



# Security analysis of continuous variable quantum key distribution based on entangled states with biased correlations

WENHUI ZHANG,<sup>1</sup> RUIXIN LI,<sup>1</sup> YAJUN WANG,<sup>1,2,4</sup>  XUYANG WANG,<sup>1,2</sup>  LONG TIAN,<sup>1,2</sup> AND YAOHUI ZHENG<sup>1,2,3</sup> 

<sup>1</sup>State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan, 030006, China

<sup>2</sup>Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China

<sup>3</sup>yhzheng@sxu.edu.cn

<sup>4</sup>YJWangsxu@sxu.edu.cn

**Abstract:** Einstein-Podolsky-Rosen (EPR) entangled states can significantly enhance the secret key rate and secure distance of continuous-variable quantum key distribution (CV-QKD). In practical imperfections always exist in the preparation of two-mode squeezing (entangled states), which present an asymmetrical variance for the two quadratures. The imperfections induced by the bias effect of the entangled states are commonly treated as part of the untrusted channel to decrease the performance of the system. Here, we theoretically quantify the influence of bias effect on the secret key rate and secure distance, and propose a solution of generating unbiased entangled states protocol. The results demonstrated that the unbiased entangled states protocol guarantees the longest secure distance and highest key rate compared to that of coherent and biased entangled states.

© 2021 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

## 1. Introduction

Quantum key distribution (QKD) [1–8] is a prominent technology for quantum information science, which shares a pre-established secret key between two trusted parties based on the laws of quantum physics. In continuous-variable (CV) QKD systems, the secret key is encoded in the quadratures of the electromagnetic field, for example, coherent states [9–13], squeezed/entangled states [2–5,14], in which homodyne or heterodyne detection techniques are used for signal extraction [2,15,16]. Multiple protocols [9,10,13,17] indicated that the secret key rate and secure distance are mainly limited by the excess noise, optical losses, and finite reconciliation efficiency during the distribution [2,15,16]. Present CV-QKD systems are already working with state-of-the-art optical channels and the reconciliation efficiency [6,15–18]. The maximum secure distance has already reached 202 km based on coherent state, in which an ultralow-loss optical fiber combined with a phase compensation and highly-efficient reconciliation procedures was applied for the enhancement [17].

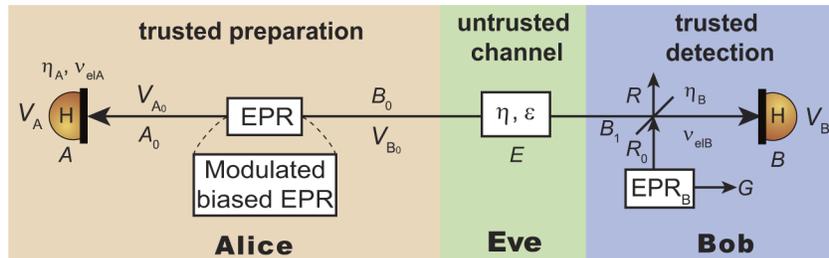
Compared with coherent-state protocol, entangled states protocol is more tolerant to excess noise, loss and reconciliation efficiency [3–5,15,19]. For instance, a -3.5 dB modulated two-mode squeezed states can significantly boost the robustness and distance for secure communication [3], in which, a secret raw key was generated between two parties connected by a noisy and lossy channel—a channel that is not secure for coherent state protocols. As the squeezing factor is improved to 10 dB, the superiority becomes more obvious. In addition, to further enhance the performance, Alice and Bob, share a pair of Einstein-Podolsky-Rosen (EPR) beams and randomly choose a quadrature (amplitude or phase) base measurement to decrypt the key [19]. Therefore, to keep the advantages of this protocol, the entanglement should be prepared not only with strong quantum correlations [20,21], but also with symmetric quantum correlations between the two

quadrature components [22,23]. However, a bias of the two quadratures always accompanies with the preparation of high degree EPR states [23–25], which originates from several interdependent factors in the EPR states production [20,22,24,25]. Compared with unbiased EPR protocol, the bias effect in practical entanglement generation is commonly treated as part of the untrusted channel to weaken the secret key rate and secure distance. Currently, EPR states protocol with single-mode squeezing had been studied in detail with asymmetrical quadrature variance [23,26]. Or a position squeezed state with probability  $P$  and a momentum one with probability  $1 - P$ , prepared to produce a Gaussian modulated average isotropic thermal state, are theoretically demonstrated to have the same performance as an equivalent entanglement-based protocol [14,26]. However, the two-mode squeezing protocol has been demonstrated without considering the bias effect [3,4,19,27]. In [24], we had experimentally and theoretically researched the bias effect in detail, and given a methodology to produce an unbiased EPR states. This inspires the following works: (1) quantitative analysis of the dependence of the system performance of CV-QKD on the bias effect; (2) how to weaken the influence of the bias effect on the secret key rate and secure distance.

Here, we quantitatively analyze the secret key rate and secure distance for three protocols: coherent, biased, and unbiased entanglement. The results indicate a superiority for unbiased EPR protocol in long-distance communication, compared with biased entanglement and coherent protocols. Further, we model the generation process of EPR entangled states and propose a solution to construct unbiased entangled states protocol.

## 2. Theoretical analysis of CV-QKD with biased EPR protocol

Our CV-QKD protocol is shown in Fig. 1, which has three parts, the sender Alice with a state preparation (the EPR entanglement source and modulator) and detection, the quantum channel, and the remote receiver Bob with state detection. The entanglement source is prepared by mixing two amplitude squeezed states with amplitude variances  $V_1(X)$  and  $V_2(X)$  at a 50/50 beam splitter (BS), which outputs are two entangled modes  $A_0$  and  $B_0$ , and belong to the trusted sender. Mode  $A_0$  is a thermal state with a variance of  $V_a(X/Y) = (V_1(X/Y) + V_2(Y/X))/2$  ( $X$  and  $Y$  are the amplitude and phase components, respectively), which is homodyne detected by Alice with a detection efficiency of  $\eta_A$ . Mode  $B_0$  with a variance of  $V_b(X/Y) = (V_1(X/Y) + V_2(Y/X))/2$ .



**Fig. 1.** Schematic diagram of the CV-QKD protocol with modulated entangled states. Alice prepares a Gaussian entangled state with variances  $V_a$  and  $V_b$ , which is modulated with a variance  $V_M$  controlled by Alice. One of the modulated entangled states mode  $V_{B_0}$  transmits through an untrusted quantum channel with a channel transmittance  $\eta$  and excess noise  $\epsilon$ , which can be fully eavesdropped by the third part-Eve. Then, the resulting state with variance  $V_B$  is homodyne detected by Bob. The other entanglement mode  $V_{A_0}$  is also homodyne detected by Alice with a variance  $V_A$ .  $\eta_A$ : detection efficiency of Alice;  $v_{elA}$ : electronic noise of Alice;  $\eta_B$ : detection efficiency of Bob;  $v_{elB}$ : electronic noise of Bob.

Then mode  $B_0$  transmits through a lossy  $\eta$  and noisy  $\epsilon$  quantum channel, which is assumed to be fully controlled by an eavesdropper Eve, consequently, makes the channel untrusted.

Then, mode  $B_0$  is also homodyne detected by a trusted receiver Bob. Bob's noisy detection is purified by placing a beam splitter with an EPR state  $\rho_{R_0G}$  input, which transmission mimics his electronic noise  $\nu_{eIB}$  and detection efficiency  $\eta_B$ . Then the point-to-point repeaterless Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound can be expressed as  $-\log_2(1 - \eta_A \eta_B \eta)$  [8,26,28], which provides the exact benchmark and the secret key capacity of the lossy communication channel (pure-loss channel).

In the EPR based CV-QKD protocol, secret key is distilled from the state information shared by the two trusted parties-Alice and Bob. Considering a protocol with reverse reconciliation (RR) and collective attacks, the secret key rate is expressed as [3,4,27,29,30]

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

The protocol is secure, while the key rate  $\Delta I > 0$  [3,31].  $I_{AB}$  is the Shannon mutual information between Alice and Bob, and  $\chi_{BE}$  is the Holevo quantity. Where  $\beta \leq 1$  refers to the reconciliation efficiency, which is determined by the signal-to-noise ratio (SNR) and algorithm being used for the reconciliation and computational power in trusted devices [32]. Nevertheless, imperfections always indwell in the devices, such as state generation (imperfect coherent or EPR state) and modulation in sender side, or state detection in Bob's station. The imperfections introduce noises and losses into the detection parts, which can seriously shorten the secure distance or limit the key rate to an extremely lower level [32]. Therefore, the key rate in entanglement-based CV-QKD should be analyzed under imperfection conditions. By introducing the imperfections as trusted noise, the Shannon mutual information  $I_{AB}$  between Alice and Bob related to the variances in the two stations and their correlation, is expressed as [4,27]

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_A}{V_{A/B}} = \frac{1}{2} \log_2 \frac{V_A}{V_A - C_{AB}^2 / V_B}, \tag{2}$$

where  $V_A$  and  $V_B$  are the variances of the quadratures measured by Alice and Bob, respectively.  $V_{A/B}$  is the conditional variance.  $C_{AB}$  is the correlation coefficient between Alice and Bob. We assume the state information from Alice transmits through a Gaussian channel-optical fiber with the transmittance  $\eta = 10^{-\alpha L/10}$  and excess noise  $\varepsilon$ , where  $\alpha$  ( $L$ ) is the loss coefficient (length) of the fiber.

For information eavesdropping, the upper bound information  $\chi_{BE}$  accessible to Eve from Bob is limited by the Holevo quantity [27].

$$\begin{aligned} \chi_{BE} &= S(\rho_E) - S(\rho_E^{X_B}) \\ &= \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{j=3}^5 G\left(\frac{\lambda_j - 1}{2}\right), \end{aligned} \tag{3}$$

where  $G(x) = (x + 1) \log_2(x + 1) - x \log_2(x)$  is the bosonic entropic function,  $X_B(Y_B)$  represents Bob's measurement for amplitude (phase) quadrature,  $\rho_E^{X_B}$  is Eve's state conditional on the measured result of Bob, and  $S$  is the Von Neumann entropy of the quantum state  $\rho$ . As Eve's system purifies the system  $A_0B_1$  ( $S(\rho_E) = S(\rho_{A_0B_1})$ ), Bob's measurement purifies the system  $A_0ERG$  ( $S(\rho_E^{X_B}) = S(\rho_{A_0RG}^{X_B})$ ), where  $A_0B_1$  and  $A_0ERG$  are the pure states.  $\chi_{BE}$  can be rewritten as

$$\chi_{BE} = S(\rho_{A_0B_1}) - S(\rho_{A_0RG}^{X_B}). \tag{4}$$

$\lambda_{1,2}$  and  $\lambda_{3,4,5}$  are the symplectic eigenvalues of the covariance matrix  $\gamma_{A_0B_1}$  and  $\gamma_{A_0RG}^{X_B}$  respectively, which are related to the noise variances of the prepared states at Alice's and Bob's stations ( $V_{A_0}$  and  $V_{B_0}$ ) [27], the transmittance  $\eta$  and excess noise  $\varepsilon$  of the quantum channel, and the efficiency  $\eta_B$  and the electronic noise  $\nu_{eIB}$  of the homodyne detector at Bob's station.

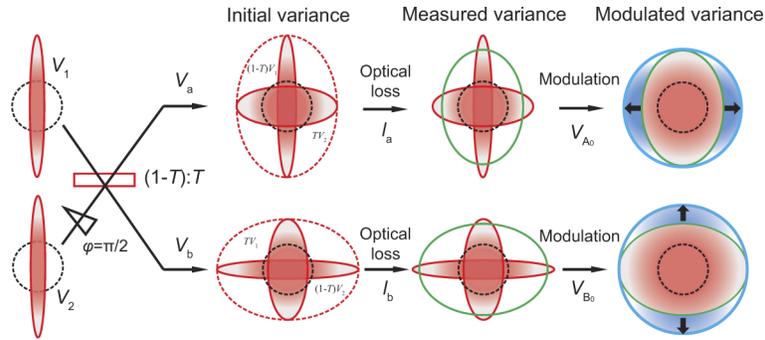
Obviously,  $I_{AB}$  and  $\chi_{BE}$  link the noise variances  $V_a(X/Y)$  and  $V_b(X/Y)$  to the secret key rate. Therefore, the variances  $V_{a,b}$  of the two EPR modes should be dwelled on the actual preparation of EPR states. In the QKD process, unbiased entangled states with symmetrical quantum correlations are usually considered by coupling two equivalent squeezed states  $V_1(X) = V_2(X)$  on a 50/50 BS [3]. In fact, the variances of the two EPR modes are related to the trusted optical channel losses  $l_{a,b}$ , the relative phase between the two squeezing beams  $\varphi$ , variances of the squeezed states  $V_{1,2}(X)$  and balance of the BS  $(1-T):T$  [20,22,24,25]. Any deviation of these parameters from the ideal value may destroy the symmetric correlations and introduce a bias effect as shown in Fig. 2 [22,24,25], which is harmful to the requirements of random quadrature base measurement and also weakens the superiority of the EPR states [23]. Taking into account the bias effect, the amplitude and phase correlation variances can be expressed as (without considering the relative phase between the two squeezing beams  $\varphi$ , the method is detailedly demonstrated in the Appendix)

$$V_a(X) = (1 - l_a)(1 - T)V_1(X) + (1 - l_a)TV_2(Y) + l_a, \tag{5}$$

$$V_a(Y) = (1 - l_a)(1 - T)V_1(Y) + (1 - l_a)TV_2(X) + l_a, \tag{6}$$

$$V_b(X) = (1 - l_b)TV_1(X) + (1 - l_b)(1 - T)V_2(Y) + l_b, \tag{7}$$

$$V_b(Y) = (1 - l_b)TV_1(Y) + (1 - l_b)(1 - T)V_2(X) + l_b. \tag{8}$$



**Fig. 2.** Conceptual illustration of the modulated thermal states protocol.  $V_1$  and  $V_2$ : the variance of two squeezed states;  $V_a$  and  $V_b$ : the variances of the two EPR modes;  $l_a$  and  $l_b$ : the trusted optical losses in the preparation part;  $V_{A_0}$  and  $V_{B_0}$ : the variances of the two modulated EPR modes.

When  $V_1(X) = V_2(X)$ , the unbiased entangled states can be prepared by a balanced BS  $T = 0.5$  or loss  $l_a = l_b$ , and more details can be found in Ref. [24]. In Ref. [24], we had firstly analyzed the origin of the bias effect in detail and directly observed an unbiased entanglement of -10.7 dB by using two single-mode squeezed states. It provides a superior unbiased entangled light source for CV-QKD protocol based on entangled states.

In general EPR states are treated as thermal states [31] with a circular noise distribution for the two quadratures. But for biased EPR states, the quadrature noise distributes to be an elliptical one as describing in Fig. 2 (initial or measured variance before mode B is sent to the untrusted channel), due to the asymmetrical noise redistribution of  $V_1(X)$  and  $V_2(X)$  to Alice and Bob. This asymmetrical noise redistribution of the practical systems is commonly treated as an untrusted part. Hence, Eve is able to extract the information from the untrusted channel, by preparing an appropriate squeezed state to restore the variance to the initial level, and pretend no information leakage to her. In this case, it decreases the performance of the system. To maintain the advanced performance with (single-mode or two-mode [3,4,26]) squeezed state, Bob should discard some

information in one of the measured quadratures, which weakens the secure distance compared with unbiased protocol [23]. On the other hand, the existing theory for homodyne protocol with EPR state requires the two quadrature of the amplitude and phase variances should be equal with each other. Therefore, a modulated thermal state is proposed for the analysis of biased entanglement, in which the small variance quadrature is modulated to generate a circular thermal state [31], showed by the modulated variance in Fig. 2. Under this circumstance,  $V_{a,b}$  evolves into  $V'_{A_0,B_0}$ ,  $V'_{A_0}(X) = V_a(X) + V_{M1}(X)$ ,  $V'_{A_0}(Y) = V_a(Y)$ ,  $V'_{B_0}(X) = V_b(X)$ ,  $V'_{B_0}(Y) = V_b(Y) + V_{M1}(Y)$ , and Eve cannot distinguish the difference between the biased or unbiased EPR protocols. CV-QKD for biased EPR states again restores the performance. Eve is allowed to achieve any attack by emulating the channel transmission and excess noise, and the bias does not affect the leakage information to Eve. Finally, the biased protocol can be treated with the standard CV-QKD theory for the pure state [3,4].

Under a high loss case with RR, i.e., communication in a long-distance fiber, the existing reconciliation algorithm suffers a low efficiency, which severely limits the key rate and distance. To overcome this problem, an additional modulation  $V_{M2}$  is added to the prepared state (modulated thermal state in Fig. 2) to further extend the secure distances [3,4,19]. In an ideal situation (noiseless and lossless in the sender and receiver), arbitrary high modulation ( $1 \sim +\infty$ ) can be applied to greatly enhance the key rate and distance. However, a practical schema is always imperfect, and squeezing level can continuously improve the security parameters, while the modulation must be optimized to tolerate the channel noise [3,19,33].

During the key distribution, mode  $B_0$  is sent to the remote trusted party-Bob, through a quantum channel characterized by the lossy  $\eta$  and noisy  $\varepsilon$ , and the covariance matrix is expressed as

$$\gamma_{A_0B_1} = \begin{pmatrix} \gamma_{A_0} & C_{A_0B_1} \\ C_{A_0B_1} & \gamma_{B_1} \end{pmatrix} = \begin{pmatrix} V_{A_0}(X) & 0 & C_{A_0B_1}(X) & 0 \\ 0 & V_{A_0}(Y) & 0 & C_{A_0B_1}(Y) \\ C_{A_0B_1}(X) & 0 & V_{B_1}(X) & 0 \\ 0 & C_{A_0B_1}(Y) & 0 & V_{B_1}(Y) \end{pmatrix}. \quad (9)$$

where  $V_{A_0}(X) = V_a(X) + V_{M1}(X) + V_{M2}(X)$  and  $V_{A_0}(Y) = V_a(Y) + V_{M2}(Y)$  are the variances of mode  $A_0$  in the amplitude and phase quadratures;  $V_{B_1}(X) = \eta(V_{B_0}(X) + \chi_{\text{line}})$  and  $V_{B_1}(Y) = \eta(V_{B_0}(Y) + \chi_{\text{line}})$  are the variances of mode  $B_1$  in the amplitude and phase quadratures;  $V_{B_0}(X) = V_b(X) + V_{M2}(X)$  and  $V_{B_0}(Y) = V_b(Y) + V_{M1}(Y) + V_{M2}(Y)$  are the variances of mode  $B_0$  in the amplitude and phase quadratures;  $C_{A_0B_1}(X) = \sqrt{\eta}C_{A_0B_0}(X)$  and  $C_{A_0B_1}(Y) = \sqrt{\eta}C_{A_0B_0}(Y)$  are the correlation between the two modes  $A_0$  and  $B_1$  in the amplitude and phase quadratures;  $C_{A_0B_0}(X) = C_{ab}(X) + V_{M1}(X)/2 + V_{M2}(X)$  and  $C_{A_0B_0}(Y) = C_{ab}(Y) + V_{M1}(Y)/2 + V_{M2}(Y)$  are the correlation between the two modes  $A_0$  and  $B_0$  in the amplitude and phase quadratures.  $C_{ab}$  is the initial correlation coefficient of the entangled states without modulation, and the detailed analysis method is in Appendix.

To simplify the analysis process, we assume a trusted noise in the detection part, and a narrow-band homodyne detector is applied [32,34,35]. Then, the modified variances of the quadratures measured by Alice and Bob are deduced as

$$V_A = \eta_A V_{A_0} + 1 - \eta_A + v_{\text{elA}}, \quad (10)$$

$$V_B = \eta\eta_B (V_{B_0} + \chi_{\text{tot}}), \quad (11)$$

where

$$\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/\eta, \quad (12)$$

$$\chi_{\text{line}} = 1/\eta - 1 + \varepsilon, \quad (13)$$

$$\chi_{\text{hom}} = (1 + \nu_{\text{elB}}) / \eta_B - 1. \quad (14)$$

Here,  $\eta_A$  and  $\nu_{\text{elA}}$  are the detection efficiency and electronic noise of Alice's station;  $\eta_B$  and  $\nu_{\text{elB}}$  are that of Bob.  $V_{A_0}$  and  $V_{B_0}$  are the variances of the two modulated EPR modes.  $\chi_{\text{tot}}$  ( $\chi_{\text{line}}$ ) denotes the total (channel) added noise of the channel input site;  $\chi_{\text{hom}}$  is the added noise of the homodyne detector for Bob's input site. Then, the correlation coefficient between Alice and Bob is deduced as [3]

$$C_{AB} = \sqrt{\eta_A \eta_B} (C_{\text{ab}} + V_{M1}/2 + V_{M2}). \quad (15)$$

Substituting with  $V_{A_0, B_0} = V$ , the symplectic eigenvalues  $\lambda_{1,2}$  of the covariance matrix  $\gamma_{A_0 B_1}$  for the analytical formula of  $\chi_{\text{BE}}$  are reduced to

$$\lambda_{1,2} = \sqrt{\frac{1}{2} (\Delta \pm \sqrt{\Delta^2 - 4D})}, \quad (16)$$

where

$$D = \eta^2 (V \chi_{\text{line}} + 1)^2, \quad (17)$$

$$\Delta = V^2 (1 - \eta)^2 + V (2 \chi_{\text{line}} \eta^2) + (\eta^2 \chi_{\text{line}}^2 + 2\eta). \quad (18)$$

The analytical formula for the symplectic eigenvalues  $\lambda_{3,4,5}$  of the covariance matrix  $\gamma_{A_0 B_1}^{\chi_B}$  are reduced to

$$\lambda_{3,4,5} = \sqrt{\frac{1}{2} (A \pm \sqrt{A^2 - 4B})}, \lambda_5 = 1, \quad (19)$$

where for homodyne protocol we have

$$A^{\text{hom}} = \frac{\Delta \chi_{\text{hom}} + V \sqrt{D} + \eta (V + \chi_{\text{line}})}{\eta (V + \chi_{\text{tot}})}, \quad (20)$$

$$B^{\text{hom}} = \sqrt{D} \frac{(\eta \chi_{\text{line}} V + \eta) \chi_{\text{hom}}^2 + [\sqrt{D} \eta (V + \chi_{\text{line}}) + V] \chi_{\text{hom}} + \eta V (V + \chi_{\text{line}})}{[\eta (V + \chi_{\text{tot}})]^2}. \quad (21)$$

Finally, the Holevo bound can be expressed as

$$\chi_{\text{BE}} = G(\lambda_1) + G(\lambda_2) - G(\lambda_3) - G(\lambda_4). \quad (22)$$

In the following section, the performance of the QKD is analyzed in detail for the unbiased and biased EPR protocols in this section.

### 3. Secret key rate and secure distance for biased and unbiased EPR protocols

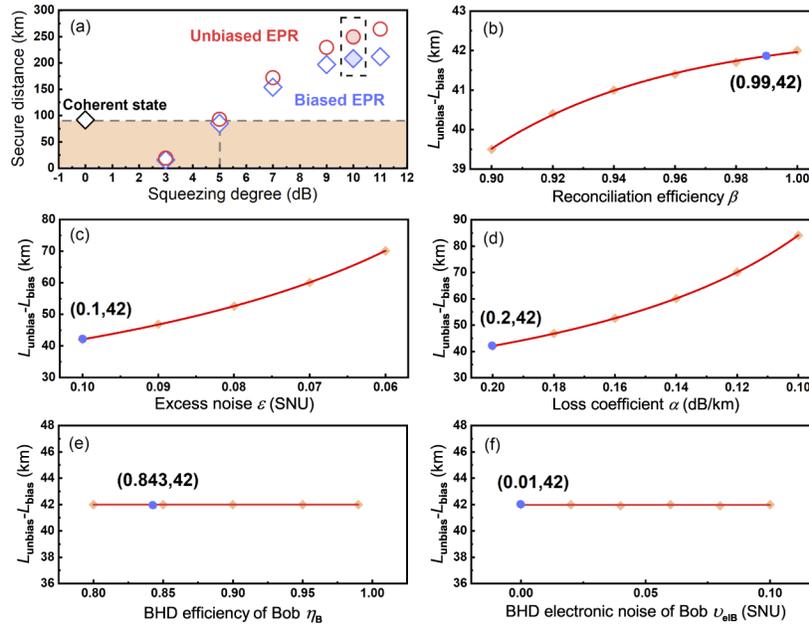
Combining the theoretical models in section 2 and appendixes, we calculate the secure key rate and secure distance of the CV-QKD based on a fiber channel. Firstly, without considering the modulation schema and side-channel effect, the maximum secure distance is compared between the biased and unbiased EPR protocols. Here the maximum distance is stipulated as the key rate decreased to  $10^{-8}$  bits/pulse. Taking the actual situation for states preparation into account, the initial system parameters for biased and unbiased protocols are given as, originating from Ref. [24]. With the precondition of  $V_1(X) = V_2(X)$ , for  $T = 0.49$ , a biased entanglement is obtained, and unbiased correlations are established for  $T = 0.5$ , and more details can be found in our previous work [24]. Then, the differences of the secure distance between the biased and unbiased entanglement protocols  $L_{\text{unbias}} - L_{\text{bias}}$  are demonstrated in Fig. 3, and the parameters for the demonstration of the six sub-graphs are listed in Table 1. With  $V_1(X) = V_2(X)$  in Fig. 3(a), the secure distance for unbiased protocol is enhanced with the increasing of the squeezing level.

**Table 1.** The parameters used to calculate the secure distance of Fig. 3.  $V_{1,2}$ : the variance of two squeezed states;  $\beta$ : reconciliation efficiency;  $\varepsilon$ : excess noise;  $\alpha$ : loss coefficient of a standard single-mode fiber;  $\eta_A$ : detection efficiency of Alice;  $\eta_B$ : detection efficiency of Bob;  $v_{elB}$ : electronic noise of Bob.  $l_a$  and  $l_b$ : the trusted optical losses in the preparation part;  $T$ : beam splitting ratio;  $V(X_a + X_b)$ : the amplitude correlation variance of the entangled states;  $V(Y_a - Y_b)$ : the phase correlation variance of the entangled states; Note:  $l_a=0.01$ ,  $l_b=0.05$ , and  $\eta_A = 0.99$ . The bias variances are calculated with equations (32) and (39) by introducing an unbalanced BS. The unbiased entangled state  $V(X_a + X_b) = V(Y_a - Y_b) = -10.1$  dB is deduced with  $T = 0.5$ , and the biased entangled state  $V(Y_a - Y_b) = -9.5$  dB and  $V(X_a + X_b) = -10.5$  dB is deduced with  $T = 0.49$ .

Number	(a)	(b)	(c)	(d)	(e)	(f)
$V_{1,2}(X)$ (dB)	variable	-12	-12	-12	-12	-12
$\beta$	0.99	variable	0.99	0.99	0.99	0.99
$\varepsilon$	0.1	0.1	variable	0.1	0.1	0.1
$\alpha$ (dB/km)	0.2	0.2	0.2	variable	0.2	0.2
$\eta_B$	0.843	0.843	0.843	0.843	variable	0.843
$v_{elB}$	0.01	0.01	0.01	0.01	0.01	variable

The secure distance starts to surpass the coherent state protocol as the squeezing level increased above 5 dB, and the biased protocol appears to be lower than the unbiased one. Meanwhile, the difference of the maximum secure distance between the two EPR states becomes larger, especially higher than 10 dB (the dotted box in Fig. 3(a)), where the bias begins to quickly weaken the secure distance compared with the unbiased protocol. In the precondition of  $V_1(X) = V_2(X) = -12$  dB, the reconciliation efficiency  $\beta$ , excess noise  $\varepsilon$ , the channel loss coefficient  $\alpha$ , efficiency  $\eta_B$ , and detection electronic noise  $v_{elB}$  of Bob are considered as the influence factors to the biased protocol. The magnitude of the reconciliation efficiency  $\beta$  amends the difference between the biased and unbiased entanglement protocols. As showing in Fig. 3(b),  $L_{unbias}$  is more superior to  $L_{bias}$  as  $\beta$  approaching the unit. And this conclusion is also suitable for a noiseless or lossless quantum channel, i.e., in Fig. 3(c) and (d), less excess noise or channel loss is more favorable to the unbiased protocol for secure distance enhancement. Moreover, in Fig. 3(e) and (f), the detection efficiency  $\eta_B$  and electronic noise  $v_{elB}$  in Bob's station have no impact on  $L_{unbias} - L_{bias}$ , which act as linear noise injection for the two protocols. From the above argument, we can see that unbiased entanglement proves to be more preferable for long-distance communication, especially for a squeezing level above 10 dB. The results are also supported by Ref. [23].

Before secret key rate calculation, we provide a channel estimation [36] analysis based on current experimental conditions for EPR protocol. A standard single-mode fiber (a loss coefficient  $\alpha = 0.2$  dB/km) serves as the transmission channel of the entangled states from Alice to Bob. Assuming one of the EPR modes in Alice station is prepared with a detection efficiency  $\eta_A > 99\%$  (an optical propagation efficiency is better than 0.2%, an interference visibility of 99.8%, a quantum efficiency inferred by the measured squeezing level is about 99.5%) [35]. In Bob's station, we suppose the transmitted states from the channel are coupled by fiber devices, and injected into space homodyne detection, which efficiency is given as  $\eta_B = 0.843$  (the optical propagation efficiency based on the fiber devices is 85.5%, homodyne detector's visibility is 99.8%, the quantum efficiency of the photodiodes is also better than 99%) [3,4,18,29,37]. Then, the key distribution is simulated with the schema in Ref. [4], and all the above parameters are used to estimate the channel. Incorporating Ref. [36,38] (models of channel estimation) and the noise variances of -10 dB, the excess noise of the protocol is estimated to be better than 0.1. In our theoretical analysis, excess noise is chosen as 0.1 to meet the realistic situation. Imperfections at Alice's and Bob's stations introduce the side-channel effects, that make the protocol more sensitive to the channel noise and can even break the security for purely attenuating channel. With the above parameters and the theoretical results for two-mode squeezing in Ref. [39,40], the side-channel limits the maximum tolerable channel noise to be approximately 0.72 SNU at

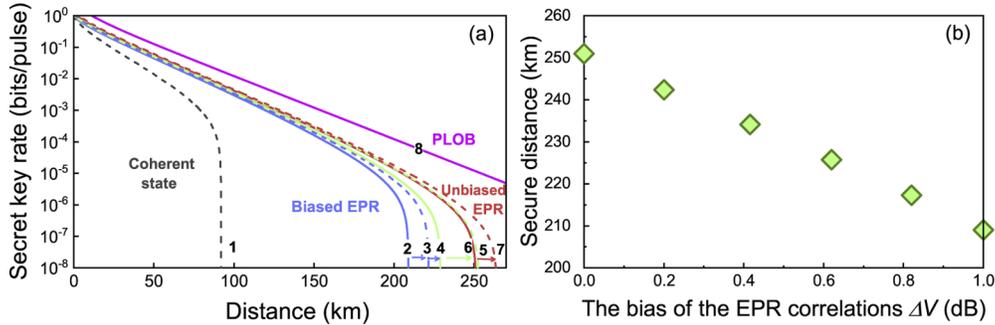


**Fig. 3.** Secure distances comparison with and without bias effect for different squeezing degree, reconciliation efficiency  $\beta$ , excess noise  $\varepsilon$ , loss coefficient of the optical fiber  $\alpha$ , the efficiency  $\eta_B$  and electronic noise  $\nu_{e|B}$  of Bob.  $L_{\text{unbias}}$  and  $L_{\text{bias}}$  are the secure distances of unbiased and biased EPR protocols. SNU: shot noise units; BHD: balanced homodyne detector.

Alice's station and 0.65 SNU at Bob's station. It demonstrated that the EPR protocol was more tolerant to the prepared and detected noises, hence we omit the side-channel effects.

In the key rate calculation, the reconciliation efficiency  $\beta=0.99$  is considered as the highest level in practical protocols [18]. Assumed an infinite number of measured samples is used to extract the key rate. For all protocols, imperfect reconciliation efficiency  $\beta < 1$  limits the modulated variances to a finite value [33]. As a consequence, there is an optimal  $V_M$  to guarantee the best performance of the QKD. Inferred from equations (32) and (39), the biased EPR can be transformed to an unbiased one by changing the variances of the squeezed states  $V_{1,2}(X)$ , the trusted optical losses  $l_{a,b}$  in the preparation part or balance of the BS  $(1-T):T$  [24]. The details for the production of unbiased entangled states were investigated in a recent paper [24]. However, in CV-QKD, channel loss is uncontrollable. To maintain the maximum entanglement level and secure distance, the balance of the BS is favorable compared with the other two parameters. Figure 4(a) shows the calculated secret key rate and maximum secure distance, and the parameters for the calculation are listed in Table 2. The results demonstrated that the unbiased EPR protocol (curves 6 and 7) is superior to the other two protocols (biased EPR and coherent protocols) in the maximum secure distance, and still can be improved by a finite modulation ( $V_{M2} = 4.7$ , the secure distance is increased from 251 km to 263 km). The biased EPR protocol (curves 2 and 3) is more robust compared with the coherent one (curve 1), but is less robust than the unbiased EPR one. The unbiased EPR of curves 4 and 5 in Fig. 4(a) is obtained by substituting  $T = 0.49$  into  $T = 0.5$  (column number 2 and number 4 in Table 2). From curves 2-5, it can be found that the weakness of the biased EPR protocol is able to compensate by transforming the biased EPR into an unbiased one. The results also show that the QKD protocols presented here are unable to beat the PLOB bound (curve 8 in Fig. 4(a)). Figure 4(b) shows a relation between the secure distance and bias effect. It also can be seen that the bias effects weaken the secure distance,

and the unbiased EPR represents the optimum choice for entangled states CV-QKD, which will greatly enhance the secret key rate and secure distance compared with the biased EPR protocols.



**Fig. 4.** (a) Key rate versus distance for coherent state, biased and unbiased entangled states protocols. The solid line represents no modulation protocol, and the dotted line is that with modulation. (b) Maximum secure distances versus the bias correlations  $\Delta V = V(Y_a - Y_b) - V(X_a + X_b)$  of the entanglement. (1) coherent state with  $V_{M2} = 10.8$ ; (2) biased entangled state with the noise variances of -10.5 dB and -9.5 dB for the amplitude and phase quadratures without modulation; (3) biased entangled state with the noise variances of -10.5 dB and -9.5 dB for the amplitude and phase quadratures with  $V_{M2} = 4.4$ ; (4) -9.3 dB unbiased entangled state without modulation; (5) -9.3 dB unbiased entangled state with  $V_{M2} = 6.7$ ; (6) -10.1 dB unbiased entangled state without modulation; (7) -10.1 dB unbiased entangled state with  $V_{M2} = 4.7$ ; (8) PLOB bound.

**Table 2.** The parameters used to calculate the secure distance of Fig. 4.  $V_{1,2}$ : the variance of two squeezed states;  $l_a$  and  $l_b$ : the trusted optical losses in the preparation part;  $T$ : beam splitting ratio;  $V(Y_a - Y_b)$ : the phase correlation variance of the entangled states;  $V(X_a + X_b)$ : the amplitude correlation variance of the entangled states;  $V_{M2}$ : optimum modulation variance;  $\beta$ : reconciliation efficiency;  $\varepsilon$ : excess noise;  $\alpha$ : loss coefficient of a standard single-mode fiber;  $\eta_A$ : detection efficiency of Alice;  $\eta_B$ : detection efficiency of Bob;  $v_{elB}$ : electronic noise of Bob.

States	Coherent states	Biased EPR		Unbiased EPR			
Number	1	2	3	4	5	6	7
$V_{1,2}(X)$ (dB)	0	-12	-12	-12	-12	-12	-12
$l_a$	0.05	0.01	0.01	0.05	0.05	0.01	0.01
$l_b$	0.05	0.05	0.05	0.05	0.05	0.05	0.05
$T$	\	0.49	0.49	0.5	0.5	0.5	0.5
$V(Y_a - Y_b)$ (dB)	0	-9.5	-9.5	-9.3	-9.3	-10.1	-10.1
$V(X_a + X_b)$ (dB)	0	-10.5	-10.5	-9.3	-9.3	-10.1	-10.1
$V_{M2}$	10.8	0	4.4	0	6.7	0	4.7
Secure distance (km)	92	209	221	229	253	251	263

Note:  $\beta=0.99$ ,  $\varepsilon=0.1$ ,  $\alpha=0.2$  dB/km,  $\eta_A=0.99$ ,  $\eta_B=0.843$ ,  $v_{elB}=0.01$ .

For a hundred-kilometer standard optical fiber channel, the visibility of the homodyne detection remains the same compared with free space, but introduces a differential phase fluctuation and excess noise between the two quantum channels. It forms the main challenge in implementing the EPR based CV-QKD, because an entangled state is more sensitive to the phase and excess noise. Although a stable controlling of the phase fluctuation is available in local EPR sources [20,35,41–43], more effort should be done to meet the long-distance optical fiber communication.

Although a rigorous experiment proof for hundred-kilometer standard optical fiber distribution is beyond the scope of this paper, this result with a bias effect analysis constitutes a fundamental advance in EPR based CV-QKD.

#### 4. Conclusion

We compare the secret key rate and secure distance of CV-QKD in three distribution protocols: coherent state, biased entangled states, and unbiased entangled states. The theoretical results show that the weakness of the biased EPR protocol in long-distance communication can be lowered by transforming it into an unbiased one, and the unbiased EPR protocol is superior to other protocols for long-distance distribution, especially the noise reduction goes beyond 10 dB. And the QKD protocols presented here are unable to beat the PLOB bound. By considering the practical imperfections (original squeezing variance, trusted optical loss, and non-ideal BS) in the preparation, transmission, and detection processes of entangled states, we provide a feasible proposal for constructing unbiased entangled states protocol. With the improvement of the phase control technique, an unbiased entanglement source [24] will be expected to apply to a practical available CV-QKD protocol and further boost the secret key rate and distance.

#### Appendixes: theoretical models of the biased entanglement

The entangled states are prepared by coupling two equivalent squeezed states  $S_1$  and  $S_2$  on a beam splitter (BS) with transmittance  $T$ . Considering the phase difference  $\varphi$  between the two squeezing beams, the output operators of the BS are

$$a = \sqrt{1-T}S_1 + \sqrt{T}S_2e^{i\varphi}, \quad (23)$$

$$b = \sqrt{T}S_1 - \sqrt{1-T}S_2e^{i\varphi}. \quad (24)$$

The amplitude quadrature operators for Alice and Bob are

$$X'_a = a + a^\dagger = \sqrt{1-T}(S_1 + S_1^\dagger) + \sqrt{T}(S_2e^{i\varphi} + S_2^\dagger e^{-i\varphi}), \quad (25)$$

$$X'_b = b + b^\dagger = \sqrt{T}(S_1 + S_1^\dagger) - \sqrt{1-T}(S_2e^{i\varphi} + S_2^\dagger e^{-i\varphi}). \quad (26)$$

Subsequently, introducing the trusted optical losses  $l_a$  and  $l_b$  in the preparation part, the amplitude quadratures for Alice and Bob becomes

$$X_a = \sqrt{1-l_a}X'_a + \sqrt{l_a}, \quad (27)$$

$$X_b = \sqrt{1-l_b}X'_b + \sqrt{l_b}. \quad (28)$$

The variances of amplitude quadrature for Alice and Bob can be expressed as

$$V_a(X) = (1-l_a)(1-T)V_1(X) + (1-l_a)T(V_2(X)\cos^2\varphi + V_2(Y)\sin^2\varphi) + l_a, \quad (29)$$

$$V_b(X) = (1-l_b)TV_1(X) + (1-l_b)(1-T)(V_2(X)\cos^2\varphi + V_2(Y)\sin^2\varphi) + l_b. \quad (30)$$

Furthermore, the sum of the amplitude quadrature operator readouts from the detection process can be deduced as

$$\begin{aligned} X_a + X_b &= \sqrt{1-l_a}X_a + \sqrt{l_a} + \sqrt{1-l_b}X_b + \sqrt{l_b} \\ &= \left(\sqrt{1-l_a}\sqrt{1-T} + \sqrt{1-l_b}\sqrt{T}\right)X_1 \\ &\quad + \left(\sqrt{1-l_a}\sqrt{T} - \sqrt{1-l_b}\sqrt{1-T}\right)(S_2e^{i\varphi} + S_2^\dagger e^{-i\varphi}) + \sqrt{l_a} + \sqrt{l_b}. \end{aligned} \quad (31)$$

(34) Finally, the amplitude correlation variance of the entangled states can be obtained as:

$$\begin{aligned}
 V(X_a+X_b) &= \left( (1-l_a)(1-T) + (1-l_b)T + 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T} \right) \langle \delta^2 X_1 \rangle \\
 &+ \left( (1-l_a)T + (1-l_b)(1-T) - 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T} \right) \\
 &\left( \cos^2\varphi \langle \delta^2 X_2 \rangle + \sin^2\varphi \langle \delta^2 Y_2 \rangle \right) + l_a + l_b \\
 &= \alpha_1 V_1(X) + \beta_1 \left( V_2(X)\cos^2\varphi + V_2(Y)\sin^2\varphi \right) + l_a + l_b,
 \end{aligned} \tag{32}$$

where  $V(X_a+X_b) = V_a(X) + V_b(X) + 2C_{ab}(X)$ ,  $X_1 = S_1 + S_1^\dagger$ ,  $X_2 = S_2 + S_2^\dagger$ ,  $Y_2 = 1/i(S_2 - S_2^\dagger)$  are the amplitude and phase operators of the two squeezed states.  $\alpha_1$  and  $\beta_1$  are the coefficients related to losses ( $l_a$  and  $l_b$ ) and beam splitting ratio  $T$ , which can be expressed as

$$\alpha_1 = (1-l_a)(1-T) + (1-l_b)T + 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T}, \tag{33}$$

$$\beta_1 = (1-l_a)T + (1-l_b)(1-T) - 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T}. \tag{34}$$

The correlation coefficient of amplitude quadrature is

$$C_{ab}(X) = \sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T} \left( V_1(X) - V_2(X)\cos^2\varphi - V_2(Y)\sin^2\varphi \right). \tag{35}$$

With the same method, the variance of phase quadrature for Alice and Bob can be expressed as

$$V_a(Y) = (1-l_a)(1-T)V_1(Y) + (1-l_a)T \left( V_2(Y)\cos^2\varphi + V_2(X)\sin^2\varphi \right) + l_a, \tag{36}$$

$$V_b(Y) = (1-l_b)TV_1(Y) + (1-l_b)(1-T) \left( V_2(Y)\cos^2\varphi + V_2(X)\sin^2\varphi \right) + l_b. \tag{37}$$

The correlation coefficient of phase quadrature is

$$C_{ab}(Y) = \sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T} \left( V_1(Y) - V_2(Y)\cos^2\varphi - V_2(X)\sin^2\varphi \right). \tag{38}$$

The phase correlations can be deduced as

$$V(Y_a - Y_b) = \alpha_2 V_1(Y) + \beta_2 \left( V_2(Y)\cos^2\varphi + V_2(X)\sin^2\varphi \right) + l_a + l_b, \tag{39}$$

where

$$\alpha_2 = (1-l_a)(1-T) + (1-l_b)T - 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T}, \tag{40}$$

$$\beta_2 = (1-l_a)T + (1-l_b)(1-T) + 2\sqrt{(1-l_a)(1-l_b)}\sqrt{T}\sqrt{1-T}, \tag{41}$$

$$V(Y_a - Y_b) = V_a(Y) + V_b(Y) - 2C_{ab}(Y). \tag{42}$$

The bias correlations for the two quadrature correlations is defined as

$$\Delta V = V(Y_a - Y_b) - V(X_a + X_b). \tag{43}$$

**Funding.** National Natural Science Foundation of China (11654002, 11804206, 11804207, 11874250, 62027821, 62035015); National Key Research and Development Program of China (2020YFC2200402); Key Research and Development Projects of Shanxi Province (201903D111001); Program for Sanjin Scholar of Shanxi Province; Program for Outstanding Innovative Teams of Higher Learning Institutions of Shanxi; Fund for Shanxi "1331 Project" Key Subjects Construction.

**Disclosures.** The authors declare no conflicts of interest.

**Data availability.** Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

## References

1. T. C. Ralph and P. K. Lam, "A bright future for quantum communications," *Nat. Photonics* **3**(12), 671–673 (2009).
2. C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," *Phys. Rev. A* **87**(2), 022308 (2013).
3. L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," *Nat. Commun.* **3**(1), 1083 (2012).
4. N. Wang, S. N. Du, W. Y. Liu, X. Y. Wang, Y. M. Li, and K. C. Peng, "Long-distance continuous-variable quantum key distribution with entangled states," *Phys. Rev. Appl.* **10**(6), 064028 (2018).
5. N. Wang, S. N. Du, W. Y. Liu, X. Y. Wang, and Y. M. Li, "Generation of Gaussian-modulated entangled states for continuous variable quantum communication," *Opt. Lett.* **44**(15), 3613–3616 (2019).
6. J. F. D. M. Lucamarini, Z. L. Yuan, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature* **557**(7705), 400–403 (2018).
7. 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), p. 175–179.
8. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photonics* **12**(4), 1012–1236 (2020).
9. F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature* **421**(6920), 238–241 (2003).
10. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," *Phys. Rev. Lett.* **95**(18), 180503 (2005).
11. A. Leverrier and P. Grangier, "Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation," *Phys. Rev. Lett.* **102**(18), 180504 (2009).
12. R. Namiki and T. Hirano, "Security of quantum cryptography using balanced homodyne detection," *Phys. Rev. A* **67**(2), 022308 (2003).
13. F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Phys. Rev. Lett.* **88**(5), 057902 (2002).
14. N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," *Phys. Rev. A* **63**(5), 052311 (2001).
15. 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**(5), 378–381 (2013).
16. H. Ko, B. S. Choi, J. S. Choe, K. J. Kim, J. H. Kim, and C. J. Youn, "High-speed and high-performance polarization-based quantum key distribution system without side channel effects caused by multiple lasers," *Photonics Res.* **6**(3), 214–219 (2018).
17. Y. C. Zhang, Z. Y. Chen, S. Pirandola, X. Y. Wang, C. Zhou, B. J. Chu, Y. J. Zhao, B. J. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," *Phys. Rev. Lett.* **125**(1), 010502 (2020).
18. 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**(1), 21 (2018).
19. V. C. Usenko and R. Filip, "Squeezed-state quantum key distribution upon imperfect reconciliation," *New J. Phys.* **13**(11), 113007 (2011).
20. T. Eberle, V. Händchen, and R. Schnabel, "Stable control of 10 dB two-mode squeezed vacuum states of light," *Opt. Express* **21**(9), 11546–11553 (2013).
21. S. Steinlechner, J. Bauchrowitz, T. Eberle, and R. Schnabel, "Strong Einstein-Podolsky-Rosen steering with unconditional entangled states," *Phys. Rev. A* **87**(2), 022104 (2013).
22. W. P. Bowen, P. K. Lam, and T. C. Ralph, "Biased EPR entanglement and its application to teleportation," *J. Mod. Opt.* **50**(5), 801–813 (2003).
23. T. Eberle, V. Händchen, J. Duhme, T. Franz, F. Furrer, R. Schnabel, and R. F. Werner, "Gaussian entanglement for quantum key distribution from a single-mode squeezing source," *New J. Phys.* **15**(5), 053049 (2013).
24. Y. J. Wang, W. H. Zhang, R. X. Li, L. Tian, and Y. H. Zheng, "Generation of -10.7 dB unbiased entangled states of light," *Appl. Phys. Lett.* **118**(13), 134001 (2021).
25. K. Wagner, J. Janousek, S. Armstrong, J. F. Morizur, P. K. Lam, and H. A. Bachor, "Asymmetric EPR entanglement in continuous variable systems," *J. Phys. B: At., Mol. Opt. Phys.* **47**(22), 225502 (2014).
26. S. Pirandola, "Limits and security of free-space quantum communications," *Phys. Rev. Res.* **3**(1), 013279 (2021).
27. A. Becir and M. R. B. Wahiddin, "Tight bounds for the eavesdropping collective attacks on general CV-QKD protocols that involve non-maximally entanglement," *Quantum Inf. Process.* **12**(2), 1155–1171 (2013).
28. S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun.* **8**(1), 15043 (2017).

29. J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouiri, 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).
30. D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," *Sci. Rep.* **6**(1), 19201 (2016).
31. C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.* **105**(11), 110501 (2010).
32. V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," *Phys. Rev. A* **81**(2), 022318 (2010).
33. X. Y. Wang, S. Y. Guo, P. Wang, W. Y. Liu, and Y. M. Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," *Opt. Express* **27**(9), 13372–13386 (2019).
34. V. C. Usenko and R. Filip, "Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense," *Entropy* **18**(1), 20 (2016).
35. W. H. Zhang, J. R. Wang, Y. H. Zheng, Y. J. Wang, and K. C. Peng, "Optimization of the squeezing factor by temperature-dependent phase shift compensation in a doubly resonant optical parametric oscillator," *Appl. Phys. Lett.* **115**(17), 171103 (2019).
36. L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," *Phys. Rev. A* **90**(6), 062310 (2014).
37. J. Mizuno, K. Wakui, A. Furusawa, and M. Sasaki, "Experimental demonstration of entanglement-assisted coding using a two-mode squeezed vacuum state," *Phys. Rev. A* **71**(1), 012304 (2005).
38. W. Y. Liu, X. Y. Wang, N. Wang, S. N. Du, and Y. M. Li, "Imperfect state preparation in continuous-variable quantum key distribution," *Phys. Rev. A* **96**(4), 042312 (2017).
39. I. Derkach, V. C. Usenko, and R. Filip, "Preventing side-channel effects in continuous-variable quantum key distribution," *Phys. Rev. A* **93**(3), 032309 (2016).
40. I. Derkach, V. C. Usenko, and R. Filip, "Continuous-variable quantum key distribution with a leakage from state preparation," *Phys. Rev. A* **96**(6), 062309 (2017).
41. W. H. Yang, S. P. Shi, Y. J. Wang, W. G. Ma, Y. H. Zheng, and K. C. Peng, "Detection of stably bright squeezed light with the quantum noise reduction of 12.6 dB by mutually compensating the phase fluctuations," *Opt. Lett.* **42**(21), 4553–4556 (2017).
42. S. Shi, L. Tian, Y. Wang, Y. Zheng, C. Xie, and K. Peng, "Demonstration of channel multiplexing quantum communication exploiting entangled sideband modes," *Phys. Rev. Lett.* **125**(7), 070502 (2020).
43. J. R. Wang, W. H. Zhang, L. Tian, Y. Wang, R. C. Yang, J. Su, and Y. H. Zheng, "Balanced Homodyne Detector with Independent Phase Control and Noise Detection Branches," *IEEE Access* **7**, 57054–57059 (2019).