entropy

Article

# Enhancing of Self-Referenced Continuous-Variable Quantum Key Distribution with Virtual Photon Subtraction

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

[1] School of Information Science and Engineering, Central South University, Changsha 410083, China; haizhong2018@foxmail.com (H.Z.); xxywyj@sina.com (Y.W.); wangxd11@foxmail.com (X.W.); llqqlq@csu.edu.cn (Q.L.); XiaoDongWu514@126.com (X.W.)

[2] School of IOT Engineering, Taihu University, Wuxi 214064, China

* Correspondence: yingguo@csu.edu.cn

Received: 28 June 2018; Accepted: 2 August 2018; Published: 6 August 2018

**Abstract:** The scheme of the self-referenced continuous-variable quantum key distribution (SR CV-QKD) has been experimentally demonstrated. However, because of the finite dynamics of Alice's amplitude modulator, there will be an extra excess noise that is proportional to the amplitude of the reference pulse, while the maximal transmission distance of this scheme is positively correlated with the amplitude of the reference pulse. Therefore, there is a trade-off between the maximal transmission distance and the amplitude of the reference pulse. In this paper, we propose the scheme of SR CV-QKD with virtual photon subtraction, which not only has no need for the use of a high intensity reference pulse to improve the maximal transmission distance, but also has no demand of adding complex physical operations to the original self-referenced scheme. Compared to the original scheme, our simulation results show that a considerable extension of the maximal transmission distance can be obtained when using a weak reference pulse, especially for one-photon subtraction. We also find that our scheme is sensible with the detector's electronic noise at reception. A longer maximal transmission distance can be achieved for lower electronic noise. Moreover, our scheme has a better toleration of excess noise compared to the original self-referenced scheme, which implies the advantage of using virtual photon subtraction to increase the maximal tolerable excess noise for distant users. These results suggest that our scheme can make the SR CV-QKD from the laboratory possible for practical metropolitan area application.

**Keywords:** quantum cryptography; continuous-variable quantum key distribution; photon subtraction

## 1. Introduction

Quantum key distribution (QKD), which is the best-known application of quantum cryptography, is able to distribute a secret key between two distant legitimate parties, called Alice and Bob, over an a priori unsecure communication channel [1–4]. There are two branches in performing quantum key distribution: the discrete-variable (DV) QKD based on modulating a single photon state and the continuous-variable (CV) QKD based on coherent detection [5–8]. CV-QKD has demonstrated the advantages of high detection efficiency and low experiment cost. More significantly, most standard telecommunication technologies could be compatible with CV-QKD, which makes CV-QKD more attractive and hence fruitful [9–14].

The major research protocol of CV-QKD is the Gaussian modulated coherent state (GMCS) CV-QKD protocol, the unconditional security of which has been demonstrated in theory [15–17]. In order to provide a phase reference for Bob's coherent detection on the received quantum signals, the conventional GMCS protocol needs to co-transmit a local oscillator (LO), a high bright classical beam, between Alice and Bob. However, due to the existence of the LO, a series of new, severe security loopholes has been proven, thus making some side-channel attacks possible [18–22], which can greatly reduce the overall security of the GMCS CV-QKD protocol. In order to obtain a more robust system against the aforementioned side-channel attacks, new schemes have been proposed in recent years [23–25]. These schemes waive the transmission of the LO between legitimate users and generate the LO locally at Bob's side with an extra laser source, which can eliminate all of the above side-channel attacks effectively. In the protocol of self-referenced (SR) CV-QKD [23], the maximal transmission distance is positively correlated with the amplitude of the reference pulses. However, an extra excess noise proportional to the amplitude of the reference pulse will be generated due to the finite dynamics of Alice's amplitude modulator [26]. This extra excess noise will limit the amplitude of the reference pulse and then greatly degrade the performance of the SR CV-QKD scheme, especially the maximal transmission distance. For example, for a more realistic value of the reference pulse amplitude of $V_R = 20V_A$ ($V_A$ is the variance of the signal pulse), the maximal transmission distance is only around 5 km [23]. Therefore, it is of great practical significance to seek a solution to extend the maximal transmission distance when the reference pulse is weak.

Facing the issue of improving the secure transmission distance of the CV-QKD protocol, many approaches have been demonstrated to be useful. For example, the photon subtraction operation, a non-Gaussian operation that has been demonstrated theoretically and experimentally in CV-QKD [27–32], is an effective approach to enhance the transmission distance of CVQKD protocols significantly. Through the photon subtraction operation, the entanglement of Gaussian states can be enhanced; thus, the maximal transmission distance of CV-QKD protocols will be extended, and the noise tolerance of the states may be improved. However, the practical operation of photon subtraction will not only increase the physical complexity of the system, but also inevitably encounter the imperfections of devices, especially the single-photon detector. Fortunately, in the prepare-and-measurement (PM) scheme of CV-QKD with a coherent state, a real photon subtraction operation can be emulated by a non-Gaussian post-selection method, which can be deemed as a virtual photon subtraction [33]. This method not only has no need for complex physical operations, but also can emulate the ideal photon-subtraction operations. Therefore, the method of virtual photon subtraction is a superior way to improve the performance of CV-QKD protocols in practice, which has been demonstrated by many researches [33–36].

In this paper, we propose the scheme of SR CV-QKD with virtual photon subtraction. One advantage of using virtual photon subtraction is that it not only has no need for increasing the practical complexity of the original SR CV-QKD protocol, but also can emulate the ideal photon-subtraction operations. Another advantage is that it can extend the maximal transmission distance without increasing the intensity of the reference pulse and, thus, can effectively avoid the reference pulse's leakage noise, which contributes to the finite dynamics of Alice's amplitude modulator. Compared to the original SR CV-QKD protocol, our simulation results show that the maximal transmission distance can be extended considerably, especially for one-photon subtraction. Meanwhile, a lower electronic noise of Bob's detector can bring about a longer extension of the maximal transmission distance. Moreover, our scheme can tolerate a larger excess noise than the original SR CV-QKD scheme, which implies the advantage of using virtual photon subtraction to increase the maximal tolerable excess noise for distant users. These results suggest that under existing technology, our modified scheme of the SR CV-QKD can make possible the SR CV-QKD from the laboratory for practical metropolitan area application.

This paper is organized as follows. In Section 2, we review the conventional Gaussian CV-QKD and the SR CV-QKD scheme. In Section 3, we first show the basic photon subtraction on a two-mode squeezed vacuum state, and then, we introduce our scheme of SR CV-QKD with virtual photon subtraction. In Section 4, we analyze the performance of our proposed scheme in the secure key rate and the maximal tolerable excess noise. Finally, we summarize this paper in Section 5.

## 2. The Conventional Gaussian and the SR CV-QKD Scheme

The conventional Gaussian CV-QKD scheme is illustrated in Figure 1a. Through the techniques of multiplexing in time and polarization, the quantum signals and the LO are co-transmitted from Alice to Bob in the quantum channel. Moreover, one can utilize the wavelength-division multiplexing technique to generate multiply-parallel quantum channels simultaneously, which are multiplexed and demultiplexed by the wavelength multiplexer and demultiplexer. At the receiver, Bob splits the quantum signals and the LO by the polarization controller and polarizing beam splitter. However, an eavesdropper can utilize the possible security loopholes of the intensity LO to perform side-channel attacks. Meanwhile, multiplexing and demultiplexing are knotty, as these are two kinds of signals that differ greatly in amplitude.

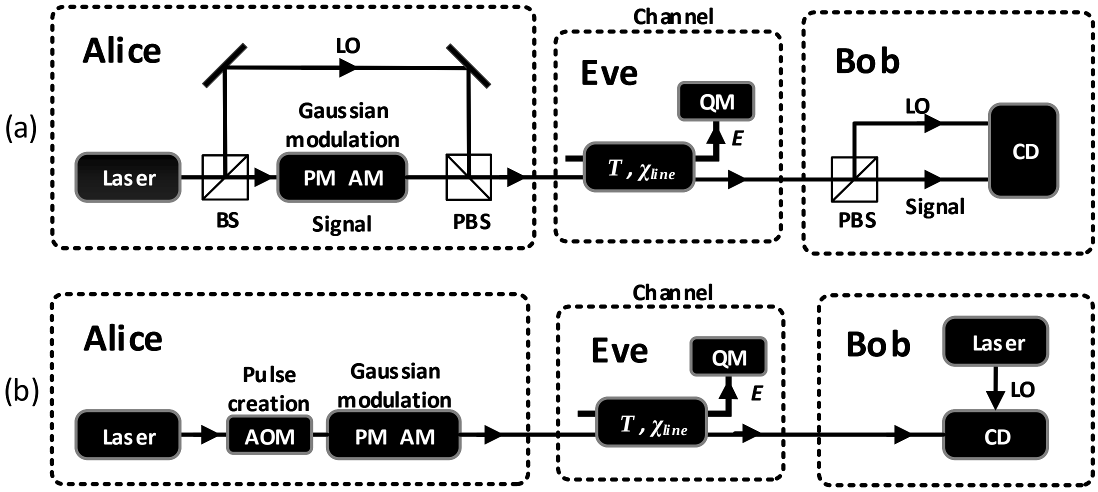


**Figure 1.** (**a**) The conventional Gaussian continuous-variable quantum key distribution (CV-QKD) scheme. The quantum signal and local oscillator (LO) are co-propagated from Alice to Bob. (**b**) The scheme of self-referenced (SR) CV-QKD. The quantum signals and reference pulses are co-transmitted through the same channel. At reception, the received pulses are measured in Bob's own phase reference frame defined by the locally-generated LO. PM, phase modulator; AM, amplitude modulator; CD, coherent detection; QM, quantum memory; AOM, acousto-optical modulator; PBS, polarizing beam splitter; $\chi_{line}$, channel-added noise; T, channel transmission; E, Eve's ancillae.

Different from the conventional Gaussian CV-QKD scheme, the SR CV-QKD scheme in [23] waives the transmission of the LO between legitimate users and operates essentially by employing a locally-generated LO, which effectively resists the possible side-channel attacks. The SR CV-QKD scheme could be generalized as shown in Figure 1b, and it contains two main steps:

Step 1: Alice prepares the Gaussian modulated coherent state $|q_A + ip_A\rangle$ as the quantum signal pulse and the other coherent state $|q_{A_R} + ip_{A_R}\rangle$ as the reference pulse. Then, she sends these coherent states to Bob without sending the LO. The two independent Gaussian random variables $(q_A, p_A)$ are both distributed as $\mathcal{N}(0, V_A)$, while the mean quadrature values of the reference pulse are fixed to $(q_{A_R}, p_{A_R})$ in Alice's phase reference frame and are publicly known. The amplitude of the reference pulse $E_R$ ($E_R = \sqrt{p_{A_R}^2 + q_{A_R}^2}$) may be several orders of amplitude larger than $\sqrt{V_A}$ and is much weaker than the amplitude of the LO.

Step 2: Bob performs a homodyne detection on the received signal pulse and a heterodyne detection on the reference pulse in his own reference frame defined by the locally-generated LO. He obtains $q_B$ or $p_B$ as one of the quadratures of the signal pulse and $q_{B_R}$ and $p_{B_R}$ as both of the quadratures of the reference pulse.

The reference pulse is used to estimate the phase deviation angle $\hat{\theta}$ between Alice's and Bob's reference frames. The $\hat{\theta}$ can be estimated by $\hat{\theta} = \theta + \phi$, where $\theta$ is the actual deviation angle and $\phi$ is the measurement error contributed by the quantum uncertainty. The covariance matrix between Alice and Bob can be written as [23]:

$$\bar{\gamma}_{AB} = \begin{pmatrix} V\mathbb{I} & C\overline{\cos\phi}\sigma_Z \\ C\overline{\cos\phi}\sigma_Z & T\eta(V+\chi)\mathbb{I} \end{pmatrix} \tag{1}$$

with $C = \sqrt{T\eta(V^2-1)}$, where $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $V$ is the variance of Alice's output state, $\chi$ is the channel noise, $T$ is the channel transmission, $\eta$ is the detector efficiency, $\overline{\cos\phi} = \int_{-\pi}^{\pi} d\phi \mathcal{P}(\phi) cos\phi$ and $\mathcal{P}(\phi)$ is the probability distribution of the random variable $\phi$ and is symmetric around $\phi = 0$.

According to the results in [23], the maximal transmission distance is positively correlated with the amplitude of the reference pulse. However, an extra excess noise proportional to the amplitude of the reference pulse will be generated due to the finite dynamics of Alice's amplitude modulator [26]. Therefore, an arbitrary large amplitude of the reference pulse is not proper, and a more realistic value, such as $E_R^2 = 20V_A$, will be rational. Unfortunately, this realistic value will restrict the maximal transmission distance of the SR CV-QKD protocol to a fairly low level, as illustrated in Section 4 later on. This issue will hinder the practical application of the SR CV-QKD scheme.

## 3. SR CV-QKD with Virtual Photon Subtraction

Photon subtraction can improve the entanglement of the two-mode squeezed vacuum (TMSV) state and hence enhance the performance of the system. In order to make the description of our scheme self-contained, we first start with the basics of photon subtraction on a TMSV state. Figure 2 describes the entire steps of the EB CV-QKD scheme with photon subtraction. An entanglement source $|\lambda\rangle$ is used to produce the TMSV state and $|\lambda\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty} \lambda^n |n, n\rangle$. Then, Alice performs heterodyne detection on mode $A$ and sends mode $B$ to a beam splitter (BS) with transmittance $\tau$. The mode $B$ is split into modes: $B'$ and $B_1$. The modes $A$, $B'$, $B_1$ form a tripartite state $\rho_{AB'B_1}$,

$$\rho_{AB'B_1} = U_{BS}[|\lambda\rangle\langle\lambda| \otimes |0\rangle\langle 0|]U_{BS}^{\dagger}. \tag{2}$$

The photon number resolving detector (PNRD) is used to perform the positive operator-valued measure (POVM) $\{\hat{\Pi}_0, \hat{\Pi}_1\}$ on mode $B'$ [37]. Only when the POVM elements $\hat{\Pi}_1$ click, the mode $A$ and $B_1$ can be kept. The kept state is given by:

$$\rho_{AB_1}^{\hat{\Pi}_1} = \frac{tr_{B'}(\hat{\Pi}_1\rho_{AB'B_1})}{tr_{AB'B_1}(\hat{\Pi}_1\rho_{AB'B_1})}, \tag{3}$$

where $tr_x(\cdot)$ is the partial trace of the multimode quantum state and $P^{\hat{\Pi}_1} = tr_{AB'B_1}(\hat{\Pi}_1\rho_{AB'B_1})$ denotes the success probability of subtracting $k$ photons.

However, the straightforward application of the above photon subtraction to the SR CV-QKD is not a desirable method, in which the reference pulse will also pass through the BS and the hardware requirement will be enhanced. Fortunately, the EB CV-QKD scheme with photon subtraction can be equivalent to the PM CV-QKD scheme with virtual photon subtraction via non-Gaussian post-selection [33]. In the post-selection step, Alice uses a post-selection filter function $Q(\cdot)$, or acceptance probability, to decide which data will be accepted. The post-selection step is carried out after Bob has performed coherent detection, which means it will not change the Gaussian state $\rho_{AB_2}^G$ and the Gaussian process $\mathcal{G}$. The mode $B_2$ is the received mode at Bob's side. Therefore, we propose the scheme of SR CV-QKD with virtual photon subtraction, which can be realized via non-Gaussian post-selection. The schematic diagram of our scheme is described in Figure 3, where $\alpha = \sqrt{2\tau}\lambda\gamma/2$, and $\gamma$ is the measurement result of mode $A$ in the EB scheme, i.e., $\gamma = x_A + ip_A$. The modulation variance of $x_A$ and $p_A$ is $\widetilde{V} = (V+1)/2$, where $V = (1+\lambda^2)/(1-\lambda^2)$ is the variance of the TMVS state in the EB scheme. Hence, according to the derived results in [33], the covariance matrix $\bar{\gamma}^G_{AB_2}$ of the Gaussian state $\rho^G_{AB_2}$ for subtracting $k$ photons can rewrite Equation (1) as:

$$\bar{\gamma}^G_{AB_2} = \begin{pmatrix} V_A\mathbb{I} & \overline{C}\sigma_Z \\ \overline{C}\sigma_Z & V_B\mathbb{I} \end{pmatrix} \tag{4}$$

with:

$$\begin{aligned} V_A &= 2V_k - 1, & (5)\\ V_B &= T_e(2\tau\lambda^2 V_k + 1 + \chi), & (6)\\ \overline{C} &= 2\sqrt{T_e\tau}\lambda V_k\overline{\cos\phi}, & (7)\\ \chi &= \frac{(1-T_e)}{T_e} + \frac{\varepsilon_{el}}{T_e} + \varepsilon_c, & (8)\\ V_k &= \frac{k+1}{1-\tau\lambda^2}, & (9) \end{aligned}$$

where $\varepsilon_{el}$ is the electronic noise of the Bob's detector, $\varepsilon_c$ is the channel excess noise and $T_e = T\eta$.

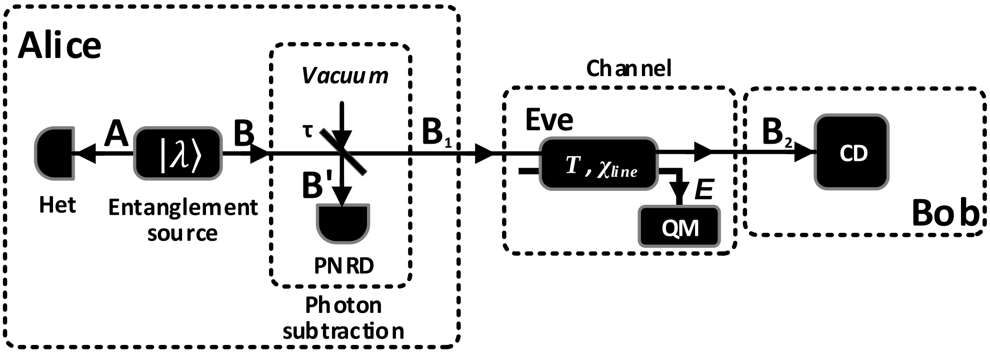


**Figure 2.** Schematic of EB CV-QKD with photon subtraction. PNRD: photon number resolving detector; Het: heterodyne detection; CD: coherent detection; QM: quantum memory.

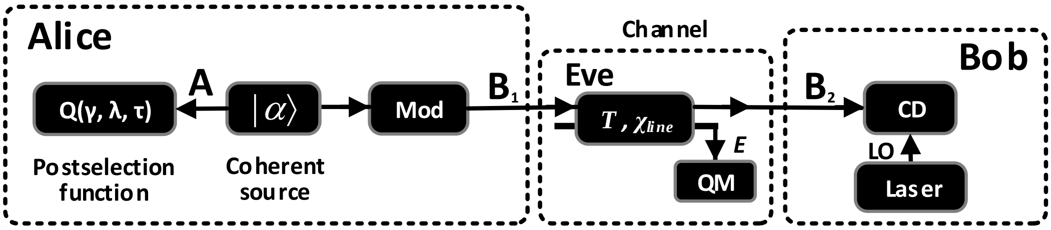


**Figure 3.** Schematic of PM SR CV-QKD with virtual photon subtraction. QM: quantum memory; CD: coherent detection; Mod: Gaussian modulator.

## 4. Performance Analysis

Usually, the secret key rate of the TMSV state is no less than the secret key rate of the equivalent Gaussian state, which shares an identical covariance matrix due to the extremality of Gaussian state [38–40]. Hence, we will use $\bar{\gamma}^G_{AB_2}$ to derive the lower bound of the secret key rate. Besides, the acceptance probability for each of the data in the post-selection step should also be taken into account. This probability is equivalent to the success probability of Alice's POVM measurement $P^{\hat{\Pi}_1}$ and can be treated as a scaling factor.

### *4.1. Individual Attacks*

The lower bound of the secret key rate of our scheme against individual attack for reverse reconciliation is:

$$K_{min}^{ind} = P^{\hat{\Pi}_1}(\beta I_{AB}^{G} - I_{EB}), \tag{10}$$

where $P^{\hat{\Pi}_1} = \frac{1-\lambda^2}{1-\tau\lambda^2}\left[\frac{\lambda^2(1-\tau)}{1-\tau\lambda^2}\right]^k$ [33], $I_{AB}^{G}$ is the mutual information between Alice's and Bob's measurements, $I_{EB}$ is mutual information between Eve's and Bob's measurements and $\beta$ is the reconciliation efficiency.

From the covariance matrix in Equation (4) and the derived results in [23], the mutual information between Alice's and Bob's measurements $I_{AB}^{G}$ can be written as:

$$I_{AB}^{G} = \frac{1}{2}\log_2\left(\frac{V'}{V_{A|B}}\right) \tag{11}$$

with $V' = (V_A + 1)/2$ and $V_{A|B} = V' - \overline{C}^2/2V_B$. Through the relationship:

$$1 - \overline{cos\phi}^2 = V_{\hat{\theta}} = \frac{\chi + 1}{V_R} + \frac{\delta_R}{T\eta V_R}, \tag{12}$$

we can get:

$$\overline{C}^2 = 4T_e\tau\lambda^2 V_k^2\overline{cos\phi}^2 = 4T_e\tau\lambda^2 V_k^2(1 - V_{\hat{\theta}}), \tag{13}$$

where $V_R = E_R^2$, $\delta_R = 1$ for single-reference-pulse mode and $V_{\hat{\theta}}$ is the variance of the estimated deviation angle $\hat{\theta}$. The upper bound of mutual information between Eve's and Bob's measurements can be given by:

$$I_{EB} = \frac{1}{2}\log_2\left(\frac{V_B}{V_{B|E}}\right) = \frac{1}{2}\log_2\left(V_B V_{B|A}\right) \tag{14}$$

with $V_{B|A} = V_B - \overline{C}^2/V_A$.

### *4.2. Collective Attacks*

The asymptotic secret key rate against collective attacks for reverse reconciliation can be given by:

$$K_{min}^{col} = P^{\hat{\Pi}_1}(\beta I_{AB}^{G} - \chi_{BE}^{G}), \tag{15}$$

where $I_{AB}^{G}$ is given by Equation (11) and $\chi_{BE}^{G}$ is the maximal stolen information. The maximal stolen information $\chi_{BE}^{G}$ can be written as:

$$\chi_{BE}^{G} = G\left(\frac{\lambda_1 - 1}{2}\right) + G\left(\frac{\lambda_2 - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right), \tag{16}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2(x)$ is the von Neumann entropy of a thermal state. The eigenvalues $\lambda_1$ and $\lambda_2$ are obtained from:

$$\lambda_{1,2}^2 = \frac{1}{2}\left(\Delta \pm \sqrt{\Delta^2 - 4D^2}\right) \tag{17}$$

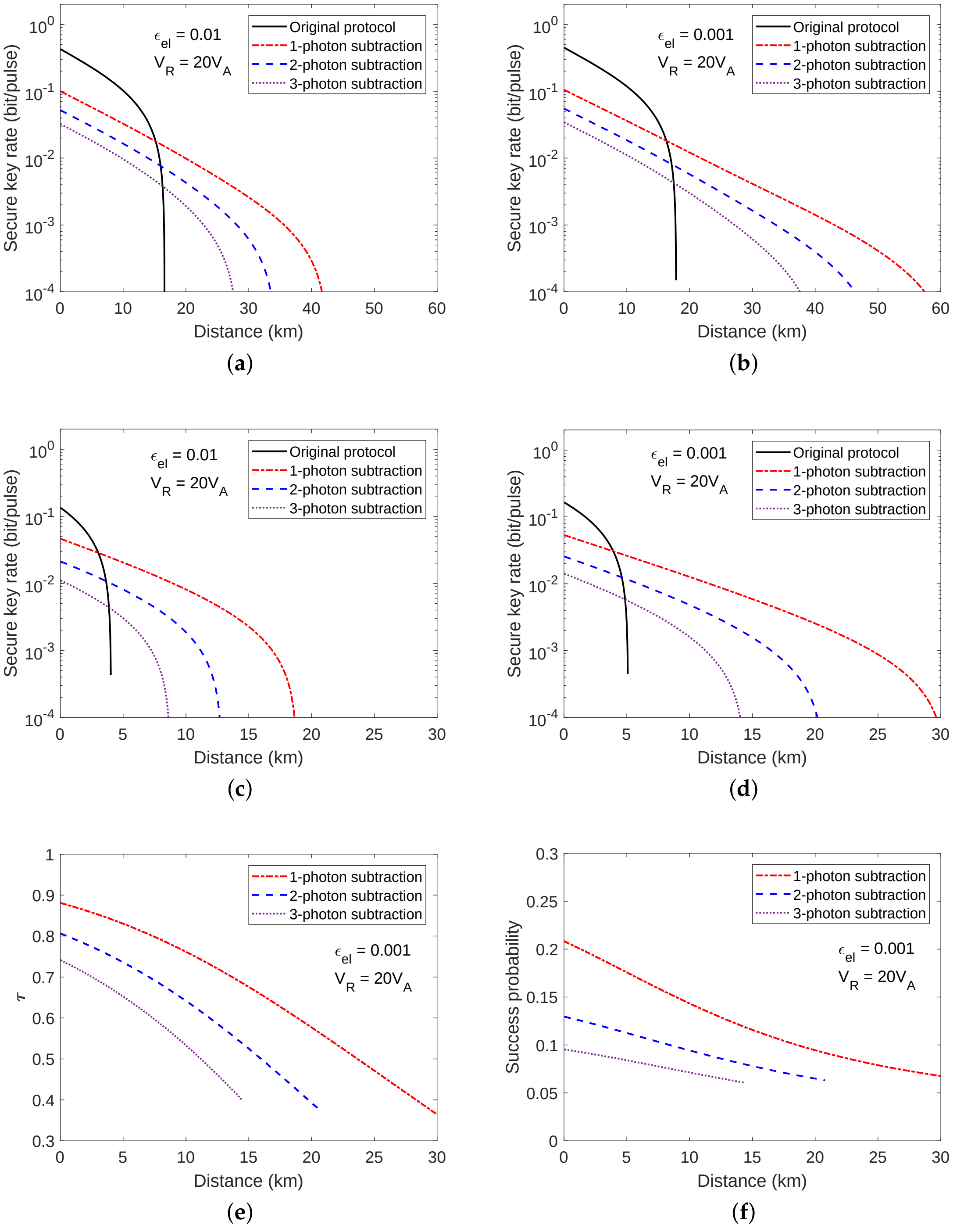
with $\Delta = V_A^2 + V_B^2 - 2\overline{C}^2$ and $D = V_A V_B - \overline{C}^2$. The square of symplectic eigenvalue $\lambda_3$ reads:

$$\lambda_3^2 = V_A(V_A - \frac{\overline{C}^2}{V_B}). \tag{18}$$

In what follows, we will assume that $V_A = 40$, $\beta = 0.95$, $\varepsilon_c = 0.01$, $\eta = 0.719$ and $\alpha = 0.2$ dB/km [23]. All the variances in this paper are in shot-noise units. Figure 4 shows our simulation results against individual and collective attacks. Figure 4a–d gives the maximum secure key rate at each transmission distance for all possible $\tau$ of Alice's BS. Note, due to the excess noise contributed by the leakage of reference pulses, here, $V_R$ is set to a more realistic value of $20V_A$, and thus, we neglect this excess noise (about $8 \times 10^{-4}$ when the dynamics of Alice's amplitude modulator is 60 dB) [26]. The figures show a considerable maximal transmission distance improvement when the photon subtraction operation is applied in the SR CV-QKD scheme, especially in the case of subtracting one photon. Furthermore, we find that our scheme of SR CV-QKD with virtual photon subtraction is sensible with the detector electronic noise. A lower electronic noise can result in a larger maximal transmission distance, as shown in Figure 4b,d. We note that the electronic noise of 0.001 is achievable, which is demonstrated in [41]. However, the secure key rate is worse than the original protocol in the short distance region. The main reason for this phenomenon is that the limited acceptance probability degrades the final key rate. $\tau$ is a key parameter, which should be determined in advance. Figure 4e shows the optimal $\tau$ at each distance for the maximum secure key rate in Figure 4d. The optimal $\tau$ decreases along with the increasing of the transmission distance, which implies a accurate estimation of $\tau$ is required for each distance. Figure 4f represents the success probability of subtracting $k$ ($k$ = 1, 2, 3) photons at each distance for the maximum secure key rate in Figure 4d. Although the success probability will be larger in the region of large $\tau$, a large success probability does not mean a large secure key rate, especially when the transmission distance becomes longer. This is because $\tau$ not only impacts the success probability, but also the entire key generation. We did not draw the optimal $\tau$ and the success probability of subtracting $k$ photons at each distance for the maximum secure key rate in Figure 4c, as their results are similar to the case when the electronic noise is 0.001.

From a practical point of view, if the secure key rate varies rapidly with $\tau$ around its optimal value, the accurate estimation of the optimal $\tau$ will need complicated implementations. Fortunately, around the optimal value of $\tau$, the secure key rate varies slowly with the change of $\tau$ at each distance, as shown in Figure 5. Particularly, between the upper bound (black dashed line) and lower bound (red dashed line) of $\tau$ at a specific distance, the secure key rate can maintain more than 90% of its optimal value ($K_{opt}$).

Another aspect of our scheme is the tolerable excess noise. As shown in Figure 6a,b, we depict the relationship between the maximal tolerable excess noise and the transmission distance for different electronic noise and all possible $\tau$. The original scheme is outperformed by the protocol of using photon subtraction at all transmission distance ranges, which implies the advantage of using photon subtraction, which increases the maximal tolerable excess noise for distant users. Moreover, if the channel is less noisy, for example, $\varepsilon_c \approx 0.005$, the one photon subtraction can expand the maximal transmission distance to 20 km for $\varepsilon_{el} = 0.01$ and 33 km for $\varepsilon_{el} = 0.001$. As the tolerable excess noise is not affected by the acceptance probability, the optimal $\tau$ for the maximal tolerable excess noise at each distance is different from that of the one for the maximum secure key rate, as shown in Figure 6c,d.



(**a**) (**b**)

(**c**) (**d**)

(**e**) (**f**)

**Figure 4.** The simulation results against individual and collective attacks. (**a**,**b**) give the maximum secure key rate as a function of the transmission distance against individual attacks, when changing the transmittance $\tau$ of Alice's beam splitter (BS); (**c**,**d**) give the maximum secure key rate against collective attacks; (**e**) shows the optimal $\tau$ corresponding to (d); (**f**) is the success probability of subtracting kphotons at each transmission distance corresponding to (d). The black solid lines show the original SR-CV-QKD protocol without photon subtraction. Other lines represent one-photon subtraction (red dashed-dotted lines), two-photon subtraction (blue dashed lines), three-photon subtraction (violet dotted lines).

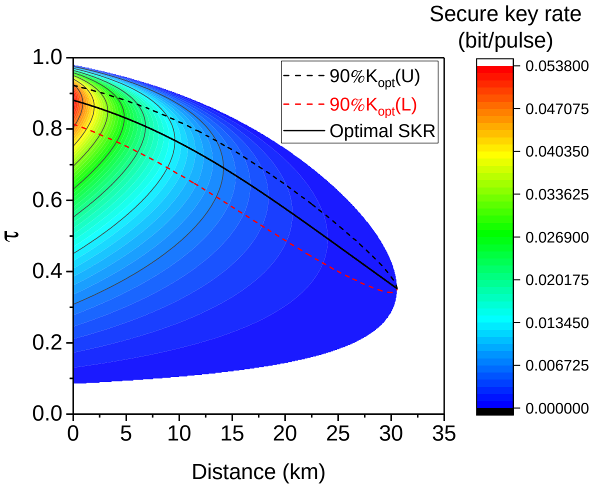


**Figure 5.** The secure key rate as a function of transmission distance and $\tau$ of Alice's BS, when the electronic noise is 0.001. The black solid line is the optimal $\tau$, while the secure key rate reaches its maximal value at each distance. The black (red) dashed line is the upper (lower) bound of $\tau$, when its secure key rate is 90% of its maximum at that distance.

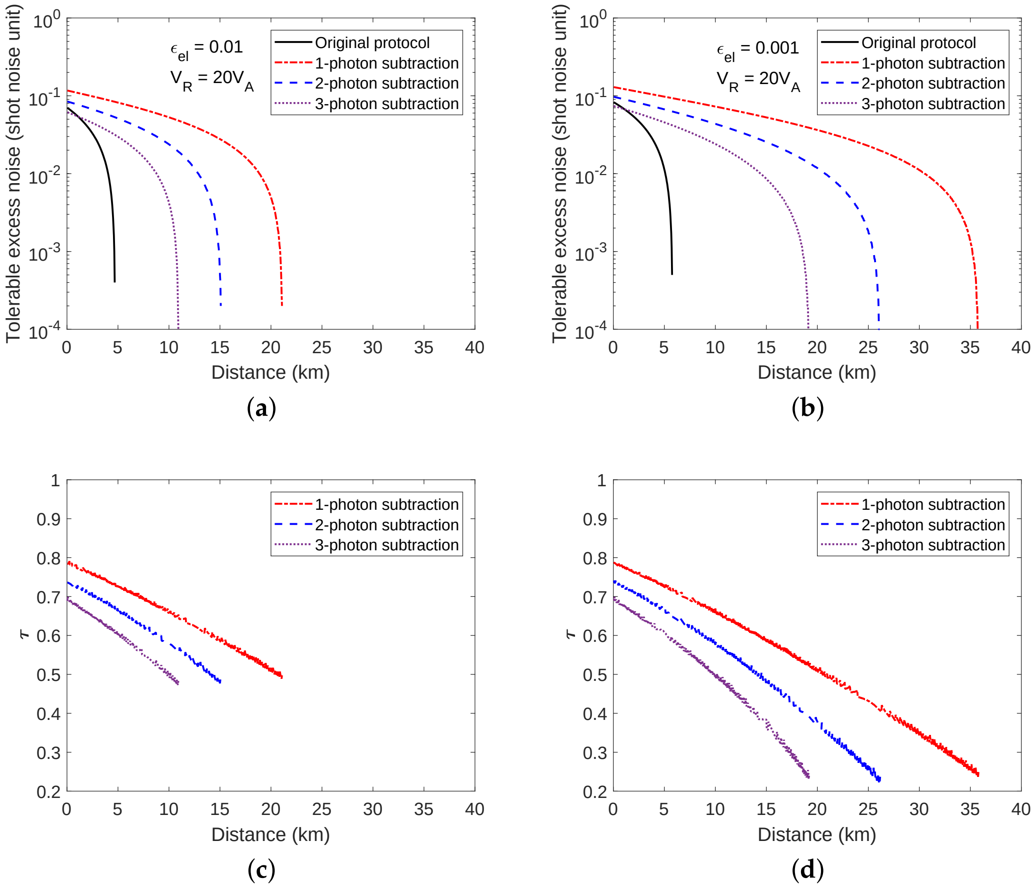


**Figure 6.** The maximal tolerable excess noise and its corresponding value of $\tau$ at each distance. (**a**,**b**) are the maximal tolerable excess noise at each distance for all possible $\tau$ when electronic noise is equal to 0.01 and 0.001; (**c**,**d**) are the optimal $\tau$ for the maximal tolerable excess noise corresponding to (a,b).

Actually, many protocols have investigated the CV-QKD with virtual photon subtraction. All of them can significantly improve the maximal transmission distance of the CV-QKD protocols. In [33], the method of virtual photon subtraction was firstly used in the conventional one-way GMCS CV-QKD scheme, the LO of which is co-transmitted with the quantum signal. The maximal transmission distance can be extended from 90–220 km (144% improvement). The protocol of two-way GMCS CV-QKD with virtual photon subtraction was investigated in [35]. The maximal transmission distance can be extended from 85–310 km (266% improvement). In [34], the four-state CV-QKD protocol combined with virtual photon subtraction can extend the maximal transmission distance from 140–330 km (136% improvement). For the protocol of measurement-device-independent CV-QKD with virtual photon subtraction, the maximal transmission distance can be extended from 42–68 km (62% improvement) [36]. In our scheme of SR CV-QKD with virtual photon subtraction, we also obtained a considerable extension of the maximum transmission distance when the detector electronic noise was 0.001. The maximum transmission distance increased from 18–58 km (222% improvement) under individual attack and from 5–30 km (500% improvement) under collective attacks, which makes possible the application of the SR CV-QKD from the laboratory to an actual metropolitan area. If we increase the amplitude of the reference pulse appropriately and control the reference pulse's leakage noise in a certain range, the maximum transmission distance can be extended further. For example, if $V_R = 50V_A$ and the detector electronic noise is equal to 0.001, the maximal transmission distance can be extended from 15–40 km. In practice, the imperfection of the detector will constrain the performance of the CV-QKD protocol. Therefore, any imperfection of the detector should be taken into account, while this was not considered in [34,36,37].

## 5. Conclusions

In this paper, we proposed the scheme of SR CV-QKD with virtual photon subtraction. It not only has no need to increase the physical complexity of the original SR CV-QKD system, but also can extend the maximal transmission distance without increasing the intensity of the reference pulse. Performance analysis results show that a considerable extension of maximal transmission distance can be obtained, especially for one-photon subtraction. Meanwhile, the scheme of SR CV-QKD with virtual photon subtraction is sensible with the detector's electronic noise. A longer maximal transmission distance can be obtained when the electronic noise is lower. Furthermore, it is more tolerable against excess noise for our scheme compared to the original protocol, which implies the advantage of using virtual photon subtraction to increase the maximal tolerable excess noise for distant users. These results suggest that under existing technology, our modified scheme of the SR CV-QKD can make possible the SR CV-QKD from the laboratory to practical metropolitan area application. However, we note that the gap between practical implementations and the theoretical analysis here should be taken into account. Any imperfection factors in the practical experiment should introduce corresponding parameters. This issue is not included in the scope of the present analysis, and deserves further study.

**Author Contributions:** Y.G. gave the general idea of the study, designed the conception of the study and performed critical revision of the manuscript. H.Z. accomplished the formula derivation and numerical simulations and drafted the article. X.W. conceived of and designed the study. Q.L. provided feasible advice and critical revision of the manuscript. X.W. provided critical revision of the manuscript. Y.W. provided critical advice and reviewed relevant studies and literature. All authors have read and approved the final manuscript.

**Acknowledgments:** This work was supported by the National Natural Science Foundation of China (Grant No. 61572529).

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

## References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*; IEEE Press: New York, NY, USA, 1984; pp. 175–179.
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]

3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The Security of Practical Quantum Key Distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301. [CrossRef]
4. Lo, H.-K.; Curty, M.; Tamaki, K. Secure Quantum Key Distribution. *Nat. Photonics* **2014**, *8*, 595. [CrossRef]
5. Grosshans, F.; Grangier, P. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]
6. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513. [CrossRef]
7. Wang, X.B.; Hiroshima, T.; Tomita, A.; Hayashi, M. Quantum information with gaussian states. *Phys. Rep.* **2007**, *44*, 1. [CrossRef]
8. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621. [CrossRef]
9. Ma, H.-X.; Bao, W.-S.; Li, H.-W. Quantum hacking of two-way continuous-variable quantum key distribution using Trojan-horse attack. *Chin. Phys. B* **2016**, *25*, 080309. [CrossRef]
10. Liu, W.-Q.; Peng, J.-Y.; Huang, P.; Huang, D.; Zeng, G.-H. Monitoring of continuous-variable quantum key distribution system in real environment. *Opt. Express* **2017**, *25*, 19429. [CrossRef] [PubMed]
11. Huang, P.; Huang, J.-Z.; Wang, T.; Li, H.-S.; Huang, D.; Zeng, G.-H. Robust continuous-variable quantum key distribution against practical attacks. *Phys. Rev. A* **2017**, *95*, 052302. [CrossRef]
12. Guo, Y.; Xie, C.L.; Liao, Q.; Zhao, W.; Zeng, G.H.; Huang, D. Entanglement-distillation attack on continuous-variable quantum key distribution in a turbulent atmospheric channel. *Phys. Rev. A* **2017**, *96*, 022320. [CrossRef]
13. Guo, Y.; Xie, C.L.; Huang, P.; Zhang, L.; Huang, D.; Zeng, G.H. Channel-parameter estimation for satellite-to-submarine continuous-variable quantum key distribution. *Phys. Rev. A* **2018**, *97*, 052326. [CrossRef]
14. Guo, Y.; Li, R.J.; Liao, Q.; Zhou, J.; Huang, D. Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier. *Phys. Lett. A* **2018**, *382*, 372–381. [CrossRef]
15. Grosshans, F. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 020504. [CrossRef] [PubMed]
16. Navascues, M.; Acín, A. Security bounds for continuous variables quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 020505. [CrossRef] [PubMed]
17. Leverrier, A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
18. Huang, J.-Z.; Weedbrook, C.; Yin, Z.-Q.; Wang, S.; Li, H.-W.; Chen, W.; Guo, G.-C.; Han, Z.-F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **2013**, *87*, 062329. [CrossRef]
19. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.-M. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A* **2013**, *87*, 052309. [CrossRef]
20. Qin, H.; Kumar, R.; Alléaume, R. Saturation attack on continuous-variable quantum key distribution system. *Proc. SPIE* **2013**, *8899*, 88990N.
21. Jouguet, P.; Kunz-Jacques, S.; Diamanti, E. Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution. *Phys. Rev. A* **2013**, *87*, 062313. [CrossRef]
22. Ma, X.-C.; Sun, S.-H.; Jiang, M.-S.; Liang, L.-M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **2013**, *88*, 022339. [CrossRef]
23. Soh, D.B.S.; Brif, C.; Coles, P.J.; Lütkenhaus, N.; Camacho, R.M.; Urayama, J.; Sarovar. M. Self-Referenced Continuous-Variable Quantum Key Distribution Protocol. *Phys. Rev. X* **2015**, *5*, 041010. [CrossRef]
24. Qi, B.; Lougovski, P.; Pooser, R.; Grice, W.; Bobrek, M. Generating the Local Oscillator Locally in Continuous-Variable Quantum Key Distribution Based on Coherent Detection. *Phys. Rev. X* **2015**, *5*, 041009. [CrossRef]
25. Huang, D.; Huang, P.; Lin, D.-K.; Wang, C.; Zeng, G.-H. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **2015**, *40*, 3695. [CrossRef] [PubMed]
26. Marie, A.; Alléaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *95*, 012316. [CrossRef]
27. Opatrný, T.; Kurizki, G.; Welsch, D.-G. Improvement on teleportation of continuous variables by photon subtraction via conditional measurement. *Phys. Rev. A* **2000**, *61*, 032302. [CrossRef]
28. Kim, M.S.; Park, E.; Knight, P.L.; Jeong, H. Nonclassicality of a photon-subtracted Gaussian field. *Phys. Rev. A* **2005**, *71*, 043805. [CrossRef]

29. Kitagawa, A.; Takeoka, M.; Sasaki, M.; Chefles, A. Entanglement evaluation of non-Gaussian states generated by photon subtraction from squeezed states. *Phys.Rev. A* **2006**, *73*, 042310. [CrossRef]
30. Navarrete-Benlloch, C.; García-Patrón, R.; Shapiro, J.H.; Cerf, N.J. Enhancing quantum entanglement by photon addition and subtraction. *Phys. Rev. A* **2012**, *86*, 012328. [CrossRef]
31. Huang, P.; He, G.-Q.; Fang, J.; Zeng, G.H. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **2013**, *87*, 012317. [CrossRef]
32. Guo, Y.; Liao, Q.; Wang, Y.-J.; Huang, D.; Huang, P.; Zeng, G.-H. Performance improvement of continuous-variable quantum key distribution with an entangled source in the middle via photon subtraction. *Phys. Rev. A* **2017**, *95*, 032304. [CrossRef]
33. Li, Z.-Y.; Zhang, Y.-C.; Wang, X.-Y.; Xu, B.-J.; Peng, X.; Guo, H. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **2016**, *93*, 012310. [CrossRef]
34. Liao, Q.; Guo, Y.; Huang, D.; Huang, P.; Zeng, G.-H. Long-distance continuous-variable quantum key distribution using non-Gaussian state-discrimination detection. *New J. Phys.* **2018**, *20*, 023015. [CrossRef]
35. Zhao, Y.-J.; Zhang, Y.-C.; Li, Z.-Y.; Yu, S.; Guo, H. Improvement of two-way continuous-variable quantum key distribution with virtual photon subtraction. *Quantum Inf. Process.* **2017**, *16*, 184. [CrossRef]
36. Zhao, Y.-J.; Zhang, Y.-C.; Xu, B.-J.; Yu, S.; Guo, H. Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction. *Phys. Rev. A* **2018**, *97*, 042328. [CrossRef]
37. Eisaman, M. D.; Fan, J.; Migdall, A.; Polyakov, S.V. Invited Review Article: Single-photon sources and detectors. *Rev. Sci. Instrum.* **2011**, *82*, 071101. [CrossRef] [PubMed]
38. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502. [CrossRef] [PubMed]
39. García-Patrón, R.; Cerf, N.J. Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.
40. Wolf, M.M.; Giedke, G.; Cirac, J.I. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.* **2006**, *96*, 080502. [CrossRef] [PubMed]
41. Huang, D.; Huang, P.; Lin, D.-K.; Zeng, G.-H. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **2016**, *6*, 19201. [CrossRef] [PubMed]

© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).