Huang, D.; Huang, P.; Lin, D.; Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci. Rep. 2016, 6, 19201. [CrossRef]
17. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys. Rev. A 2011, 84, 062317. [CrossRef]
18. Milicevic, M.; Chen, F.; Zhang, L.; Gulak, P.G. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. NPJ Quantum Inf. 2018, 4, 21. [CrossRef]
19. Wang, X.; Zhang, Y.; Yu, S.; Guo, H. High speed error correction for continuous-variable quantum key distribution with multi-edge type LDPC code. Sci. Rep. 2018, 8, 10543. [CrossRef] [PubMed]
20. Kikuchi, K. Fundamentals of coherent optical fiber communications. J. Lightwave Technol. 2016, 34, 157. [CrossRef]
21. Qi, B. Simultaneous classical communication and quantum key distribution using continuous variables. Phys. Rev. A 2016, 94, 042340. [CrossRef]
22. Qi, B.; Lim, C.C.W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. Phys. Rev. Appl. 2018, 9, 054008. [CrossRef]
23. Huang, D.; Huang, P.; Lin, D.-K.; Wang, C.; Zeng, G.-H. High-speed continuous-variable quantum key distribution without sending a local oscillator. Opt. Lett. 2015, 40, 3695. [CrossRef] [PubMed]
24. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the Local Oscillator Locally in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. Phys. Rev. X 2015, 5, 041009. [CrossRef]
25. Soh, D.B.S.; Brié, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar, M. Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. Phys. Rev. X 2015, 5, 041010. [CrossRef]
26. Huang, D.; Huang, P.; Wang, T.; Li, H.S.; Zhou, Y.M.; Zeng, G.H. Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol. Phys. Rev. A 2016, 94, 032305. [CrossRef]
27. Fossier, S.; Diamanti, E.; Debuisschert, T.; Tualle-Brouri, R.; Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J. Phys. B 2009, 42, 114014. [CrossRef]
28. Zhang, H.; Fang, J.; He, G. Improving the performance of the four-state continuous-variable quantum key distribution by using optical amplifiers. Phys. Rev. A 2012, 86, 022338. [CrossRef]
29. Guo, Y.; Li, R.J.; Liao, Q.; Zhou, J.; Huang, D. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifiers. Phys. Lett. A 2017, 382, 372–381. [CrossRef]
30. Subacius, D.; Zavrityev, A.; Trifonov, A. Backscattering limitation for fiber-optic quantum key distribution systems. Appl. Phys. Lett. 2005, 86, 011103. [CrossRef]
31. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. Nat. Commun. 2017, 8, 15043. [CrossRef] [PubMed]
32. Renner, R.; Cirac, J.I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Phys. Rev. Lett. 2009, 102, 110504. [CrossRef] [PubMed]
33. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of continuous-variable quantum key distribution. Phys. Rev. A 2010, 81, 062343. [CrossRef]
34. 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] [PubMed]