ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

# Finite-size analysis of continuous-variable quantum key distribution with entanglement in the middle

Ying Guo(郭迎), Yu Su(苏玉), Jian Zhou(周健), Ling Zhang(张玲), Duan Huang(黄端)

**Citation:**Chin. Phys. B . 2019, 28(1): 010305. **doi:** 10.1088/1674-1056/28/1/010305
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

**What follows is a list of articles you may be interested in**

---

## Noiseless linear amplification for the single photon entanglement of arbitrary polarization-time-bin qudit

Ling-Quan Chen(陈灵泉), Yu-Bo Sheng(盛宇波), Lan Zhou(周澜)
Chin. Phys. B . 2019, 28(1): 010302. **doi:** 10.1088/1674-1056/28/1/010302

## Finite-size analysis of eight-state continuous-variable quantum key distribution with the linear optics cloning machine

Hang Zhang(张航), Yu Mao(毛宇), Duan Huang(黄端), Ying Guo(郭迎), Xiaodong Wu(吴晓东), Ling Zhang(张玲)
Chin. Phys. B . 2018, 27(9): 090307. **doi:** 10.1088/1674-1056/27/9/090307

## Continuous-variable quantum key distribution based on continuous random basis choice

Weiqi Liu(刘维琪), Jinye Peng(彭进业), Peng Huang(黄鹏), Shiyu Wang(汪诗寓), Tao Wang(王涛), Guihua Zeng(曾贵华)
Chin. Phys. B . 2018, 27(7): 070305. **doi:** 10.1088/1674-1056/27/7/070305

## Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle

Fang-Li Yang(杨芳丽), Ying Guo(郭迎), Jin-Jing Shi(石金晶), Huan-Li Wang(王焕礼), Jin-Jin Pan(潘矜矜)
Chin. Phys. B . 2017, 26(10): 100303. **doi:** 10.1088/1674-1056/26/10/100303

## Spherical reconciliation for a continuous-variable quantum key distribution

Zhao Lu(卢钊), Jian-Hong Shi(史建红), Feng-Guang Li(李风光)
Chin. Phys. B . 2017, 26(4): 040304. **doi:** 10.1088/1674-1056/26/4/040304

---

# Finite-size analysis of continuous-variable quantum key distribution with entanglement in the middle*

Ying Guo(郭迎)[1,2], Yu Su(苏玉)[2], Jian Zhou(周健)[2], Ling Zhang(张玲)[2], and Duan Huang(黄端)[2,†]

[1] School of Physics and Information Science, Hunan Normal University, Changsha 410006, China
[2] School of Automation, Central South University, Changsha 410083, China

(Received 26 June 2018; revised manuscript received 26 October 2018; published online 25 December 2018)

Continuous-variable quantum key distribution (CVQKD) protocols with entanglement in the middle (EM) enable long maximal transmission distances for quantum communications. For the security analysis of the protocols, it is usually assumed that Eve performs collective Gaussian attacks and there is a lack of finite-size analysis of the protocols. However, in this paper we consider the finite-size regime of the EM-based CVQKD protocols by exposing the protocol to collective attacks and coherent attacks. We differentiate between the collective attacks and the coherent attacks while comparing asymptotic key rate and the key rate in the finite-size scenarios. Moreover, both symmetric and asymmetric configurations are collated in a contrastive analysis. As expected, the derived results in the finite-size scenarios are less useful than those acquired in the asymptotic regime. Nevertheless, we find that CVQKD with entanglement in the middle is capable of providing fully secure secret keys taking the finite-size effects into account with transmission distances of more than 30 km.

**Keywords:** continuous-variable quantum key distribution, entanglement in the middle, finite-size, coherent attack

**PACS:** 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/28/1/010305

## 1. Introduction

Quantum key distribution (QKD) permits two authenticated partners Alice and Bob to share secret keys over an insecure quantum channel.[1,2] These keys can be applied to authenticate and encrypt. In theory, QKD provides unconditional security guaranteed by the Heisenberg uncertainty principle, which can ensure secure communication despite the existence of an eavesdropper called Eve. Two possible ways have been put forward to implement QKD. One is discrete-variable (DV) QKD which uses a single photon to encode the transmissive information,[3–5] and there have been increased experimental efforts in this area recently.[6–12] The other is continuous-variable (CV) QKD,[13–20] which encodes information in phase space ($\hat{x}$ and $\hat{p}$) and has attracted much attention.[21,22]

In CVQKD systems, secret information is encoded in the quadratures at Alice's side, and the receiver Bob can decode the information by performing homodyne detection or heterodyne detection with high efficiency.[23–25] Up to now, Gaussian-modulated coherent state CVQKD systems have been demonstrated to be secure against both collective and coherent attacks, and have also been proved to defend well against coherent attacks in a finite-size scenario by exploiting postselection technology[26] and an entropic uncertainty relationship.[27] The unconditional security of CVQKD based on a perfect optical source has also been researched in Refs. [28]– [34]. From the perspective of practical realizations, the CVQKD scheme has the potential to integrate with a telecommunication network since standard optical telecommunication technologies are applicable for CVQKD. However, a chief limitation of CVQKD protocols is the secure transmission distance. There are several approaches to settling the matter. The first is to find or design a suitable error correcting code, like LDPC codes, to enhance the reconciliation efficiency,[35–37] which can lead to a significant improvement in the transmission distance under low signal-to-noise ratio scenarios. The second solution is to employ a better performance protocol such as the entanglement in the middle (EM)-based CVQKD protocol.[38]

In contrast to the point-to-point CVQKD, in the EM-based CVQKD, the entangled resource that is placed between Alice and Bob is created by an untrusted third party Charlie, and even probably by Eve. For all these, secure keys can still be generated between Alice and Bob to encrypt information. Furthermore, this protocol has been proved to improve the transmission distance significantly. Consequently, the better performance of the protocol has attracted increasing attention.[39] However, a problem that cannot be neglected is that Eve controls the entangled source, which means that Eve can perform any type of attack, including collective and coherent attacks, in this protocol. So it is necessary to analyze the security under both types of attack. Similarly to the device-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61572529, 61871407, and 61801522) and the China Postdoctoral Science Foundation (Grant Nos. 2013M542119 and 2014T70772).

†Corresponding author. E-mail: duanhuang@csu.edu.cn

© 2019 Chinese Physical Society and IOP Publishing Ltd 

independent (DI) CVQKD protocols which provide a way for Alice and Bob to share keys without understanding the inner workings of the device or even the dimension of the space in which the quantum state is located,[40,41] this entangled protocol has been proposed to create a secret relationship between two legal parties Alice and Bob.

When it comes to security analysis of EM-based CVQKD protocols, there is a lack of security in the finite-size case. As a matter of fact, when we make an assumption that only a limited number of signals are swapped between Alice and Bob, it is obviously that the key rate will go down. Even so, finite-size analysis is a necessary step towards more general safety certification in the composable framework.[27,42,43] While theoretical research on the effects of finite-size has been completed in previous works,[44–47] there are no results proposed yet which are relevant to finite-size in the EM-based CVQKD protocol.

In order to optimize the security analysis of the protocols, in this paper we consider the security of entangling sources in the middle in a finite-size scenario. Since Eve controls the entangled source, Eve could prepare any arbitrary type of attack that she wants. Therefore, both collective and coherent attacks are taken into account in the security analysis of the protocol. For a single channel, a Gaussian collective attack maximizes the eavesdropper's extractable information. Because of the particularity of the protocols of entanglement in the middle, the effects of coherent attacks are more powerful when two channels are available. To make the security analysis more practical and realistic, the finite-size effects are taken into consideration during the parameter estimation procedures. Both symmetric and asymmetric configurations are collated in a contrastive analysis. Differently from DI CVQKD protocols, EM-based CVQKD must have perfect control of their measurement devices and must focus on building secret relationships by employing a source of entanglements transmitted from the middle to the remote legitimate ends, whereas DI QKD is typical of a relaxation of security hypotheses made in general QKD,[48] aiming to design encryption protocols to prevent increasingly powerful eavesdroppers. The EM-based CVQKD has its own merits, and is easier to implement in practice compared to DI QKD.

This paper is organized as follows. A detailed description of the entanglement in the middle CVQKD protocol against two-mode Gaussian attacks is given in Section 2. In Section 3, we analyze the security of the protocol and calculate the key rate in the asymptotic regime. In Section 4, the calculation process of the secret key rate considering finite-size effects is depicted in detail. Simulation results and analysis are given in Section 5. Finally, Section 6 presents conclusions.

## 2. CVQKD protocol with entanglement in the middle

As shown in Fig. 1, we suggest CVQKD with entanglement in the middle. The entangled resource that is placed between Alice and Bob is created by the third party Charlie, which may be attacked by Eve. The resource is used to generate a secure key and encrypt data. In the process of transmission, there is a high probability of being attacked by Eve. Eve's attacks include two entangled clones on both sides of the source. We assume that Eve's attacks are Gaussian attacks, because Gaussian attacks can acquire the most information in the protocols. Eve may employ her own quantum channel to substitute the quantum channel between Alice and Bob to eavesdrop on the communication message. At the same time, the loss channels have the transmissions $T_1$ (for Alice's link) and $T_2$ (for Bob's link), respectively. For $T_1 = 1$, it can be reverted to the traditional point-to-point case that Alice is the entangled resource. In the middle, Charlie's (or Eve's) Einstein–Podolski–Rosen (EPR) state has two entangled modes, one for Alice and the other for Bob. The EPR state is produced by the combination of two single-mode squeezed states via a 50:50 beam splitter

$$\hat{X}_A = (\hat{X}_1 + \hat{X}_2)/\sqrt{2}, \quad \hat{X}_B = (\hat{X}_1 - \hat{X}_2)/\sqrt{2}. \tag{1}$$

and $V$ is the variance of the two entangled modes, i.e., $V = V(A) = V(B)$.

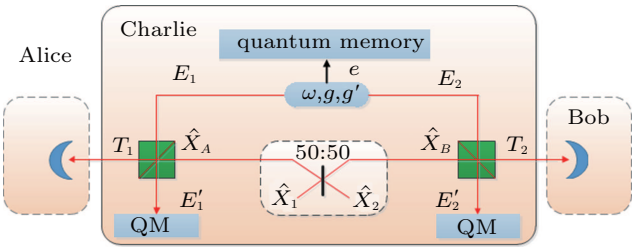



**Fig. 1.** EM-based CVQKD protocol, where the entangled source is placed in the middle between Alice and Bob. Alice performs heterodyne detection to detect one half of the EPR state, while Bob exploits homodyne detection to measure the other half of the EPR state. The Gaussian attack on the links is performed by Eve using ancillas $E_1$ and $E_2$.

Hereafter, we assume that Eve performs a coherent Gaussian attack, since this attack is more powerful than a collective Gaussian attack. The two-mode Gaussian attack is realized by two beam splitters. Employing the two beam splitters, the incoming modes $\hat{X}_A$ and $\hat{X}_B$ blend with two ancillary modes $E_1$ and $E_2$ which are extracted from a reservoir of ancillas. After the beam splitters, the output ancillas, $E_1'$ and $E_2'$, are stored in the quantum memory. Eve can measure the output ancillas $E_1'$ and $E_2'$ to steal information.

At the destination, Alice and Bob receive the information transmitted over the noisy channel, and then need to measure

the information they received via heterodyne detection or homodyne detection. For the measurement process, a local oscillator is required as a reference pulse. In addition, depending on the measurement, we also need to adjust the pulse from the local oscillator.

## 3. Security analysis

To derive the secret key rate in the finite-size analysis, we make an assumption that Eve performs a coherent Gaussian attack. We expound the procedures for computing the total covariance matrices and asymptotic secret key rate. However, what we achieved in the asymptotic regime is an ideal case. To fill the gap between theory and practice, we will obtain the secret key rate with finite-size effects in the next section.

### 3.1. Coherent Gaussian attack

The correlation of the two-mode Gaussian state $\rho_{E_1E_2}$ is described by covariance matrix (CM) given by

$$\gamma_{E_1E_2} = \begin{pmatrix} \omega_1 \boldsymbol{I} & \boldsymbol{G} \\ \boldsymbol{G} & \omega_2 \boldsymbol{I} \end{pmatrix}, \tag{2}$$

where $\boldsymbol{I} = \mathrm{diag}(1,1)$ and $\boldsymbol{G} = \mathrm{diag}(g,g')$. The parameter $\omega_1 \geq 1$ accounts for the variance of excess noise injected by $E_1$ in Alice's link, while $\omega_2 \geq 1$ is the variance of excess noise brought by $E_2$ in Bob's link. The parameters $g$ and $g'$ are correlated, demonstrating the two-mode correlations. For a physical attack, these parameters must satisfy the constraints given in Refs. [49] and [50]. By imposing the uncertainty principle,[49] we have the bona-fide conditions given by

$$|g| < \sqrt{\omega_1\omega_2}, \quad |g'| < \sqrt{\omega_1\omega_2}, \quad \nu^2 \geq 1, \tag{3}$$

where $\nu$ is the smallest symplectic eigenvalue. The symplectic eigenvalue of $\gamma_{E_1E_2}$ can be calculated as

$$\nu^2 = \frac{1}{2}(\chi - \sqrt{\chi^2 - 4\det\gamma_{E_1E_2}}), \tag{4}$$

where $\chi = \omega_1^2 + \omega_2^2 + 2gg'$. For $\nu^2 \geq 1$, we have $f(\omega_1,\omega_2,g,g') \geq 1$. Taking $g' = -g$, we have $f \geq 1$, corresponding to $|g'| \leq \phi$, where

$$\phi = \min\{\sqrt{(\omega_1-1)(\omega_2+1)}, \sqrt{(\omega_1+1)(\omega_2-1)}\}. \tag{5}$$

Based on the bona-fide conditions, by changing the values of $g$ and $g'$, we have different types of attack. As an example, for $g = g' = 0$, the two-mode Gaussian state $\rho_{E_1E_2}$ is a tensor product, leading to the standard Gaussian collective attacks which are realized by two independent entangling cloners. For $g \neq 0$ and $g' \neq 0$, Eve can perform a coherent attack, in which two entangling cloners are correlative (more details are shown in Appendix A).

### 3.2. The secret key rate in the asymptotic regime

The secret key rate of CVQKD protocols involves three factors in the asymptotic regime: the modulation variance $V$, the channel's transmissivity $T$, and the variance of excess noise $\omega$. The modulation variance $V$ is supposed to be a given parameter. Direct reconciliation is equivalent to reverse reconciliation in EM-based CVQKD protocols, so we will just consider the secret key rate for the reverse reconciliation

$$K = \beta \cdot S(A:B) - S(B:E), \tag{6}$$

where $\beta$ is the reconciliation efficiency, $S(A:B)$ is the Alice–Bob Shannon mutual information, and $S(B:E)$ represents the Shannon mutual information between Bob and Eve. The covariance matrix of the protocols is expressed as[51] (the detailed steps are shown in Appendix B)

$$\gamma_{AB} = \begin{pmatrix} a\boldsymbol{I} & c\boldsymbol{Z} \\ c\boldsymbol{Z} & b\boldsymbol{I} \end{pmatrix}, \tag{7}$$

where

$$a = VT_1 + (1-T_1)\omega_1, \tag{8}$$

$$b = VT_2 + (1-T_2)\omega_2, \tag{9}$$

$$c = \sqrt{V^2-1}\sqrt{T_1}\sqrt{T_2} + g\sqrt{1-T_1}\sqrt{1-T_2}. \tag{10}$$

The mutual information of Alice and Bob is defined when the EPR state is squeezed and homodyne measurement is performed

$$S(A:B) = \frac{1}{2}\log_2\frac{a}{a-c^2/b}. \tag{11}$$

Bob performs homodyne measurement, and Eve provides a purification of the whole system, so the formula for the Eve–Bob Shannon mutual information is

$$S(B:E) = S(E) - S(E|B) = S(AB) - S(A|B), \tag{12}$$

where $S(AB) = G[(\lambda_1-1)/2] + G[(\lambda_2-1)/2]$ and $S(A|B) = G[(\lambda_3-1)/2]$. The entropy function $G(x)$ is expressed as

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{13}$$

and the symplectic eigenvalues are given by

$$\lambda_{1,2}^2 = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D^2}], \tag{14}$$

where $\Delta = a^2 + b^2 - 2c^2$ and $D = ab - c^2$. To calculate $S(A|B)$, we work out Alice's correlation matrix on the basis of Bob's result of measurement $x_b$ or $p_b$. Assuming that the measurement result we have derived is $x_b$, it is employed according to the following formula:

$$\gamma_A^{x_b} = \gamma_A - \boldsymbol{\sigma}_{AB}^{\mathrm{T}}(\boldsymbol{X}\gamma_b\boldsymbol{X})^{-1}\boldsymbol{\sigma}_{AB}, \tag{15}$$

where $\boldsymbol{X} = \mathrm{diag}(1,0,1,0,\ldots,1,0)$. Consequently, $\lambda_3$ can be calculated via

$$\lambda_3^2 = a(a - c^2/b). \tag{16}$$

## 4. Performance analysis in finite-size scenarios

In QKD experiments, the transmission of a secret key is not unending. This means that Alice and Bob exchange finite signals. Moreover, only a portion of the transmitted signals are applied to extract the key and the rest are used for channel parameter estimation. In this case, we extend the parameter estimation[52] from the traditional point-to-point CVQKD protocols to the EM-based CVQKD protocols. To obtain the minimum key rate, we choose the minimum of the transmissivity and the maximum of excess noise.

### 4.1. Parameter estimation of transmissivity and excess noise

After the EPR states have been transmitted over the noisy channel, Alice and Bob's output variables $x_1$ and $x_2$ can be depicted by the following formulas:

$$x_1 = \sqrt{T_1}\hat{x}_A + x_{\mathrm{N1}}, \tag{17}$$

$$x_2 = \sqrt{T_2}\hat{x}_B + x_{\mathrm{N2}}, \tag{18}$$

where $x_{\mathrm{N1}}$ and $x_{\mathrm{N2}}$ are excess noise, and the variance $\mathrm{Var}(x_{\mathrm{N1}}) = \omega_1, \mathrm{Var}(x_{\mathrm{N2}}) = \omega_2$, $\mathrm{Var}(\hat{x}_A) = \mathrm{Var}(\hat{x}_B) = V$.

In the CVQKD protocols, there is no doubt that the influence of finite-size on the key rate is mainly reflected in parameter estimation. In the covariance matrix, except for the modulation variance of the entangled source, there are two unknown parameters: transmissivity and excess noise. The raw key is used for both parameter estimation and key generation, and we use $m$ to denote the number of parameter estimation signals. Let us estimate $T_1$ and $\omega_1$ first; $T_2$ and $\omega_2$ can be obtained by the same method. $A_i$ and $C_i$ $(i = 1, 2, \ldots, m)$ are the implementation of $x_1$ and $\hat{x}_A$, respectively. From Eq. (17), the transmissivity $T_1$ and the excess noise $\omega_1$ follow the relations

$$\hat{T}_1 = \frac{(\hat{C}_{CA})^2}{V^2}, \tag{19}$$

$$\hat{\omega}_1 = \frac{\sum_{i=1}^{m}(A_i - t_1 C_i)^2}{m}, \tag{20}$$

where the covariance $C_{CA} = \sqrt{T_1}V$ and its estimated value of the maximum likelihood is expressed as

$$\hat{C}_{CA} = \frac{\sum_{i=1}^{m} C_i A_i}{m}. \tag{21}$$

We can derive the variances of the estimated transmissivity $\hat{t}_1$ and the excess noise $\hat{\omega}_1$

$$\mathrm{Var}(\hat{T}_1) = \frac{4}{m}\cdot T_1^2\left(2 + \frac{\omega_1}{T_1 V}\right) =: \sigma_1^2, \tag{22}$$

$$\mathrm{Var}(\hat{\omega}_1) = \frac{2}{m}\cdot \omega_1^2. \tag{23}$$

Correspondingly, the estimated values of transmissivity $T_2$ and excess noise $\omega_2$ can be obtained through the same procedure

$$\mathrm{Var}(\hat{T}_2) = \frac{4}{m}\cdot T_2^2\left(2 + \frac{\omega_2}{T_2 V}\right) =: \sigma_2^2, \tag{24}$$

$$\mathrm{Var}(\hat{\omega}_2) = \frac{2}{m}\cdot \omega_2^2. \tag{25}$$

In the end, one can calculate $T_{1\min}, T_{2\min}$ and $\omega_{1\max}, \omega_{2\max}$ from

$$T_{1\min} = T_1 - 6.5\sigma_1, \quad T_{2\min} = T_2 - 6.5\sigma_2, \tag{26}$$

$$\omega_{1\max} = \omega_1 + 6.5\omega_1\sqrt{\frac{2}{m}}, \quad \omega_{2\max} = \omega_2 + 6.5\omega_2\sqrt{\frac{2}{m}}. \tag{27}$$

The estimated channel transmissivity and the corresponding excess noise are acquired, and thus the secret key rate in consideration of finite-size effects can be obtained.

### 4.2. Secret key rate with finite-size effects

Based on the estimated channel transmissivity and the corresponding excess noise, the secret key rate considering the finite-size effects is derived as

$$K_{\mathrm{f}} = \frac{n}{N}(K(V, T_{1\min}, T_{2\min}, \omega_{1\max}, \omega_{2\max}) - \Delta(n)), \tag{28}$$

where $N$ is the number of all signals swapped by Alice and Bob, $n$ is the number of signals used to extract the key, and the sifted key rate $n/N$ is $1/2$ in this scheme. The parameter $\Delta(n)$ is related to the privacy amplification of post-processing. We can incorporate the relationship into the following formula

$$\Delta(n) = 7\sqrt{\frac{\log_2(2/\varepsilon)}{n}}, \tag{29}$$

where $\varepsilon$ is a smoothing parameter.[47]

## 5. Numerical simulation results

According to the previous analysis, we can obtain a relation between the secret key rate and the related parameters. In Fig. 2, we plot the parameter $\Delta(n)$ as a function of $n$. As we can see from the figure, $\Delta(n)$ mainly depends on the size of raw key $n$, while the influence of $\varepsilon$ on $\Delta(n)$ is negligible. For $n = 10^8$, the value of $\Delta(n)$ can be reduced to 0.01.

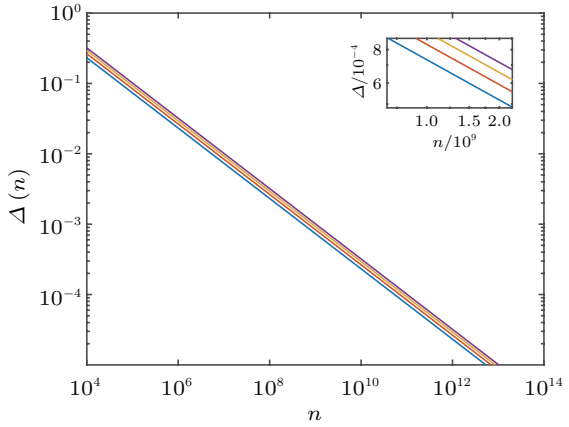



**Fig. 2.** The parameter $\Delta(n)$ as a function of $n$. Here, we take $\dim H = 2$, and from left to right, $\varepsilon = 10^{-7}, 10^{-8}, 10^{-9}, 10^{-10}$.

Figure 3 shows the relationship between parameter $g$ and the mutual information. We assume that parameter $g = g'$ in the attack implementation, and the channel loss is 0.8 dB. As shown in the simulation results, the parameter $g$ has an effect on the mutual information between Alice and Bob $S(A:B)$ and on the information hacking by Eve $S(B:E)$. As parameter $g$ increases, $S(A:B)$ increases, whereas $S(B:E)$ reduces. For $g = 0$, the two-mode Gaussian state $\rho_{E_1E_2}$ is a tensor product, leading to the standard Gaussian collective attacks which are realized by two independent entangling cloners. For coherent attacks, the value of $g$ is set as $-\sqrt{(\omega_1-1)(\omega_2+1)}$, which provides more eavesdropping information for Eve.

Figure 4(a) shows the performance of the EM-based CVQKD protocols against collective Gaussian attack with symmetric configuration, while figure 4(b) presents the protocols against collective Gaussian attack with asymmetric configuration, and the best performance among the four schemes is obtained. Figure 4(c) corresponds to the EM-based CVQKD protocols against coherent attack with symmetric configuration, and it has the worst performance when compared with the other three scenarios. Figure 4(d) shows the performance of the EM-based CVQKD protocols against coherent attack with asymmetric configuration. As far as we know, a Gaussian collective attack can extract the maximum information in the general protocols. However, in the protocol of entanglement in the middle, coherent attacks perform more powerfully than collective attacks as shown by comparing Fig. 4(a) with Fig. 4(c). Under the same conditions, the secret key rates of the EM-based CVQKD protocol under coherent attack are inferior to those under collective attack. We can observe that the secret key rates in the finite-size scenarios are lower than those in the asymptotic regime. And with the increase of block size, the key rates increase. By comparing Fig. 4(a) with Fig. 4(b) or Fig. 4(c) with Fig. 4(d), we can derive that the asymmetric configuration can put up with more losses than the symmetric configuration.

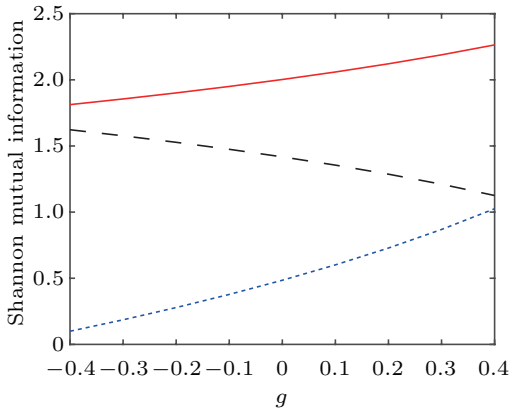



**Fig. 3.** The relationship between parameter $g$ and the mutual information. Solid red line denotes the mutual information between Alice and Bob $S(A:B)$. Large dashed black line denotes the information eavesdropped by Eve $S(B:E)$. Small dashed blue line denotes the secret key rate $K$. The modulation variance $V$ is 10, the reconciliation efficiency is 0.95, and the channel loss is 0.8 dB. The $\omega_1$ and $\omega_2$ are set as 1.1.

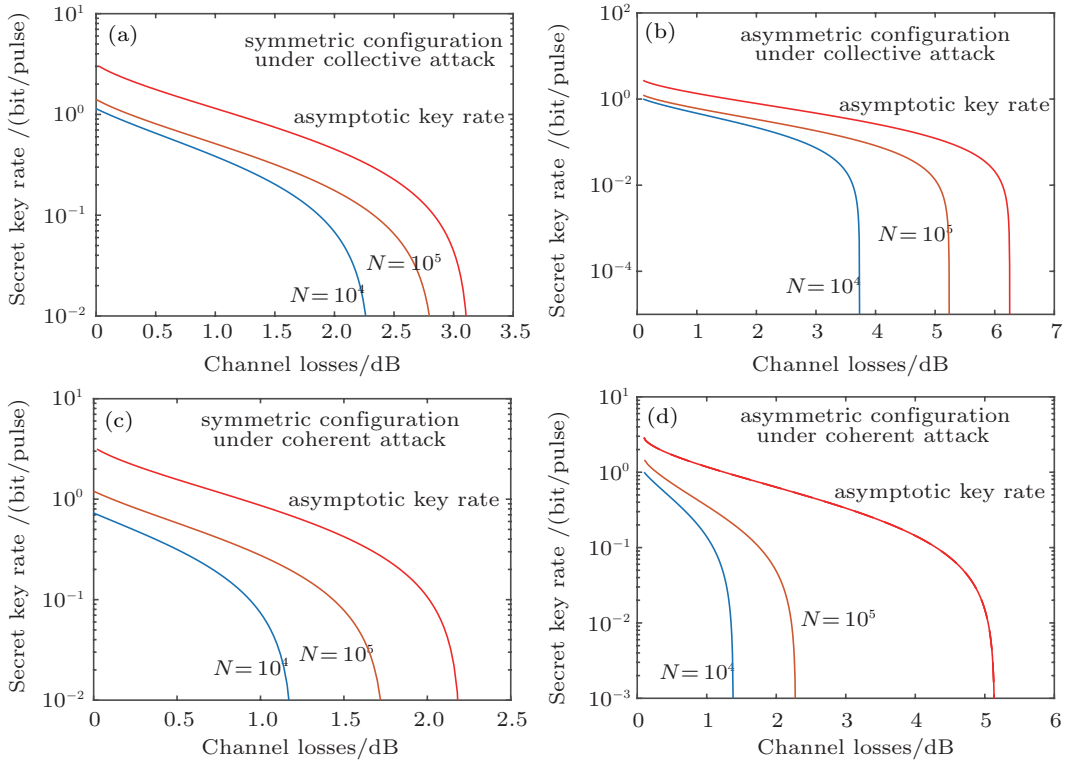



**Fig. 4.** (a) Secret key rate under Gaussian collective attack with symmetric configuration. (b) Secret key rate under collective Gaussian attack with asymmetric configuration. (c) Secret key rate under coherent attack with symmetric configuration. (d) Secret key rate under coherent attack with asymmetric configuration. In the asymmetric configuration, the entangled source is placed near Alice with $T_1 = 0.99$. For the coherent attack, the value of $g$ is $-\sqrt{(\omega_1-1)(\omega_2+1)}$. The blue line, orange line and red line represent the block lengths of $N = 10^4$, $10^5$ and $\infty$, respectively. The modulation variance $V$ is 10, the reconciliation efficiency is 0.95, the theoretical excess noise is set as 1.1, the security parameter $\varepsilon$ is set as $10^{-10}$, and $\eta = n/N = 0.5$.

Figure 5(a) shows the secret key rates as a function of losses and excess noise against collective attack, while figure 5(b) presents the performance of the protocols considering the parameters of loss and excess noise under coherent attack. The modulation variance $V$ is 10, the reconciliation efficiency is 0.95, and the security parameter $\varepsilon$ is set as $10^{-10}$. Through simulation, we can conclude that the secret key rates are not only associated with the channel losses, but also with the excess noise. Moreover, when the excess noise has a slight change, the secret key rates under coherent attacks will be significantly changed. While Eve performs collective attacks, the secret key rates are not as affected by excess noise as they are under coherent attacks. These results further indicate that coherent attacks can extract more information than collective attacks in the protocols.

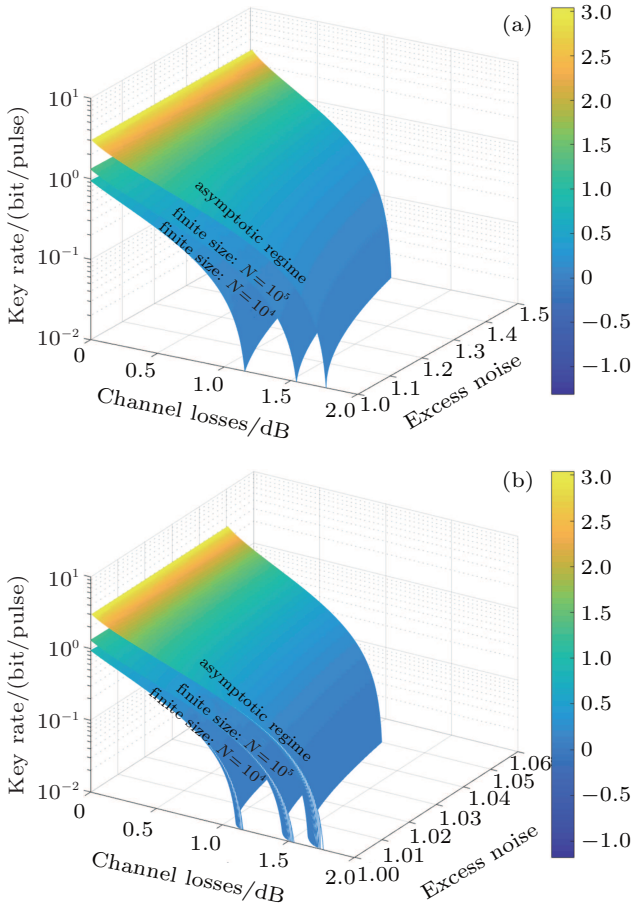



**Fig. 5.** (a) Secret key rate under collective attacks. (b) Secret key rate under coherent attacks. In both figures, from top to bottom, the block lengths $N=\infty$, $10^5$ and $10^4$. The modulation variance $V$ is 10, the reconciliation efficiency is 0.95, and the security parameter $\varepsilon$ is set as $10^{-10}$.

## 6. Conclusion

We have studied the EM-based CVQKD protocols, focusing on their security against collective attack and coherent attack in finite-size scenarios. This happens when the two parties exchange a limited number of signals in the quantum communication stage. In our analysis, we assume that the reconciliation efficiency is less than 1, meaning that the error correction and privacy amplification are imperfect. In the EM-based CVQKD protocols, the entangled source is created by an untrusted third party which might be controlled by Eve, so that Eve can use various attack strategies. During the attack implementation, Eve prepares two entangled clones and then injects them into two quantum channels, respectively. By changing the correlation between the two entangled clones, Eve can employ different methods of attack to steal information. Our simulation results show that when Eve performs a Gaussian coherent attack, it can extract more information than a Gaussian collective attack in the protocols of entanglement in the middle. To take the worst case scenario into consideration, we assume that Eve performs coherent attacks, leading to a decline in realizable maximum transmission distance and secret key rate. The key rate in a finite-size scenario is inferior to that in the asymptotic regime. And the transmission distance can be improved in asymmetric configuration. Taking finite-size effects into account, when the size reaches $10^5$, the secret key rate can achieve $10^{-2}$ with transmission distances of more than 30 km under coherent attacks. Finally, we need to mention that what we have analyzed in this paper is not the final result of finite-size analysis on the CV-QKD protocols with entanglement in the middle. Further research into finite-size effects is needed in the composable security framework.[53]

## Appendix A: calculation of bona-fide conditions

Consider a two-mode CM of the form

$$\boldsymbol{V}=\begin{pmatrix}\omega_1 & 0 & g & 0\\ 0 & \omega_1 & 0 & g'\\ g & 0 & \omega_2 & 0\\ 0 & g' & 0 & \omega_2\end{pmatrix}, \tag{A1}$$

where $\omega_1,\omega_2$ are the variance of excess noise and $\omega_1,\omega_2\geq 1$. According to the uncertainty principle, we can derive the bona-fide conditions

$$\boldsymbol{V}>0,\ \ \nu^2\geq 1, \tag{A2}$$

where $\nu$ is the smallest symplectic eigenvalue. The formula for calculating the symplectic eigenvalue of $V$ is

$$\nu^2=\frac{1}{2}(\chi-\sqrt{\chi^2-4\det\boldsymbol{V}}), \tag{A3}$$

where $\chi=\omega_1^2+\omega_2^2+2gg'$.

The positivity of the matrix $\boldsymbol{V}$ is equal to the positivity of its principal minors. Through the conditions of $\omega_1\geq 1$ and $\omega_2\geq 1$, we can derive that the first two minors are positive. The third minor gives

$$\boldsymbol{V}_3=\begin{pmatrix}\omega_1 & 0 & g\\ 0 & \omega_1 & 0\\ g & 0 & \omega_2\end{pmatrix}, \tag{A4}$$

which satisfies the condition

$$\det\boldsymbol{V}_3>0\Leftrightarrow\omega_1(\omega_1\omega_2-g^2)>0, \tag{A5}$$

then, we can derive that

$$|g| < \sqrt{\omega_1 \omega_2}. \tag{A6}$$

Finally, the fourth minor corresponds to the determinant

$$\det \boldsymbol{V} = (\omega_1 \omega_2 - g^2)(\omega_1 \omega_2 - g'^2), \tag{A7}$$

in terms of positive condition $\det \boldsymbol{V} > 0$, and we calculate the condition that $g'$ has to satisfy

$$|g'| < \sqrt{\omega_1 \omega_2}. \tag{A8}$$

According to the condition $\nu^2 \geq 1$, we can derive an inequality $f(\omega_1, \omega_2, g, g') \geq 1$. The graph of this inequality is symmetric around the origin and the bisector $g' = -g$. On the bisector $g' = -g$, we have that $f \geq 1$ corresponds to $|g'| \leq \phi$, where

$$\phi = \min\{\sqrt{(\omega_1 - 1)(\omega_2 + 1)}, \sqrt{(\omega_1 + 1)(\omega_2 - 1)}\}. \tag{A9}$$

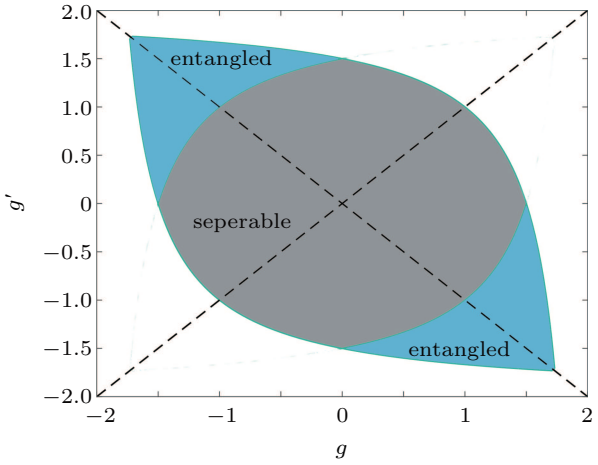



**Fig. A1.** Correlations between $g$ and $g'$ when the thermal noise $\omega_1 = \omega_2 = 2$. Points in the external white area are not accessible (having correlations too strong to be compatible with quantum mechanics). Accessible points (i.e., satisfying the bona-fide conditions) are represented by the delimited region, which is further divided in sub-regions. The gray area corresponds to separable attacks, while the two peripheral blue areas correspond to entangled attacks. The two dashed lines represent the two bisectors $g' = g$ and $g' = -g$.

The accessible region can be further divided into sub-regions according to the attacks performed with separable or entangled ancillas $E_1$ and $E_2$. In fact, we can easily write out the separability condition of $\rho_{E_1E_2}$ by considering the symplectic eigenvalue $\widetilde{\nu}$ of the minimum transposition. We can derive the positive eigenvalue

$$\widetilde{\nu}^2 = \frac{1}{2}(\widetilde{\chi} - \sqrt{\widetilde{\chi}^2 - 4\det \boldsymbol{V}}), \tag{A10}$$

where $\widetilde{\chi} = \omega_1^2 + \omega_2^2 - 2gg'$. Then we have $\rho_{E_1E_2}$ separable when $\widetilde{\nu} \geq 1$, and this leads to the corresponding inequality $\widetilde{f}(\omega_1, \omega_2, g, g') \geq 1$ which is symmetric around the origin and the bisector $g' = g$. As shown in Fig. A1, we call the inner area separable attacks where the attacks are performed with separable ancillas ($\widetilde{\nu} \geq 1$), while the two peripheral areas are called entangled attacks with the attacks performed with entangled ancillas ($\widetilde{\nu} < 1$).

In the area of separable attacks, when $g = g' = 0$, the two-mode Gaussian state $\rho_{E_1E_2}$ is a tensor product, corresponding to the standard Gaussian collective attacks which are realized by two independent entangling cloners. For entangled attacks, two entangling cloners are correlative. In the bottom-right region, we can obtain the positive EPR attack, which is the attack with the highest degree of entanglement when $g = -g' = \phi$. In the top-left region, the most entangled attack, the negative EPR attack, can be derived when $g = -g' = -\phi$.

## Appendix B: calculation of covariance matrix

The covariance matrix of the EPR state generated by Charlie can be given by

$$\gamma = \begin{pmatrix} V\boldsymbol{I} & \sqrt{V^2-1}\boldsymbol{Z} \\ \sqrt{V^2-1}\boldsymbol{Z} & V\boldsymbol{I} \end{pmatrix}, \tag{B1}$$

where $\boldsymbol{Z} = \mathrm{diag}(1, -1)$.

According to Eve's covariance matrix in Eq. (2), we obtain the CM of the incipient system

$$\gamma_1 = \gamma \oplus \gamma_{E_1E_2} = \begin{pmatrix} \gamma & 0 \\ 0 & \gamma_{E_1E_2} \end{pmatrix}. \tag{B2}$$

Eve's attack can be realized by two beam splitters. Employing the two beam splitters, the incoming modes $\hat{X}_A$ and $\hat{X}_B$ blend with two ancillary modes $E_1$ and $E_2$, resulting in the CM

$$\gamma_2 = \begin{pmatrix} V\boldsymbol{I} & 0 & \sqrt{V^2-1}\boldsymbol{Z} & 0 \\ 0 & \omega_1\boldsymbol{I} & 0 & \boldsymbol{G} \\ \sqrt{V^2-1}\boldsymbol{Z} & 0 & V\boldsymbol{I} & 0 \\ 0 & \boldsymbol{G} & 0 & \omega_2\boldsymbol{I} \end{pmatrix}. \tag{B3}$$

The transmittance matrix is given by

$$\gamma_{\mathrm{T}} = \begin{pmatrix} \sqrt{T_1}\boldsymbol{I} & \sqrt{1-T_1}\boldsymbol{I} & 0 & 0 \\ -\sqrt{1-T_1}\boldsymbol{I} & \sqrt{T_1}\boldsymbol{I} & 0 & 0 \\ 0 & 0 & \sqrt{T_2}\boldsymbol{I} & \sqrt{1-T_2}\boldsymbol{I} \\ 0 & 0 & -\sqrt{1-T_2}\boldsymbol{I} & \sqrt{T_2}\boldsymbol{I} \end{pmatrix}, \tag{B4}$$

where $T_1$ represents the transmissivity of the entangled source to Alice and $T_2$ represents the transmissivity of the entangled source to Bob.

After the output modes are transmitted to Alice and Bob over insecure channels, the CM is derived as

$$\gamma_3 = (\gamma_{\mathrm{T}})^{\mathrm{T}} \cdot \gamma_2 \cdot \gamma_{\mathrm{T}}. \tag{B5}$$

For $g = -g'$, the resulting CM can be calculated as

$$\gamma_{AB} = \begin{pmatrix} a\boldsymbol{I} & c\boldsymbol{Z} \\ c\boldsymbol{Z} & b\boldsymbol{I} \end{pmatrix}, \tag{B6}$$

where

$$a = VT_1 + (1-T_1)\omega_1, \tag{B7}$$

$$b = VT_2 + (1-T_2)\omega_2, \tag{B8}$$

$$c = \sqrt{V^2-1}\sqrt{T_1}\sqrt{T_2} + g\sqrt{1-T_1}\sqrt{1-T_2}. \tag{B9}$$

## References


[1] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[2] Zeng G H 2010 *Quantum Private Communication* (Berlin: Springer-Verlag Press) Chap. 3

[3] Takeda S, Fuwa M, van Loock P and Furusawa A 2015 *Phys. Rev. Lett.* **114** 100501

[4] Gessner M, Pezzé L and Smerzi A 2016 *Phys. Rev. A* **94** 020101

[5] Li H W, Zhao Y B, Yin Z Q, Wang S, Han Z F, Bao W S and Guo G C 2009 *Opt. Commun.* **20** 4162

[6] Wang S, Chen W, Yin Z Q, He D Y, Hui C, Hao P L, Fan-Yuan G J, Wang C, Zhang L J, Kuang J, Liu S F, Zhou Z, Wang Y G, Guo G C and Han Z F 2018 *Opt. Lett.* **43** 2030

[7] Wang S, Yin Z Q, Chau H F, Chen W, Wang C, Guo G C and Han Z F 2018 *Quantum Sci. Technol.* **3** 025006

[8] Yin Z Q, Wang S, Chen W, Han Y G, Wang R, Guo G C and Han Z F 2018 *Nat. Commun.* **9** 457

[9] Wang S, Yin Z Q, Chen W, He D Y, Song X T, Li H W, Zhang L J, Zhou Z, Guo G C and Han Z F 2015 *Nat. Photon.* **9** 832

[10] Wang C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2017 *Optica* **4** 1016

[11] Wang S, Chen W, Yin Z Q, Li H W, He D Y, Li Y H, Zhou Z, Song X T, Li F Y, Wang D, Chen H, Han Y G, Huang J Z, Guo J F, Hao P L, Li M, Zhang C M, Liu D, Liang W Y, Miao C H, Wu P, Guo G C and Han Z F 2014 *Opt. Express* **22** 21739

[12] Wang S, Chen W, Guo J F, Yin Z Q, Li H W, Zhou Z, Guo G C and Han Z F 2012 *Opt. Lett.* **37** 1008

[13] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621

[14] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[15] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238

[16] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504

[17] Guo Y, Xie C L, Huang P, Li J W, Zhang L, Huang D and Zeng G H 2018 *Phys. Rev. A* **97** 052326

[18] Gong L, Song H, He C, Liu Y and Zhou N 2014 *Phys. Scr.* **89** 035101

[19] Song H, Gong L, He C, Liu Y and Zhou N 2012 *Acta Phys. Sin.* **61** 154206 (in Chinese)

[20] Huang P, Fang J and Zeng G H 2014 *Phys. Rev. A* **89** 042330

[21] Ma H X, Bao W S and Li H W 2016 *Chin. Phys. B* **25** 080309

[22] Liu W Q, Peng J Y, Huang P, Huang D and Zeng G H 2017 *Opt. Express* **25** 19429

[23] Huang D, Fang J, Wang C, Huang P and Zeng G H 2013 *Chin. Phys. Lett.* **30** 114209

[24] Huang D, Lin D K, Huang P, Wang C, Liu W Q, Fang S H and Zeng G H 2015 *Opt. Express* **23** 17511

[25] Huang D, Huang P, Wang T, Li H S, Zhou Y M and Zeng G H 2016 *Phys. Rev. A* **94** 032305

[26] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 *Phys. Rev. Lett.* **110** 030502

[27] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502

[28] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504

[29] Navascués M and Acín A 2005 *Phys. Rev. Lett.* **94** 020505

[30] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev. A* **72** 050303(R)

[31] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503

[32] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502

[33] Pirandola S, Braunstein S L and Lloyd S 2008 *Phys. Rev. Lett.* **101** 200504

[34] Leverrier A and Grangier P 2011 *Phys. Rev. Lett.* **106** 259902(E)

[35] Lin D K, Huang D, Huang P, Peng J Y and Zeng G H 2015 *Int. J. Quantum Inf.* **13** 1550010

[36] Wang X Y, Zhang Y C, Li Z Y, Xu B J, Yu S and Guo H 2018 *Quantum Information and Computation* **17** 1123

[37] Milicevic M, Feng C, Zhang L M and Gulak P G 2017 arXiv:1702.07740v2 [quant-ph]

[38] Weedbrook C 2013 *Phys. Rev. A* **87** 022308

[39] Guo Y, Liao Q, Wang Y J, Huang D, Huang P and Zeng G H 2017 *Phys. Rev. A* **95** 032304

[40] Marshall K and Weedbrook C 2014 *Phys. Rev. A* **90** 042311

[41] Gehring T, Händchen V, Duhme J, Furrer F, Franz T, Pacher C, Werner R F and Schnabel R 2015 *Nat. Commun.* **6** 8795

[42] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501

[43] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501

[44] Renner R 2008 *International Journal of Quantum Information* **06** 1

[45] Scarani V and Renner R 2008 *Phys. Rev. Lett.* **100** 200501

[46] Cai R Y Q and Scarani V 2009 *New J. Phys.* **11** 045024

[47] Leverrier A, Grosshans F and Grangier P 2010 *Phys. Rev. A* **81** 062343

[48] Pironio S, Acín A, Brunner N, Gisin N, Massar S and Scarani V 2009 *New J. Phys.* **11** 045021

[49] Pirandola S, Serafini A and Lloyd S 2009 *Phys. Rev. A* **79** 052327

[50] Pirandola S 2013 *New J. Phys.* **15** 113046

[51] Zhang Z Y, Shi R H, Zeng G H and Guo Y 2018 *Quantum Inf. Process.* **17** 133

[52] Ruppert L, Usenko V C and Filip R 2014 *Phys. Rev. A* **90** 062310

[53] Furrer F, Franz T, Berta M, Scholz V B, Tomanichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502