Research Article | Vol. 27, No. 9 | 29 Apr 2019 | OPTICS EXPRESS 13372

Optics EXPRESS

Realistic rate–distance limit of continuous-variable quantum key distribution

XUYANG WANG,[1,2,3] SIYOU GUO,[1] PU WANG,[1] WENYUAN LIU,[1] AND YONGMIN LI[1,2,*]

[1] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[2] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*
[3] *wangxuyang@sxu.edu.cn*
[*] *yongmin@sxu.edu.cn*

Abstract: Continuous variable quantum key distribution (CV QKD) is a promising candidate for the deployment of quantum cryptography. At present, the longest distance is limited to ~100 km at fiber-based quantum channel. We investigated in depth the realistic rate–distance limit (RDL) of CV QKD, considering reconciliation efficiency, finite-size effect, and realistic excess noise under collective attack. It is shown that the excess noise generated on Bob's side degrades significantly the transmission distance and we verify it in experiment. The improvement in RDL by reconciliation efficiency depends on the excess noise level, considerable increase of RDL by improving the reconciliation efficiency occurs only for relative large excess noises. A convergence modulation variance, useful in calculation simplification, is found. Furthermore, we restudy the finite-size analysis and eliminates a loophole arising from the Holevo-bound information monotonicity and a safe RDL is guaranteed. Based on the revised finite-size analysis, the optimum ratio determining the amount of data used for parameter estimation is analyzed.

1. Introduction

Quantum key distribution (QKD) allows two distant parties to share secret keys based on the laws of quantum physics. Eavesdropping on the key information are inevitably discovered, and the eavesdropped information can be eliminated to ensure security. This technology can provide an effective solution for high-security applications. Current QKD protocols can be divided into three categories [1–8]: discrete-variable (DV), continuous-variable (CV), and distributed phase-reference (DPR) protocols. The DV QKD protocol employs the discrete variables of a quantum state, such as the polarization or phase of single photons, whereas in the CV scheme, the key information is encoded in continuous variables, such as the quadratures of quantized electromagnetic modes (coherent states or squeezed states). The DPR coding scheme resorts to the phase difference between two successive signal pulses or the photon arrival times to encode the key information. In the paper, we focus on CV protocols.

Early CV protocols primarily focused on squeezed and entangled states [9–12]. In 2002, Grosshans and Grangier proposed the famous GG02 protocol [13], which realized QKD using only a coherent state instead of nonclassical states. Then reverse reconciliation method was designed to beat the 3-dB limit. In 2003, the GG02 protocol was demonstrated experimentally [14]; afterward, CV QKD entered a period of rapid development. Various protocols were proposed and realized experimentally [15–27]. Prototypes were also developed, and some field tests were reported [28–31]. At present, CV QKD can be realized using low-cost off-the-shelf components with good compatibility with classical communications. Thus, it is considered a promising candidate for enabling the deployment of quantum cryptography in future networks. Currently, the longest distance of CV QKD remains limited to ~100 km in experiments. The performance of the CV QKD system depends mainly on the reconciliation efficiency, finite-size effect, and

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

excess noise. In this work, we investigated in depth the realistic rate-distance limit (RDL) of CV QKD, considering reconciliation efficiency, finite-size effect, and realistic excess noise under collective attack.

At present, a reconciliation efficiency of 99%, near the Shannon limit, can be achieved [32]. In this study, it is found that improvements in the rate-distance limit (RDL) by increasing reconciliation efficiency depend on the excess noise. When the excess noise is larger, the improvement is more obvious. A convergence modulation variance is found and can be used to substitute the optimal modulation variance, especially for long transmission distances. Revisiting the finite-size effect, we reveal a loophole from the monotonicity of the Holevo bound. A safe and tight RDL is then used to ensure the security of system. The optimal ratio determining the amount of data used for parameter estimation is analyzed. The statistic effect and privacy amplification effect due to finite size are analyzed and we found that statistic effects are dominant. Based on a detailed investigation of the CV QKD system, we find that the excess noise generated on Bob's side is the main factor restricting the RDL and verify it in experiment. Finally, we discuss the possible ways to break the realistic RDL.

In Sec. 2, RDLs of several typical CV QKD protocols and the related experimental results are reviewed. In Sec. 3, the RDLs for different reconciliation efficiencies are analyzed. In Sec. 4, the finite-size effect on the RDL is analyzed. A loophole due to the monotonicity of the Holevo bound was revealed and eliminated and a safe and tight RDL was established. Section 5 focuses on the excess noise analysis model and the realistic RDL is presented. Finally, Sec. 6 presents the conclusions and the methods to break the realistic RDL are discussed.

2. Review of the RDL under realistic parameters

Presently, various CV QKD protocols have been proposed, such as one-way, two-way, and measurement-device-independent (MDI) protocols. Hereafter, we focus on the one-way coherent-state protocols that have been experimentally demonstrated in all-fiber systems. The secret key rate ΔI under collective attack and reverse reconciliation condition can be calculated by

$$\Delta I = \beta I_{AB} - \chi_{BE} \,, \tag{1}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, β is the reverse reconciliation efficiency, and χ_{BE} is the maximum information accessed by Eve bounded by the Holevo quantity. The RDLs of several typical protocols with realistic parameters in the asymptotic case are presented in Fig. 1, as well as some representative experimental results. Notably, only collective attack is considered in our study.

To achieve reasonable RDLs under realistic conditions, typical parameters are used: reconciliation efficiency $\beta = 0.95$, excess noise $\varepsilon = 0.01$ (shot noise units, SNU), detection efficiency $\eta = 0.6$, electronic noise $v_e = 0.1$, and a transmission loss of 0.2 dB/km. The modulation variance is optimized according to the transmission distance (or the transmission efficiency T). All variances are normalized to the shot noise N_0. The inset figure shows that the coherent-state protocol with heterodyne detection performs slightly better than the coherent-state protocol with homodyne detection (GG02 protocol) at a short distance. With increasing distance, their RDLs nearly converge. The unidimensional coherent-state protocol [26, 33] with advantages of easy modulation, low cost, and fewer random number requirements, has comparable performance with the above two-dimensional coherent protocols. The non-Gaussian-state protocols could realize high-speed gigahertz quantum communication using phase-shift keying technology [34]. It mainly includes two-state, four-state, and eight-state protocols. The number of states is larger, the performance is better. For eight-state protocol, the performance approaches the GG02 protocol [35]. Here, the typical four-state protocol is presented.

In Fig. 1, we can see that the transmission distances achieved in various experiments are less than 100 km, although the theoretical maximum transmission distance approaches ~400 km with

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

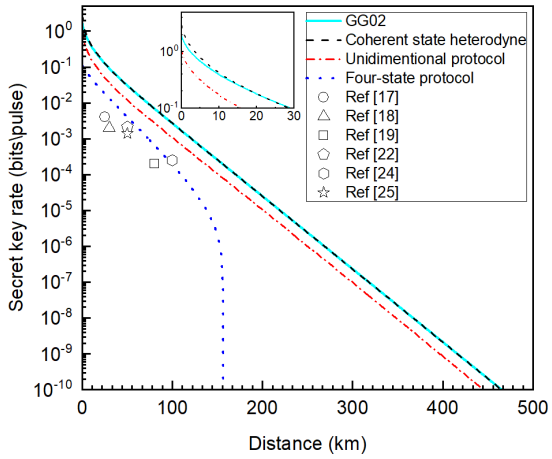

Fig. 1. RDLs and experimental results for typical CV QKD protocols.

the secret key rate of 10^{-9} in the asymptotic case. In this case, with a pulse rate of 1 GHz and secret key rate of 10^{-9}, a secret key bit rate of approximately 10 bit per second can be achieved. There is a large gap between the currently achieved distances of ~100 km and the theoretically maximum transmission distance of 400 km. In the following, we analyze three fundamental factors which affect the RDL.

3. Improvement in RDL by enhancing reconciliation efficiency

One method for improving the RDL is to enhance the reconciliation efficiency. The reconciliation efficiency recently reached 0.99 [32], which is close to the Shannon limit. In the following, we investigate the RDL of the GG02 protocol with different reconciliation efficiencies.

In Fig. 2, the red lines present the RDLs at a reconciliation efficiency of $\beta = 0.99$ under different excess noise levels. Comparing them to the blue lines representing the performance

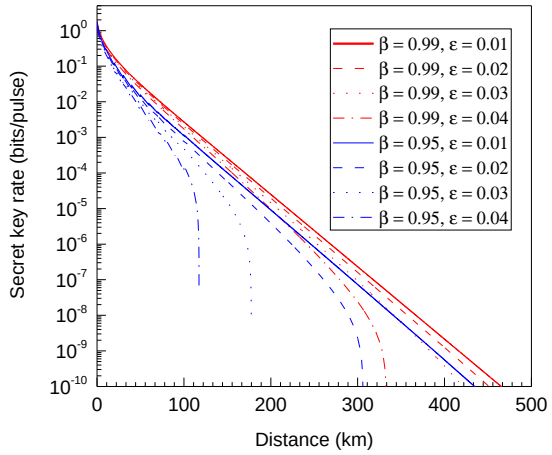

Fig. 2. RDLs at different reconciliation efficiencies of 0.99 (red lines) and 0.95 (blue lines).

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

at an efficiency $\beta = 0.95$, we observe that the improvement in the RDL is dependent on the excess noise level. When the excess noise is larger, the improvement of the performance is more obvious. Table 1 presents the performance improvement arising from the enhanced reconciliation efficiency (from 0.95 to 0.99) versus different excess noise levels at a constant distance or secret key rate. For fixed distances, the larger the excess noises, the better the secret key rate

Table 1. Performance improvement arising from the enhanced reconciliation efficiency (from 0.95 to 0.99) versus different excess noise levels at a constant distance or secret key rate.

Excess noise	The secret key rate ratio (dB)		Improved distance (km)	
(SNU)	@50 km	@100 km	@10^{-5} bit/pulse	@10^{-8} bit/pulse
0.01	2.99	3.88	21.6	26.1
0.02	3.45	4.93	31.5	67.9
0.03	4.03	6.78	52.7	164.4
0.04	4.81	11.97	84.3	193.2

improvement. The reason of this phenomena is because that higher excess noise degrades βI_{AB}, whereas increases χ_{BE}, which makes the value of the latter approaches that of the former. In this case, the enchancement of β is more favorable to the secret key rate improvement. It is also noted that for a constant secret key rate, the distance improvement is more evident for a higher excess noise level.

From Fig. 2, the decreased performance due to using lower reconciliation efficiency at the excess noise level 0.01 is not obvious. The theoretically achievable distance at $\beta = 0.95$ and $\varepsilon = 0.01$ is still far longer than the real transmission distance of ~100 km; therefore, we infer that the reconciliation efficiency is not the primary contributor to the largest achievable distance at $\varepsilon = 0.01$.

Usually in theoretical analysis, the reconciliation efficiency of 1 is used to achieve the best performance of a protocol. In this case, larger modulation variance is better. In the above analysis under realistic conditions, realistic efficiency of < 1 is used. In order to achieve the best performance, an optimal modulation variance is adopted according to the transmission distance. For sufficiently large distances, the optimal modulation variance converges to a constant value that depends on the reconciliation efficiency, as shown in Fig. 3(a).

Figure 3 presents the optimal modulation variance versus the transmission distance. In Fig. 3(a), from top to bottom, the reverse reconciliation efficiencies are 0.99, 0.97, 0.95, and 0.93, with convergence variances of 10.07, 5.20, 3.71, and 2.92, respectively. To plot Fig. 3(b), the same efficiency $\beta = 0.99$ is used for different excess noise levels. It is shown that the optimal modulation variance and convergence variance remain almost unchanged for different excess noise levels. Upon reaching a maximum transmission distance which depends on the excess noise levels, the convergence variances suddenly disappear at the stop lines, as marked in Fig. 3(b).

Figure 4 plots the RDLs with optimal modulation variances and convergence variances at different excess noise levels. We observe that little difference appears between the RDLs of the optimal modulation variance and the convergence variance at the same excess noise (Fig. 4(a)). Even for short distances, the difference is not significant, as shown in Fig. 4(b). In some cases, particularly for long transmission distances, the convergence variance can be used to simplify the calculation. In the following calculation considering the finite-size effect and realistic excess noise, the convergence modulation variance is used instead of the optimal modulation variance.

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

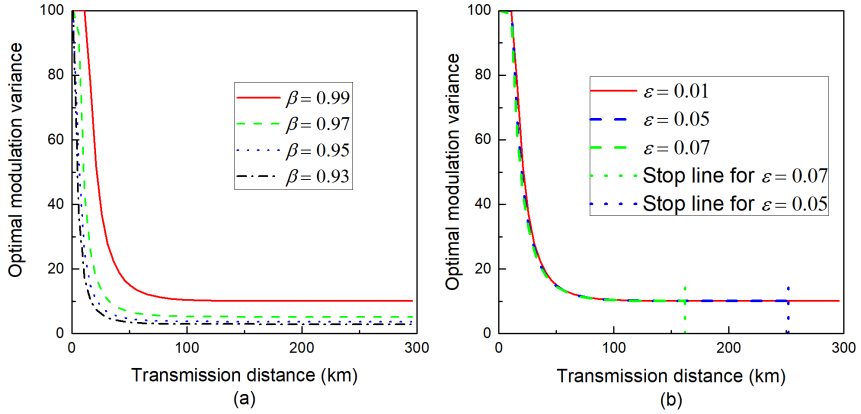

Fig. 3. Optimal modulation variance versus the transmission distance at different reconciliation efficiencies and different excess noise levels. (a) The curves at different reconciliation efficiencies where $\varepsilon = 0.01$. (b) The curves at different excess noise where $\beta = 0.99$.

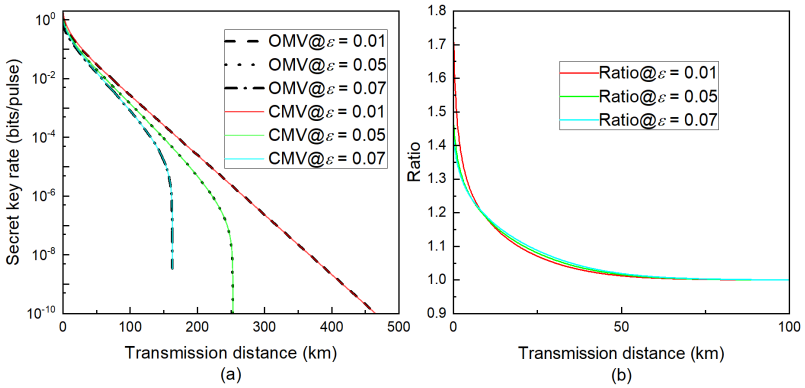

Fig. 4. The RDLs with optimal modulation variances and convergence variances at different excess noise levels. (a) The y-axis is the secret key rate. (b) The y-axis is the ratio of the secret key rate at optimal modulation variance (OMV) to that at convergence modulation variance (CMV).

4. RDL considering the finite-size effect

In the above analysis, we mainly consider the RDLs in the asymptotic case. As the total number of data samples in real scenarios is always finite, the finite-size effect must be considered. The expression used to calculate the secret key rate considering the finite-size effect is [33, 36–38]

$$\Delta I_{AB}^{f} = (n/N) \cdot \left(\beta I_{AB}^{\delta_{PE}} - \chi_{BE}^{\delta_{PE}} - \Delta(n, \delta_{PA}) \right), \tag{2}$$

where ΔI_{AB}^{f} is the secret key rate in a finite-size situation. δ_{PE} is the distribution probability of the estimated parameters such as the channel efficiency T and noise variance σ^2, that is beyond the confidence intervals when considering the finite-size effect. It is different from the asymptotic case in which the channel parameters can be perfectly estimated. In this case, the minimum Shannon mutual information $I_{AB}^{\delta_{PE}}$ and the maximum Holevo information $\chi_{BE}^{\delta_{PE}}$ can be calculated based on the confidence intervals of the estimated parameters.

n is the number of data samples used to distill the secret key rate, N represents the total

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

number of samples, and the rest of the data samples with numbers $m = N - n$ are used for parameter estimation. $\Delta(n, \delta_{PA})$ is a correction term for the achievable mutual information in the finite case, and δ_{PA} is the probability of an error during privacy amplification. Usually, conservative values of $\delta_{PE} = \delta_{PA} = 10^{-10}$ are utilized.

The monotonicity of information I_{AB} and χ_{BE} is the basis for analyzing the finite-size effect. In our review of the finite-size effect, we find that one assumption in the finite-size analysis is incorrect which generates a loophole. In the original analysis [34], a conclusion is achieved that the information χ_{BE} eavesdropped by Eve obeys the following inequalities:

$$\left.\frac{\partial \chi_{BE}}{\partial t}\right|_{\sigma^2} < 0 \text{ and } \left.\frac{\partial \chi_{BE}}{\partial \sigma^2}\right|_{t} > 0\,, \tag{3}$$

where the variable t is the square root of transmission efficiency T, $\sigma^2 = N_0 + \nu_e + \eta T \varepsilon$ is the noise variance of Bob's data. The variable η is the detection efficiency, N_0 is the shot noise, ν_e is the electronic noise, and ε is the excess noise. More details can be seen in [39]. However, through a detailed numerical analysis, we find that the curve representing Holevo information versus T is not monotonically decreasing. The calculation method in Appendix can be used to verify the convexity of χ_{BE}. Thus, we should restudy the finite-size effect.

The results of numerical calculations are presented in Fig. 5. The blue dot, black dashed,

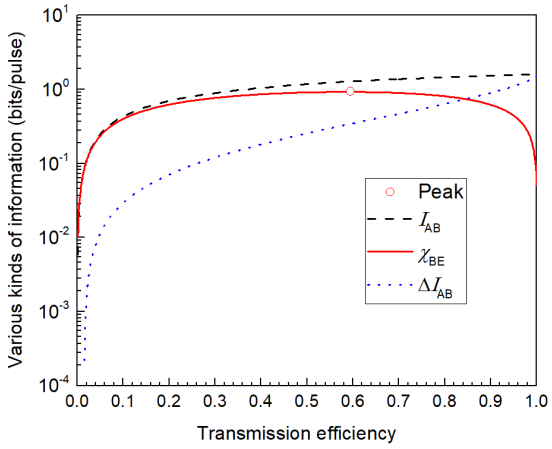

Fig. 5. Various kinds of information versus the transmission efficiency.

and red solid curves represent the secret key rate ΔI_{AB}, Shannon mutual information I_{AB}, and the Holevo bound information χ_{BE}, respectively. We can see clearly that χ_{BE} versus T is not monotonically decreasing. A red circle is used to mark the peak. The three curves are based on the condition that the variable σ^2 is constant.

To calculate the secret key rate, the variables t and σ^2 should be evaluated from the experiment data. Because of the finite-size effect, the estimated values $\hat{t}$ and $\hat{\sigma}^2$ may have any value in the confidence ranges $[t_{\min}, t_{\max}]$ and $[\sigma^2_{\min}, \sigma^2_{\max}]$, respectively, with the probability $1 - \delta_{PE}$. In order to calculate a safe secret key rate, calculating the maximum value of χ_{BE} should be divided into two situations because of its convex function character versus T. In this case, the expressions used to calculate the secret key rate in the regime of finite-size effect can be written as

$$\begin{cases} \Delta I^f_{AB} = \frac{n}{N}\left[\beta \cdot I_{AB}\left(t_{\min}, \sigma^2_{\max}\right) - \chi_{BE}\left(t_{\max}, \sigma^2_{\max}\right) - \Delta(n, \delta_{PA})\right], & t_{\max} < t_{\text{peak}} \\ \Delta I^f_{AB} = \frac{n}{N}\left[\beta \cdot I_{AB}\left(t_{\min}, \sigma^2_{\max}\right) - \chi_{BE}\left(t_{\min}, \sigma^2_{\max}\right) - \Delta(n, \delta_{PA})\right], & t_{\min} > t_{\text{peak}} \end{cases} \tag{4}$$

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

where t_{peak} is the square root of T_{peak}, which corresponds to T where Eve eavesdrops the maximum information. When the transmission efficiency is larger than t_{peak}, t_{min} is used to maximize the information χ_{BE}. When the transmission efficiency is smaller than t_{peak}, t_{max} is used to maximize the information χ_{BE}. If t_{peak} is located within $[t_{\text{min}}, t_{\text{max}}]$, we can move the value of t_{peak} out of the region by changing the modulation variance. On the other hand, the information χ_{BE} versus noise σ^2 is a monotonic increasing function, and σ^2_{max} is used in any case. Because the mutual information I_{AB} has the following properties

$$\left.\frac{\partial I_{AB}}{\partial t}\right|_{\sigma^2} > 0 \text{ and } \left.\frac{\partial I_{AB}}{\partial \sigma^2}\right|_{t} < 0\,, \tag{5}$$

Thus t_{min} and σ^2_{max} are used to calculate the minimum mutual information I_{AB} in any cases.

Using Eq. (4), safe and tight RDLs can be achieved as shown in Fig. 6(a). The dashed

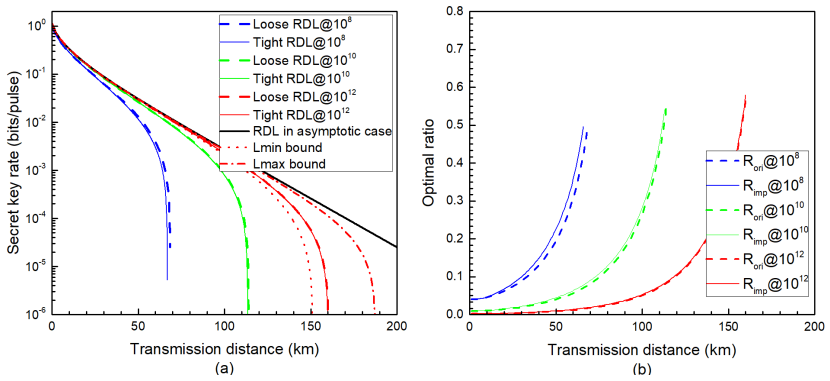

Fig. 6. (a) Tight and loose RDLs with different numbers of total samples. (b) The corresponding optimal ratio.

curves are loose RDLs, and the solid curves are tight RDLs. From left to right, the numbers of total samples are 10^8 (blue lines), 10^{10} (green lines), and 10^{12} (red lines). When the total number of samples is larger, the difference between the solid and dashed lines of the same color is minimized and the red dashed and solid lines nearly overlap. The black line represents the asymptotic case. Here, the tight or loose RDLs are drawn with optimal ratios, as shown in Fig. 6(b). The ratio is defined as dividing m by the total number N, where m is the amount of data used for the parameter estimation. When the distance or total number N varies, the optimal ratio R corresponding to the largest secret key rate varies accordingly. Here, the optimal ratio can be determined by scanning all possible ratios at a fixed distance and total number N. Obviously, the optimal ratio $R_{\text{imp}} = m/N$ with the improved tight calculation method has the same variation tendency as the ratio $R_{\text{ori}} = m/N$ in the original loose calculation method. Both ratios increase with increasing transmission distance for a constant number of total samples. For a fixed transmission distance, the optimal ratios decrease with increases in the number of total samples. This is a very useful rule in determining the number of data used for parameter estimation in experiment.

The solid lines in Fig. 6(a) only reflect the expected case $E(\hat{t})$ or $E(\hat{\sigma}^2)$. In fact the estimated values $\hat{t}$ or $\hat{\sigma}^2$ can take any values in the confidence regions $[t_{\text{min}}, t_{\text{max}}]$ and $[\sigma^2_{\text{min}}, \sigma^2_{\text{max}}]$ with a probability of $1 - \delta_{PE}$ in realistic conditions. For example, when the total number of samples is on the order of 10^{12}, the RDL should be distributed between the red dotted line (L_{min} bound) and the red dotted-dashed line (L_{max} bound). The longest transmission distance is nearly 190 km.

In the above, the finite-size effect is analyzed by analyzing two main factors simultaneously.

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

One is the statistics effect generated by $\beta I_{AB}^{\delta_{PE}} - \chi_{BE}^{\delta_{PE}}$; the other is the privacy amplification effect generated by $\Delta(n, \delta_{PA})$. In the following, we investigate the effect of them on the key rate individually. The reduction of the secret key rate due to the statistic effect is defined as

$$\Delta_{ST} = \beta I_{AB} - \chi_{BE} - \left(\beta I_{AB}^{\delta_{PE}} - \chi_{BE}^{\delta_{PE}}\right), \tag{6}$$

and the reduction of the secret key rate due to the privacy amplification effect is defined as

$$\Delta_{PA} = \Delta(n, \delta_{PA}) . \tag{7}$$

The total reduction is therefore

$$\Delta = \Delta_{PA} + \Delta_{ST} . \tag{8}$$

Then reduction ratios are defined by

$$R_{ST} = \Delta_{ST}/\Delta \text{ and } R_{PA} = \Delta_{PA}/\Delta . \tag{9}$$

Figure 7 plots the reduction ratios versus the transmission distance at different total numbers of samples. From left to right, the numbers of total samples of the blue, green, and red lines are 10^8, 10^{10}, and 10^{12}, respectively. The solid lines are the reduction ratios due to the statistics effect. The dot lines are the reduction ratios due to the privacy amplification effect. Comparing the solid and dashed lines, the statistic effect is more important than the privacy amplification effect. When the number of total samples is fixed, the ratios R_{ST} and R_{PA} decrease and increase, respectively, with the transmission distance. When the transmission distance is fixed, the ratios R_{ST} and R_{PA} increase and decrease, respectively, with the number of total samples.

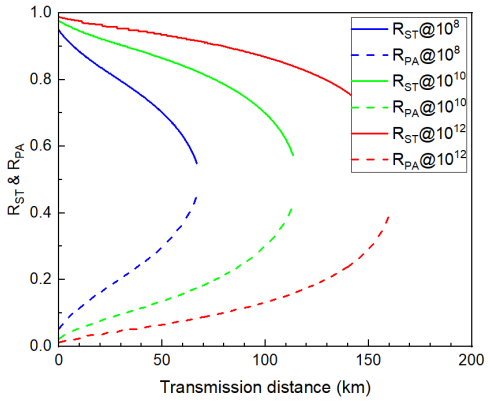

Fig. 7. The reduction ratios R_{ST} and R_{PA} versus the transmission distance with different total numbers of samples.

5. Realistic RDLs

In the above analysis, we can see that the finite-size effect play a key role in limiting the transmission distance. In this section, the RDLs considering realistic excess noise are analyzed and realistic RDLs are achieved.

In general, the estimated excess noise in CV QKD system increases with the distance. Controlling the excess noise to less than 0.01 for long transmission distances in experiments is

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

extremely challenging [19, 25]. It is shown that the excess noise ε_l from the fiber based quantum channel is usually small [40] and the excess noise ε_a generated on Alice's side is usually constant. In this case, we find that the excess noise ε_b generated on Bob's side mainly contribute to above phenomenon. The excess noise ε_b can be attributed to the measurement error, such as the error due to the fluctuations of the relative phase (between the signal and the local oscillator) and the drift of the homodyne output. To illustrate this question clearly, a typical model for describing Alice's and Bob's variable in CV QKD is as follows:

$$y = t \cdot x + z\,, \tag{10}$$

where the variable y represents the measured quadrature of the signal field by Bob, and its variance is denoted as V_B. The variable x is Alice's variable encoded on the quadrature of prepared quantum states, and its variance is V_M. The variable z follows a Gaussian distribution with the variance $\sigma^2 = \eta T\left(\varepsilon_a + \varepsilon_l\right) + \varepsilon_b + N_0 + \nu_e$ and a mean of zero, where the excess noise ε_b generated on Bob's side is introduced to reflect the measurement error. Eq. (10) can be transformed into a variance form as

$$V_B = \eta T V_M + \eta T\left(\varepsilon_a + \varepsilon_l\right) + \varepsilon_b + N_0 + \nu_e\,. \tag{11}$$

The realistic excess noise ε_r can be calculated by

$$\varepsilon_r = \left(\eta T\left(\varepsilon_a + \varepsilon_l\right) + \varepsilon_b\right)/\eta T = \varepsilon_a + \varepsilon_l + \varepsilon_b/\eta T\,. \tag{12}$$

Notably, the excess noise is referred to the input port of the channel for security. From Eq. (12), we can see that the excess noise increase with the transmission efficiency T and the detection efficiency η due to the term $\varepsilon_b/\eta T$. This is due to the fact that ε_b generated on Bob's side occurs after the transmission of the quantum state and thus doesn't attenuate with the channel transmission efficiency. When referred to the input port of the quantum channel, it will be amplified by a factor of $1/\eta T$. In order to verify the above theoretical analysis, the excess noises at different transmission distances were measured using a CV QKD prototype [30]. The traditional method to estimate the excess noise can be seen in [36]. In our experiment, the parameters are set to $V_M = 10$, $\nu_e = 0.1$, $\eta = 0.6$. The measurement results are shown in Table 2, from which we can see that the estimated excess noise increases with the transmission distance. For comparison, Fig. 8 shows the experimental outcomes (black square points) and the simulated realistic excess noise ε_r (cyan solid line) as a function of the transmission distance. The relevant parameters for simulation of ε_r are $\varepsilon_a + \varepsilon_l = 0.005$, $\varepsilon_b = 0.0005$, and $\eta = 0.6$. We find that the experimental results agree with the theoretical predictions approximately.

The realistic RDLs versus the distance for a GG02 protocol in both the asymptotic (black

Table 2. Excess noises at different transmission distances.

Distance (km)	0	20	50	80	100
Excess noise	0.00517	0.01337	0.01582	0.07212	0.09791
Standard Deviation	0.00233	0.0042	0.00972	0.02419	0.02916

dashed line) and finite-size cases (blue, green and red lines) are also illustrated in Fig. 8. For comparison, the performance of the system at a fixed excess noise of $\varepsilon = 0.01$ in asymptotic case is also presented (black solid line). For the realistic RDL, because the realistic excess noise rapidly increases with the transmission distance, the maximum transmission distance is limited to approximately 100 km. It is very different from the case with a fixed excess noise. The blue, green, and red lines are the conditions considering the finite-size effect. From left to right, the

#361145 https://doi.org/10.1364/OE.27.013372

Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

total numbers of samples are 10^8, 10^{10}, and 10^{12}, respectively. When the total number is 10^{12}, the red line nearly overlaps with the black dashed line, indicating that further increases in the total number of samples have no effect on the RDL. The results of Fig. 8 reflect the limitations of the CV QKD system under realistic excess noise.

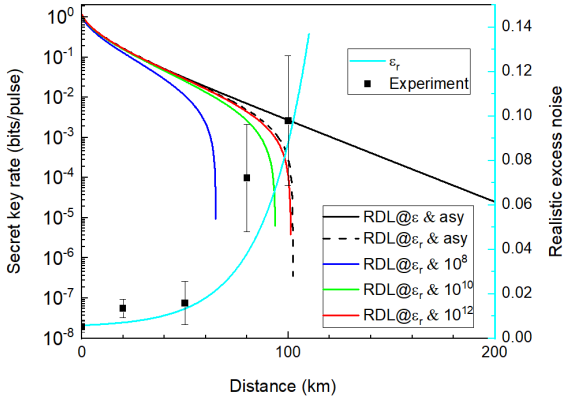

Fig. 8. Realistic excess noise and RDLs as a function of distance in asymptotic (asy) and finite-size cases.

6. Conclusions and discussion

In this study, we investigate the realistic RDL of CV QKD. At first, we present the RDLs considering the fixed excess noise and the experimental results of several typical protocols. Theoretical calculations indicate that the longest distance of 400 km can be achieved with a secret key rate of 10^{-9} bits/pulse. However, the real transmission distance is limited to ~100 km with the channel loss of 0.2 dB/km. In order to find the reasons for this gap, the RDLs considering reconciliation efficiency, finite-size effect, and realistic excess noise are analyzed under collective attack. We find that the improvement in RDL by enhancing reconciliation efficiency is dependent on the excess noise. If the excess noise is larger, the improvement is more obvious. The convergence modulation variance is found as a substitute for the optimal modulation variance, thus simplifying the calculation. Furthermore, the RDL considering the finite-size effect is restudied; a loophole due to the monotonicity of χ_{BE} is eliminated and a tight RDL is presented. The optimal ratios determining the number of data used to evaluate the parameters are analyzed in different conditions. The reduction ratios due to the statistic and privacy amplification effects are analyzed individually, we find that the statistical effect is more important than the privacy amplification effect. More importantly, the excess noise generated on Bob's side play a crucial role on the realistic RDL, which was verified by our experiment.

The above simulations are based on standard telecom single-mode fibers with a typical attenuation of 0.2 dB/km. If ultralow-loss fiber with attenuation of < 0.16 dB/km, or satellite-based free-space quantum communication technology are exploited, a longer distance could be anticipated. For future experimental research, some approaches can be attempted to break the realistic RDL, such as precisely calibrating the excess noise generated on Bob's side and attributing it to virtual electronic noise. Innovative methods to accurately characterize the excess noise of the system may also be developed. On the other hand, the realistic RDL in the regime of composable security against coherent attacks will be considered in a further theoretical analysis.

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

Appendix: calculation of the secret key rate

To calculate the secret key rate ΔI, an Entanglement-based scheme as shown in Fig. 9 was used. On Alice's side, an Einstein-Podolsky-Rosen (EPR) state ρ_{AB_0} is used. It can be determined by its covariance matrix γ_{AB_0}, with the following form

$$\gamma_{AB_0} = \begin{bmatrix} V \cdot I & \sqrt{V^2-1} \cdot \sigma_z \\ \sqrt{V^2-1} \cdot \sigma_z & V \cdot I \end{bmatrix}, \tag{13}$$

where

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{14}$$

After the transmission of mode B_0 through the channel characterized by efficiency T and

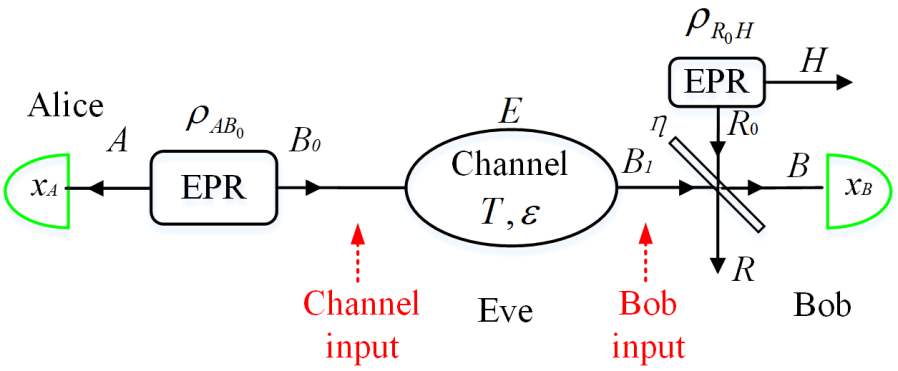

Fig. 9. Entanglement-based scheme.

excess noise ε , the covariance matrix γ_{AB_1} has the following form

$$\gamma_{AB_1} = \begin{bmatrix} V \cdot I & \sqrt{T\left(V^2-1\right)} \cdot \sigma_z \\ \sqrt{T\left(V^2-1\right)} \cdot \sigma_z & T\left(V+\chi_{\text{line}}\right) \cdot I \end{bmatrix}, \tag{15}$$

where $\chi_{\text{line}} = (1-T)/T + \varepsilon$ is the total noise added relative to channel input and $(1-T)/T$ is losses-induced vacuum noise. The balanced homodyne detector (BHD) with detection efficiency η can be model as a beam splitter with transmission η and a perfect BHD. The electronic noise v_e of it can be modelled by a thermal state ρ_{R_0} with variance V_N entering the other input port of the beam splitter, which is given by

$$V_N = 1 + v_e/(1-\eta). \tag{16}$$

The thermal state ρ_{R_0} could be considered as the reduced state obtained from an EPR state ρ_{R_0H}. Then the covariance matrix γ_{AB} characterizing the state ρ_{AB} after the beam splitter is given by

$$\gamma_{AB} = \begin{bmatrix} V \cdot I & \sqrt{\eta T\left(V^2-1\right)} \cdot \sigma_z \\ \sqrt{\eta T\left(V^2-1\right)} \cdot \sigma_z & T\left(V+\chi_{\text{tot}}\right) \cdot I \end{bmatrix}, \tag{17}$$

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

where $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T$ is the total added noise between Alice and Bob relative to the channel input, and $\chi_{\text{hom}} = (1-\eta)/\eta + v_e/\eta$ is the total noise introduced by the BHD relative to Bob's input.

Usually, the secret key rate considering reverse reconciliation under collective attack in the asymptotic limit can be calculated by the following expression

$$\Delta I = \beta I_{AB} - \chi_{BE}, \tag{18}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, β is the reverse reconciliation efficiency, and χ_{BE} is the maximum information accessed by Eve bounded by the Holevo quantity.

I_{AB} can be calculated directly using Shannon's equation as follows

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_A}{V_{A|B}}, \tag{19}$$

where V_A is the quadrature variance for Alice, being the diagonal element of matrix γ_A describing mode A . Further, $V_{A|B}$ is the conditional quadrature variance which is equal to the diagonal element of the conditional matrix $\gamma_{A|B}$ and given by

$$\gamma_{A|B} = \gamma_A - \sigma_{AB}\left(X\gamma_B X\right)^{MP}\sigma_{AB}^T, \tag{20}$$

where

$$X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; \tag{21}$$

γ_A , γ_B , and σ_{AB} are all submatrices of the covariance matrix γ_{AB} and appear in the decomposition of matrix γ_{AB} in Eq. (21); and MP represents the Moore-Penrose matrix inverse.

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB}^T & \gamma_B \end{bmatrix}. \tag{22}$$

Eve's accessible information can be calculated using

$$\chi_{BE} = S(\rho_E) - S\left(\rho_E^{x_B}\right), \tag{23}$$

where $S(\rho)$ is the von Neumann entropy of the quantum state ρ. For an n-mode Gaussian state ρ, this entropy can be calculated using the symplectic eigenvalues of the covariance matrix γ characterizing ρ as follows

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \tag{24}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. The symplectic eigenvalues of a covariance matrix γ with N modes can be calculated by finding the absolute eigenvalues of the matrix $i\Omega\gamma$.

As states ρ_{AB_1E} and $\rho_{ARHE}^{x_B}$ are pure, $S(\rho_E) = S\left(\rho_{AB_1}\right)$ and $S\left(\rho_{ARH}^{x_B}\right) = S\left(\rho_E^{x_B}\right)$. The entropy $S(\rho_{AB})$ can be calculated from the symplectic eigenvalues $\lambda_{1,2}$ of the covariance matrix γ_{AB}. In order to present the expression of $\lambda_{1,2}$ concisely, the covariance matrix γ_{AB} is rewritten as

$$\gamma_{AB} = \begin{bmatrix} a\cdot I & c\cdot\sigma_z \\ c\cdot\sigma_z & b\cdot I \end{bmatrix}. \tag{25}$$

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

From Eq. (24), the symplectic eigenvalues can be written as

$$\lambda_{1,2} = \sqrt{\frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4D^2}\right]}, \tag{26}$$

where

$$\Delta = a^2 + b^2 - 2c^2 \text{ and } D = ab - c^2. \tag{27}$$

Similarly, the entropy $S\left(\rho_{ARH}^{x_B}\right)$ can be determined from the symplectic eigenvalues $\lambda_{3,4,5}$ of the covariance matrix $\gamma_{ARH}^{x_B}$. The matrix $\gamma_{ARH}^{x_B}$ characterizing the state $\rho_{ARH}^{x_B}$ after Bob's projective measurement can be determined using the following equation

$$\gamma_{ARH}^{x_B} = \gamma_{ARH} - \sigma_{ARH;B}(X\gamma_B X)^{MP}\sigma_{ARH;B}^T. \tag{28}$$

Matrices γ_{ARH}, γ_B and $\sigma_{ARH;B}$ appear in the decomposition of matrix γ_{ARHB}, i.e. ,

$$\gamma_{ARHB} = \begin{bmatrix} \gamma_{ARH} & \sigma_{ARH;B} \\ \sigma_{ARH;B}^T & \gamma_B \end{bmatrix}, \tag{29}$$

which can be obtained by rearranging the lines and columns of matrix γ_{ABRH} describing the state ρ_{ABRH}. Specifically, γ_{ABRH} can be obtained by applying a beam splitter transformation $S_{B_1R_0}$ to modes B_1 and R_0, as follows

$$\gamma_{ABRH} = \left[I \oplus S_{B_1R_0} \oplus I\right]\left[\gamma_{AB_1} \oplus \gamma_{R_0H}\right]\left[I \oplus S_{B_1R_0} \oplus I\right]^T, \tag{30}$$

where

$$S_{B_1R_0} = \begin{bmatrix} \sqrt{\eta}I & \sqrt{1-\eta}I \\ -\sqrt{1-\eta}I & \sqrt{\eta}I \end{bmatrix}. \tag{31}$$

Finally, the symplectic eigenvalues $\lambda_{3,4,5}$ of the covariance matrix $\gamma_{ARH}^{x_B}$ can be derived as

$$\lambda_{3,4} = \sqrt{\frac{1}{2}\left[A \pm \sqrt{A^2 - 4B^2}\right]} \text{ and } \lambda_5 = 1, \tag{32}$$

where

$$A = \frac{1}{b + \chi_{\text{hom}}}\left[b + aD + \chi_{\text{hom}}\Delta\right] \text{ and } B = \frac{D}{b + \chi_{\text{hom}}}\left[a + \chi_{\text{hom}}\Delta\right]. \tag{33}$$

Base on the above expressions, we can calculate the Shannon mutual information I_{AB}, and the Holevo bound information χ_{BE}. Finally, the secret key rate can be obtained. Using these expressions we can conveniently verify the convexity of χ_{BE}.

Funding

National Key R&D Program of China (2016YFA0301403); National Natural Science Foundation of China (NSFC) (11504219, 61378010); Key Research and Development Projects of Shanxi Province (201803D121065); Shanxi 1331KSC.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, 1984), pp. 175–179.
2. V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

3. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**(2), 621–669 (2012).
4. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nat. Commun. **8**, 15043 (2017).
5. M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate-distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–407 (2018).
6. K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A **68**(2), 022317 (2003).
7. D. Stucki, N. Brunner, N. Gisin, V. Scarani and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87**(19), 194108 (2005).
8. D. Bacco, J. B. Christensen, M. A. U. Castaneda, Y. H. Ding, S. Forchhammer, K. Rottwitt, L. K. Oxenlowe, "Two-dimensional distributed-phase-reference protocol for quantum key distribution," Sci. Reports **6**, 36756 (2016).
9. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**(1), 010303(R) (1999).
10. N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of Gaussian keys using squeezed states," Phys. Rev. A **63**(5), 052311(2001).
11. D. Gottesman and J. Preskill, "Secure quantum key distribution using squeezed states," Phys. Rev. A **63**(2), 022309 (2001).
12. C. Silberhorn, N. Korolkova, and G. Leuchs, "Quantum key distribution with bright entangled beams," Phys. Rev. Lett. **88**(16), 167902 (2002).
13. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**(5), 057902 (2002).
14. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
15. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," Phys. Rev. Lett. **93**(17), 170504 (2004).
16. R. García-Patrón and N. J. Cerf, "Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**(19), 190503 (2006).
17. J. Lodewyck, M.Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**(4), 042305 (2007).
18. X. Y. Wang, Z. L. Bai, S. F. Wang, Y. M. Li, and K. C. Peng, "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise," Chin. Phys. Lett. **30**(1), 010305 (2013).
19. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
20. R. kumar, H. Qin, R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," New J. Phys. **17**(4), 043027 (2015).
21. V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**(6), 062337 (2015).
22. C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel," Sci. Rep. **5**, 14607 (2015).
23. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "Locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**(4), 041009 (2015).
24. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
25. X. Y. Wang, W. Y. Liu, P. Wang, and Y. M. Li, "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution," Phys. Rev. A **95**(6), 062330 (2017).
26. S. Fossier, E. Diamanti, T. Debuisschert, A Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**(4), 045023 (2009).
27. N. Wang, S. N. Du, W. Y. Liu, X. Y. Wang, Y. M. Li, K. C. Peng, "Long-Distance Continuous-Variable Quantum Key Distribution with Entangled States," Phys. Rev. Applied **10**(6), 064028 (2018).
28. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, "Field test of classical symmetric encryption with continuous variables quantum key distribution," Opt. Express **20**(13), 14030–14041 (2012).
29. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett. **41**(15), 3511–3514 (2016).
30. Y. M. Li, X. Y. Wang, Z. L. Bai, W. Y. Liu, S. S. Yang, and K. C. Peng, "Continuous variable quantum key distribution," Chin. Phys. B. **26**(4), 040303 (2017).
31. F. Karinou, H. H. Brunner, C. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, C. X, M. Peev, A. Poppe, "Toward the integration of CV quantum key distribution in deployed optical networks," IEEE Photonic Tech. Lett. **30**(7), 650–653 (2018).
32. M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," NPJ Quantum Inf. **4**, 21 (2018).
33. P. Wang, X. Y. Wang, J. Q. Li, and Y. M. Li, "Finite-size analysis of unidimensional continuous-variable quantum

#361145 https://doi.org/10.1364/OE.27.013372
Journal © 2019 Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019

Optics EXPRESS

key distribution under realistic conditions," Opt. Express **25**(23), 27995–28009 (2017).
34. Z. Qu, I. B. Djordjevic, and M. A. Neifeld. "RF-subcarrier-assisted four-state continuous variable QKD based on coherent detection," Opt. Lett. **41**(23), 5507–5510 (2016).
35. A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation," Phys. Rev. A **83**(4), 042312 (2011).
36. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**(6), 062343 (2010).
37. P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables," Phys. Rev. A **96**(4), 042332 (2017).
38. X. Y. Zhang, Y. C. Zhang, Y. J. Zhao, X. Y. Wang, S. Yu, and H. Guo, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," Phys. Rev A **96**(4), 042334 (2017).
39. P. Jouguet, S. K. Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**(3), 032309 (2012).
40. J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Controlling excess noise in fiber-optics continuous-variable quantum key distribution," Phys. Rev. A **72**(5), 050303(R) (2005).

#361145 https://doi.org/10.1364/OE.27.013372

Received 27 Feb 2019; revised 14 Apr 2019; accepted 15 Apr 2019; published 25 Apr 2019