symmetry

MDPI

*Article*

# Security Analysis of Imperfect Gaussian Modulation Caused by Amplitude Modulator in Continuous–Variable Quantum Key Distribution

**Zhenghua Li [1], Xiangyu Wang [1,*], Ziyang Chen [2,*], Bingjie Xu [3] and Song Yu [1]**

[1] State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China

[3] Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China

* Correspondence: xywang@bupt.edu.cn (X.W.); chenziyang@pku.edu.cn (Z.C.)

**Abstract:** Continuous-variable quantum key distribution (CV–QKD) is a system that provides secret keys for symmetric key systems. In the application of CV–QKD, the practical security of the system is crucial. In this article, we investigate the practical security issues caused by non–ideal Gaussian modulation, which is caused by fitting defects of the amplitude modulator's (AM) modulation curve. We provide the effect of fitting error on parameter estimation. We also give the relationship between the fitting order and the secret key rate. The simulation results indicate that the system is completely unable to communicate during first–order fitting. During second–order fitting, the system's performance decreases by more than half. During third–order fitting, the system's performance will be consistent with the ideal. Therefore, to ensure the performance of the CV–QKD system, the fitting order must be at least three or higher.

**Keywords:** continuous–variable quantum key distribution; non–ideal Gaussian modulation; parameter estimation; secret key rate

check for updates

**Citation:** Li, Z.; Wang, X.; Chen, Z.; Xu, B.; Yu, S. Security Analysis of Imperfect Gaussian Modulation Caused by Amplitude Modulator in Continuous–Variable Quantum Key Distribution. *Symmetry* **2023**, *15*, 1452. https://doi.org/10.3390/sym15071452

Academic Editor: Christos Volos

Received: 21 June 2023
Revised: 14 July 2023
Accepted: 17 July 2023
Published: 20 July 2023

## 1. Introduction

Continuous–variable quantum key distribution (CV–QKD) can allow Alice and Bob to complete secure communication over untrusted channels [1–4]. The CV–QKD system has unconditional security. So, people have conducted in-depth research on the security of CV–QKD. Nowadays, the security of CV–QKD has been proven in many aspects [5–9]. In addition, due to the greater compatibility between CV–QKD and existing communication systems [10], CV–QKD experiments have been completed in various scenarios [11–18], especially in networked applications [19–23]. From the perspective of modulation format, CV–QKD can be divided into discrete modulation and Gaussian modulation CV–QKD. Among them, Gaussian modulation CV–QKD has a more comprehensive security proof and has received widespread attention.

In practical environments, the Gaussian modulation CV–QKD experimental system will generate security loopholes due to the non–ideality of the device [24,25]. Eve can attack these security loopholes, such as local oscillator fluctuation attacks, detector saturation attacks, etc. [26–29], making the system no longer secure. In order to resist these attacks, many new protocols, such as continuous–variable one–sided device–independent (CV–1SDI) and continuous–variable measurement device–independent (CV–MDI QKD), have been proposed [30–32]. But these new protocols are often more complex to implement. A more direct and effective method is to eliminate errors by adding feedback control or real–time monitoring, such as analyzing the preparation of imperfect Gaussian states or analyzing measurement angle errors [33–39].

In the entanglement–based (EB) model of Gaussian-modulated CV–QKD, the Gaussian state is obtained by performing Gaussian operations on the quadrature components of the light field. In the corresponding prepare–and–measure (PM) model, it is difficult to directly modulate the quadrature components, so it is usually indirect to modulate the amplitude and phase to prepare Gaussian states. In experiments, amplitude and phase modulation are usually achieved using a lithium niobate–based amplitude modulator (AM) and phase modulator. However, the input and output of the AM are not linear. So, we need to generate Gaussian data by fitting a modulation curve. A too–low fitting order will cause errors in the Gaussian data. The non–ideal Gaussian state can lead to security loopholes in CV–QKD. So, analyzing the impact of the non–linearity of the AM on the security of Gaussian-modulated CV–QKD systems is worthy of in–depth research.

In this article, we analyze the impact of non–ideal Gaussian modulation on the performance of the CV–QKD system from multiple perspectives. This non–ideal Gaussian modulation is caused by the fitting error of the AM modulation curve. Specifically, we analyze the changes in excess noise and transmittance under different fitting orders from the perspective of parameter estimation. Furthermore, we analyze the changes in the secret key rate under different fitting orders. Our research results indicate that in the case of low–order fitting (first and second orders), the excess noise (transmittance) is 0.19 (0.019), which is significantly different from the ideal excess noise (transmittance) of 0.01 (0.1). In addition, during first–order fitting, there is no secret key rate, and during second–order fitting, the secret key rate will also be greatly reduced. So, only when third–order fitting is above, the performance of the CV–QKD system can approach ideal performance.

This paper is organized as follows. In Section 2, we give expressions for the quadrature components under ideal and non–ideal Gaussian modulation. In Section 3, we conduct security analysis, mainly including parameter estimation and secret key rate. In Section 4, we simulate and analyze the transmittance, excess noise, and secret key rate under different fitting orders. In Section 5, we give the conclusions of this paper.

## 2. Non–Ideal Gaussian Modulation in CV–QKD System

In this section, we present the ideal Gaussian modulation implementation in the PM scheme. Next, we show that in practical systems, non–ideality in the modulation curve fitting of the AM can cause defects in the Gaussian modulation. In addition, we also give the quadrature components expression sent by Alice with or without non–ideal Gaussian modulation.

### *2.1. The Realization Process of Gaussian Modulation*

In this section, we illustrate how to realize the preparation of the Alice Gaussian state in EB in the PM scheme of CV–QKD; that is, the quadrature components are realized by modulating the amplitude and phase. In Gaussian modulation coherent–state (GMCS) CV–QKD, Alice needs to prepare the Gaussian state $|\alpha_{\mathrm{A}}\rangle$, $\alpha_{\mathrm{A}} = |\alpha_{\mathrm{A}}|e^{i\theta} = x + ip$, where $x$ and $p$ are independent quadrature components that conform to the Gaussian distribution

$$p(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{x^2}{2\sigma^2}) \quad p(p) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp(-\frac{p^2}{2\sigma^2}). \tag{1}$$

Since $x$ and $p$ are independent of each other, their joint density distribution is

$$p(x,p) = p(x)p(p) = \frac{1}{2\pi\sigma^2} \exp(-\frac{x^2+p^2}{2\sigma^2}). \tag{2}$$

In practical systems, it is difficult to directly modulate the quadrature components $x$ and $p$ of the light field state. So, let $x = A\cos\theta$ and $p = A\sin\theta$, where $A$ is the amplitude, and $\theta$ is the phase. By transforming the probability density matrix

$$|J| = \begin{vmatrix} \frac{\partial x}{\partial A} & \frac{\partial p}{\partial A} \\ \frac{\partial x}{\partial \theta} & \frac{\partial p}{\partial \theta} \end{vmatrix}, \tag{3}$$

we can further obtain

$$P(A,\theta) = P(x,p)|J| = \frac{A}{2\pi\sigma^2}\exp\left(-\frac{A^2}{2\sigma^2}\right). \tag{4}$$

We can regard Equation (4) as the joint probability density of $p(A)$ satisfying the Rayleigh distribution and $p(\theta)$ satisfying the uniform distribution:

$$p(A) = \frac{A}{\sigma^2}\exp\left(-\frac{A^2}{2\sigma^2}\right) \quad p(\theta) = \frac{1}{2\pi}. \tag{5}$$

At this point, we will correspond the modulation of $x$ and $p$ to the modulation of $A$ and $\theta$. So, in practical systems, we can achieve Gaussian modulation through amplitude and phase modulators. According to the Box–Muller method [40], the amplitude and phase can be obtained from two independent $U_1$ and $U_2$ uniformly distributed within the [0, 1] interval:

$$A = \sqrt{-2V_{\mathrm{A}}\ln U_1} \quad \theta = 2\pi U_2. \tag{6}$$

$x$ and $p$ can be expressed as:

$$x = A\cos\theta = \sqrt{-2V_{\mathrm{A}}\ln U_1}\cos(2\pi U_2), \tag{7}$$

$$p = A\sin\theta = \sqrt{-2V_{\mathrm{A}}\ln U_1}\sin(2\pi U_2). \tag{8}$$

### 2.2. Non–Ideal Gaussian Modulation Caused by Amplitude Modulator Curve

In this section, we point out that during the Gaussian modulation process, the non–ideal fitting of the modulation curve of the AM can cause defects in Gaussian modulation. As mentioned in Section 2.1, in practical systems, Gaussian modulation is achieved through AM and phase modulation. For the phase modulator, its modulation principle can be described as

$$\alpha_{\mathrm{out}} = \alpha_{\mathrm{in}}\exp\left(j\frac{V_{\mathrm{PM}}}{V_\pi}\pi\right), \tag{9}$$

where $V_{\mathrm{PM}}$ is the modulation voltage of the phase modulator, $V_\pi$ is the half–wave voltage value of the phase modulator, and $\alpha_{\mathrm{in}}$ and $\alpha_{\mathrm{out}}$ are the input and output of the optical field. According to Equation (9), the angle change of the phase modulator is linearly related to the modulation voltage. So, after knowing the half–wave voltage, we can directly adjust the modulation voltage $V_{\mathrm{PM}} = 2\pi U_2 V_\pi/\pi$ to achieve the ideal phase modulation. For AM, their modulation principle can be described as

$$\alpha_{\mathrm{out}} = \alpha_{\mathrm{in}}[1 - \cos(\pi V_{\mathrm{AM}}/V_\pi)]/2. \tag{10}$$

According to Equation (10), the equation of the modulation curve is

$$\eta_t = \frac{\alpha_{\mathrm{out}}}{\alpha_{\mathrm{in}}} = [1 - \cos(\pi V_{\mathrm{AM}}/V_\pi)]/2. \tag{11}$$

According to Equation (11), the input and output of the AM are non–linear, as shown in Figure 1. Under ideal amplitude modulation, we make $\alpha_{\text{out}} = \sqrt{-2V_A \ln U_1}$, and the modulation voltage value $V_{\text{AM}}$ is

$$V_{\text{AM}} = \frac{V_\pi}{\pi} \arccos\left(1 - \frac{2\sqrt{-2V_A \ln U_1}}{\alpha_{\text{in}}}\right). \tag{12}$$

By loading $V_{\text{PM}}$, $V_{\text{AM}}$ can achieve ideal Gaussian modulation, and the output ideal Gaussian state is

$$\alpha_{\text{ideal}} = \alpha_{\text{in}} \exp\left(j\frac{V_{\text{PM}}}{V_\pi}\pi\right)[1 - \cos(\pi V_{\text{AM}}/V_\pi)]/2. \tag{13}$$

Its quadrature components are expressed as

$$x_{\text{ideal}} = \alpha_{\text{in}} \cos\left(\frac{V_{\text{PM}}}{V_\pi}\pi\right)[1 - \cos(\pi V_{\text{AM}}/V_\pi)]/2, \tag{14}$$

$$p_{\text{ideal}} = \alpha_{\text{in}} \sin\left(\frac{V_{\text{PM}}}{V_\pi}\pi\right)[1 - \cos(\pi V_{\text{AM}}/V_\pi)]/2. \tag{15}$$

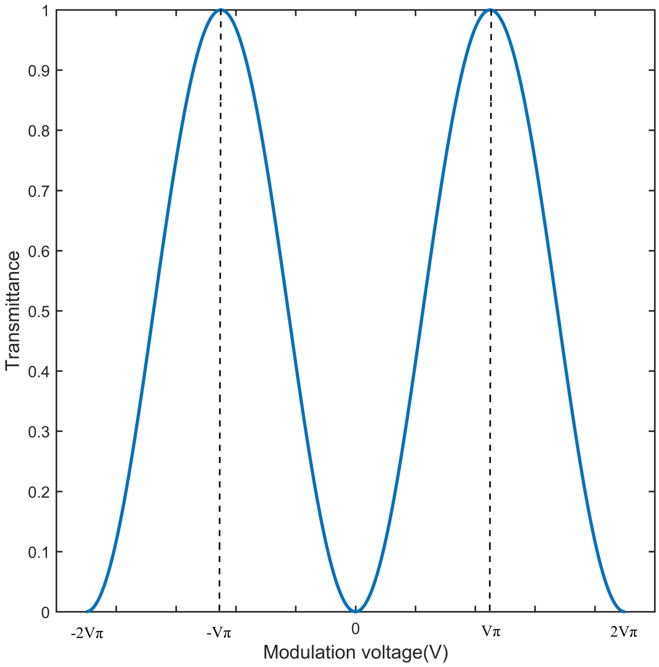

**Figure 1.** Modulation curve of amplitude modulator.

However, in practical Gaussian modulation, we do not know the ideal modulation curve of the AM. In order to obtain the modulation curve of the desired AM, we need to provide a stepped signal to the AM, record its input and output $(x_i, y_i)$, and then obtain the modulation curve by fitting $(x_i, y_i)$

$$y_i = \sum_{n=1}^{N} a_n {x_i}^n. \tag{16}$$

During the fitting process, there may be some errors that cannot be completely consistent with the ideal curve. This leads to an error between the modulation voltages $V'_{\text{AM}}$ and $V_{\text{AM}}$ calculated based on Equation (16),

$$V'_{\text{AM}} = V_{\text{AM}} + \Delta V. \tag{17}$$

where $\Delta V$ is the modulation voltage error caused by curve fitting. At this point, the actual modulated quadrature components are

$$x_{\text{fact}} = \alpha_{\text{in}} \cos\left(\frac{V_{\text{PM}}}{V_\pi}\pi\right)[1 - \cos(\pi V'_{\text{AM}}/V_\pi)]/2, \tag{18}$$

$$p_{\text{fact}} = \alpha_{\text{in}} \sin\left(\frac{V_{\text{PM}}}{V_\pi}\pi\right)[1 - \cos(\pi V'_{\text{AM}}/V_\pi)]/2. \tag{19}$$

By combining formulas Equations (13)–(19), it can be concluded that the modulation curve of the AM is non–linear, which leads to a larger $\Delta V$ in lower order fitting, resulting in a larger error between $(x_{\text{fact}}, p_{\text{fact}})$ and $(x_{\text{idea}}, p_{\text{idea}})$, which seriously affects the safety of the system.

## 3. Practical Security Analysis of Non–ideal Gaussian Modulation

In this section, we investigate the impact of non–ideal Gaussian modulation caused by the AM on system security in actual CV–QKD systems. Our research includes the impact of transmittance and excess noise on the parameter estimation process. In addition, we further provide a calculation method for the secret key rate.

### *3.1. Parameter Estimation under Non–ideal Gaussian Modulation*

In the GMCS CV–QKD system, we generally regard the quantum channel as a linear channel. Under the assumption of this linear channel, the relationship between Alice and Bob's data is

$$y = tx + z, \tag{20}$$

where $x$ is the data at Alice, $y$ is the data received at Bob, $t$ is the equivalent transmittance, and $z$ is the noise item, mainly including shot noise, electrical noise, and excess noise. According to the relationship described in Equation (20), we can obtain that the data received by Bob are

$$x_{\text{B}} = \sqrt{\eta T}(x_{\text{A}} + x_\varepsilon) + x_{\text{ele}} + N_0, \tag{21}$$

$x_{\text{B}}$ represents the data after balance homodyne detection at the Bob, $\eta$ and $x_{\text{ele}}$ is the detection efficiency and electrical noise of the detector, $x_{\text{A}}$ is the Gaussian data prepared by Alice, $x_\varepsilon$ is the excess noise introduced by the system, $T$ is the transmission of the channel, and $N_0$ is the shot noise.

After the above derivation, we learn the specific expression of $x_{\text{A}}$ and $x_{\text{B}}$. Next, we need to use the variance and covariance of $x_{\text{A}}$ and $x_{\text{B}}$ to estimate $T$ and $\varepsilon$,

$$\left\langle x_{\text{A}}^2 \right\rangle = V_{\text{A}}, \tag{22}$$

$$\left\langle x_{\text{B}}^2 \right\rangle = \eta T(V_{\text{A}} + \varepsilon) + 1 + v_{\text{ele}}, \tag{23}$$

$$\langle x_{\text{A}} x_{\text{B}} \rangle = \sqrt{\eta T} V_{\text{A}}, \tag{24}$$

where $V_{\text{A}}$ is the modulation variance, $\varepsilon$ is the excess noise, and $v_{\text{ele}}$ is the electrical noise variance. The units of these values are shot noise units. According to Equations (22)–(24), we can derive the expressions for $T$ and $\varepsilon$ as follows:

$$T = \frac{\langle x_{\text{A}} x_{\text{B}} \rangle^2}{\eta \left\langle x_{\text{A}}^2 \right\rangle^2}, \tag{25}$$

$$\varepsilon = \frac{\left\langle x_{\text{B}}^2 - 1 - v_{\text{ele}} \right\rangle}{\left(\langle x_{\text{A}} x_{\text{B}} \rangle / \left\langle x_{\text{A}}^2 \right\rangle\right)^2} - \left\langle x_{\text{A}}^2 \right\rangle. \tag{26}$$

When there is an error in the modulation curve fitted by the AM, Gaussian modulation will have defects. At this point, $x_{\mathrm{A}}$ and $x_{\mathrm{B}}$ become $x_{\mathrm{A}}^{'}$ and $x_{\mathrm{B}}^{'}$, which are brought into Equations (25) and (26) as follows:

$$T^{'} = \frac{\left\langle x_{\mathrm{A}} x_{\mathrm{A}}^{'} \right\rangle^2}{\langle x_{\mathrm{A}}^2 \rangle^2} T, \tag{27}$$

$$\varepsilon^{'} = \frac{\left\langle x_{\mathrm{A}}^{'2} \right\rangle + \varepsilon}{(\langle x_{\mathrm{A}} x_{\mathrm{A}}^{'} \rangle / \langle x_{\mathrm{A}}^2 \rangle)^2} - \left\langle x_{\mathrm{A}}^2 \right\rangle. \tag{28}$$

From Equations (27) and (28), it can be seen that when there is non–ideal Gaussian modulation, $T^{'}, \varepsilon^{'}$ and $T, \varepsilon$ are not the same. This difference will lead to parameter estimation error and further lead to a decrease in secret key rate, resulting in security loopholes.

### *3.2. Calculation of Secret Key Rate*

In this section, we derive the secret key rate of the GMCS CV–QKD protocol. We select the most widely used GG02 protocol for analysis. In the GG02 protocol, we consider reverse reconciliation collective attacks, whose secret key rate can be expressed as

$$k = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{29}$$

where $\beta$ is the reverse reconciliation efficiency, $I_{\mathrm{AB}}$ is the mutual information between Alice and Bob, and $\chi_{\mathrm{BE}}$ is the information stolen by Eve according to Bob's information. $I_{\mathrm{AB}}$ and $\chi_{\mathrm{BE}}$ can be obtained through the covariance matrix $r_{\mathrm{AB}}$ of the system,

$$r_{\mathrm{AB}} = \begin{pmatrix} V\mathrm{II}_2 & \sqrt{\eta T(V^2-1)}\sigma_z \\ \sqrt{\eta T(V^2-1)}\sigma_z & (\eta T(V-1+\varepsilon)+1+v_{\mathrm{ele}})\mathrm{II}_2 \end{pmatrix}, \tag{30}$$

where $V = V_{\mathrm{A}} + 1$, $\mathrm{II}_2$ is the unit variance of $2 \times 2$, and $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Mutual information $I_{\mathrm{AB}}$ can be solved through the variance and conditional variance of Bob's data:

$$I_{\mathrm{AB}} = \frac{1}{2} \log\left(\frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}}\right), \tag{31}$$

where $V_{\mathrm{B}} = \eta T(V-1+\varepsilon) + 1 + v_{\mathrm{ele}}$ and $V_{\mathrm{B|A}} = \eta T\varepsilon + 1 + v_{\mathrm{ele}}$. In addition,

$$\chi_{\mathrm{BE}} = S(E) - S(E|x_{\mathrm{B}}), \tag{32}$$

where $S(E)$ represents the von Neumann entropy for Eve to master the quantum state, and $S(E|x_{\mathrm{B}})$ is the conditional entropy for mastering the quantum state after knowing Bob's measurement results. Due to Eve's purification effect, $\chi_{\mathrm{BE}}$ can be rewritten as

$$\chi_{\mathrm{BE}} = S(\rho_{\mathrm{AB}}) - S(\rho_{\mathrm{AB}}|x_{\mathrm{B}}). \tag{33}$$

In this way, both $S(\rho_{\mathrm{AB}})$ and $S(\rho_{\mathrm{AB}}|x_{\mathrm{B}})$ can be solved based on the covariance matrix $r_{\mathrm{AB}}$. Since it has been proven that Gaussian state attacks are optimal collective attacks, considering Gaussian attacks, $\chi_{\mathrm{BE}}$ can be further simplified as

$$\chi_{\mathrm{BE}} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{34}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, $\lambda_{1,2}$ is the symplectic eigenvalue of the covariance matrix of quantum state $\rho_{AB}$, and $\lambda_{3,4,5}$ is the symplectic eigenvalue of the covariance matrix of quantum state $\rho_{AB|x_B}$. The solution for $\lambda_{1,2}$ is as follows:

$$\lambda_{1,2} = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \tag{35}$$

where $A = V^2(1-2T) + 2T + T^2(V + 1/T - 1 + \varepsilon)^2$, and $B = T^2[V(1/T - 1 + \varepsilon) - 1]^2$. Next, $\lambda_{3,4,5}$ can be solved by the covariance matrix $r_{\mathrm{A}|x_B}$,

$$r_{\mathrm{A}|x_B} = r_{\mathrm{A}} - r_{\mathrm{AB}}(Xr_{\mathrm{B}}X)^{MP}{r_{\mathrm{AB}}}^T, \tag{36}$$

where $X = diag(1,0,1,0,\ldots)$, MP is the Moore–Penrose inverse of the matrix. At this point, we can obtain

$$\lambda_{3,4} = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \tag{37}$$

where

$$C = \frac{A[(1-\eta+v_{\mathrm{ele}})/\eta] + V\sqrt{B} + T(V + 1/T - 1 + \varepsilon)}{T\{V + [\eta T(\varepsilon - 1) + 1 + v_{\mathrm{ele}}]/\eta T\}}, \tag{38}$$

$$D = \sqrt{B}\frac{V + \sqrt{B}[(1-\eta+v_{\mathrm{ele}})/\eta]}{T\{V + [\eta T(\varepsilon - 1) + 1 + v_{\mathrm{ele}}]/\eta T\}}. \tag{39}$$

Finally, the data of $\lambda_5$ in different scenarios are all 1. Through the derivation of Equations (29)–(39), we obtain the final secret key rate k.

## 4. Simulation and Analysis

This section simulates and analyzes the impact of non–ideal Gaussian on the CV–QKD system. Firstly, we provide the impact of different fitting orders on the generated Gaussian data. Then, we analyze the changes in transmittance and excess noise under different fitting orders. Finally, we analyze the changes in the secret key rate under different fitting orders.

In the Gaussian coherent-state protocol, Alice needs to prepare data that conform to the Gaussian distribution. However, due to the non–ideality of the AM modulation curve fitting, there is a certain error between the prepared data and the ideal Gaussian distribution. So, we conducted simulation research on the Gaussian distribution under different fitting orders. In the simulation, we set $V_{\mathrm{A}} = 4$, and the results are shown in Figure 2.

Figure 2a shows the ideal Gaussian distribution, while Figure 2b–d show the Gaussian distribution under first–order, second–order, and third–order fitting, respectively. The reason why we only reach the third–order is because we found that the Gaussian distribution produced by third–order fitting and higher–order fitting is almost identical. From Figure 2, it is evident that compared to the ideal Gaussian distribution, when the fitting order is lower (first–order, second–order), the non–ideal Gaussian modulation is greater. It is not until after the third order that a more ideal Gaussian distribution can be obtained. This indicates that in practical systems, we should use at least third–order or higher fitting to generate Gaussian data.

Through Equations (18) and (19) in Section 2.2, we can know that when there is an error in Gaussian modulation, it will have an impact on the transmittance and excess noise of the actual system. Therefore, we simulated and analyzed the changes in transmittance and excess noise under different fitting orders, and the results are shown in Figure 3.

In the simulation, we set the ideal excess noise to 0.01 and the transmittance to 0.1. From Figure 3, we can clearly see that during the first–order and second–order fitting, there will be errors in parameter estimation, and it will not be consistent with the theoretical value until after the third order. In particular, in the first order, the transmittance is 0.019, and the excess noise is 0.19. In this case, there is no secret key generation, which has a serious impact on the performance of the system. This further indicates that in practical systems, we should pay attention to the impact of the AM modulation curve on the system and use high–order fitting for modulation.

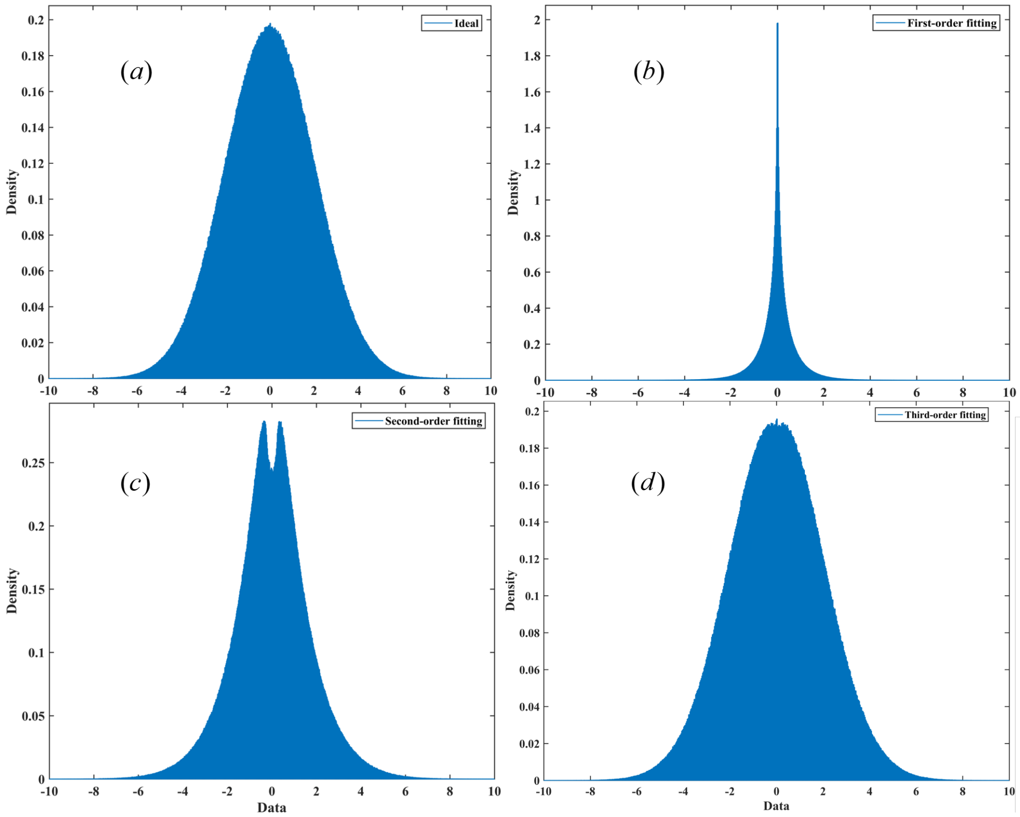

**Figure 2.** The Gaussian distribution under different fitting orders, including (**a**) ideal Gaussian distribution, (**b**) first–order fitting, (**c**) second–order fitting, and (**d**) third–order fitting.

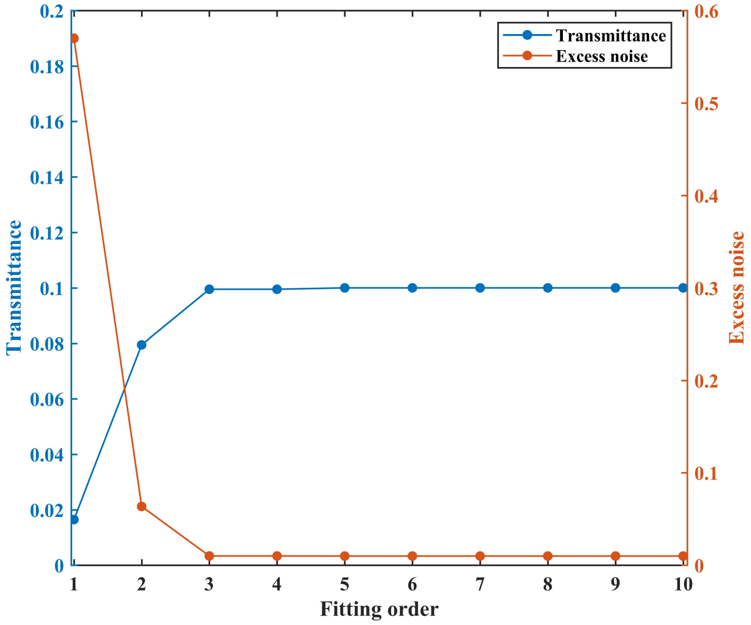

**Figure 3.** The changes in excess noise and transmittance under different fitting orders. The red dotted line represents excess noise, and the blue dotted line represents transmittance. The ideal transmittance is 0.1 and the ideal excess noise is 0.01.

For the CV–QKD system, the size of excess noise has a significant impact on the secret key rate. According to Equation (26) in Section 3, the magnitude of excess noise is correlated with the variance of the modulation data. So, we conducted simulation research on its specific relationship, and the results are shown in Figure 4.

In the simulation, the ideal excess noise is set to 0.01. We can clearly conclude from the simulation that the size of excess noise is directly proportional to the modulation variance during the first–order and second–order fitting. In first–order fitting, for every 1 change in variance, the excess noise increases by 0.1853. In second–order fitting, for every 1 change in variance, the excess noise increases by 0.0271. It does not change with the modulation variance during the third–order fitting. In summary, when the fitting order is less than three, excess noise will significantly increase with modulation variance, leading to a decrease in system performance.

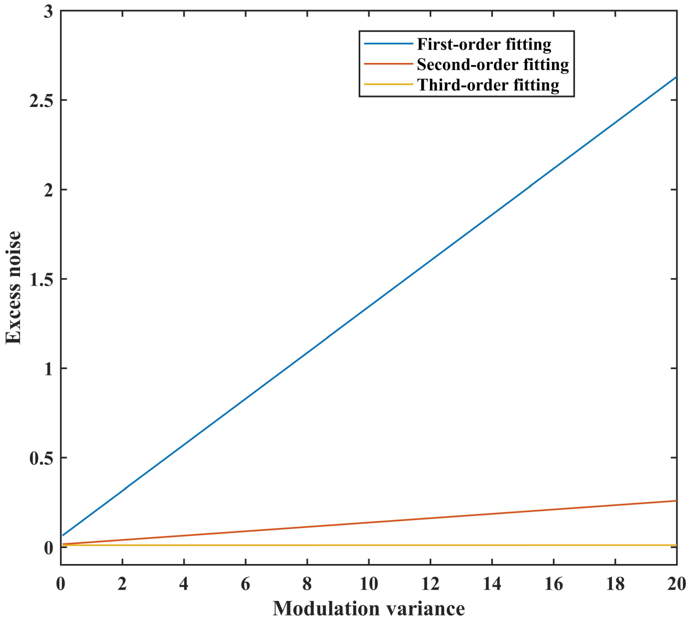

**Figure 4.** The relationship between excess noise and modulation variance under different fitting orders. The blue line represents first–order fitting, the red line represents second–order fitting, and the yellow line represents third–order fitting. The ideal excess noise is set to 0.01.

In the process of parameter estimation, transmittance is also important. We also analyzed the relationship between transmittance and modulation variance. The results are shown in Figure 5. The ideal transmittance is set to 0.1. From Figure 5, we can clearly see that under the first–order, second–order, and third–order fitting, the transmittance does not change with the magnitude of modulation variance. The magnitude of transmittance is only related to the order of fitting. During first–order fitting, the estimated transmittance is 0.017. During second–order fitting, the estimated transmittance is 0.067. When fitting in the third order, it is the same as the ideal transmittance. Therefore, when we use too–low order fitting of the modulation curve of the AM, it will lead to severe inaccuracy in the estimation of transmittance, especially when the first–order is used.

The performance of the CV–QKD system is mainly evaluated through secret key rate and transmission distance. So, we simulated the changes in the secret key rate and transmission distance under different fitting orders, as shown in Figure 6. In Figure 6, we set the $V_A$ as 4, the $\eta$ as 0.613, the $v_{ele}$ as 0.01, and the $\beta$ as 0.95. The blue solid line represents second–order fitting, the black solid line represents ideal fitting, and the red dashed line represents third–order fitting. Due to the severe non–ideal Gaussian modulation during first–order fitting, when the modulation variance is 4, which cannot generate a secret key rate. So, the first–order fitting situation is not shown in Figure 6. In Figure 6, we can observe that compared to ideal Gaussian modulation, the transmission distance and secret key rate reduce by half during second–order fitting. When fitting in the third–order, the secret key rate and transmission distance are almost consistent with ideal Gaussian modulation.

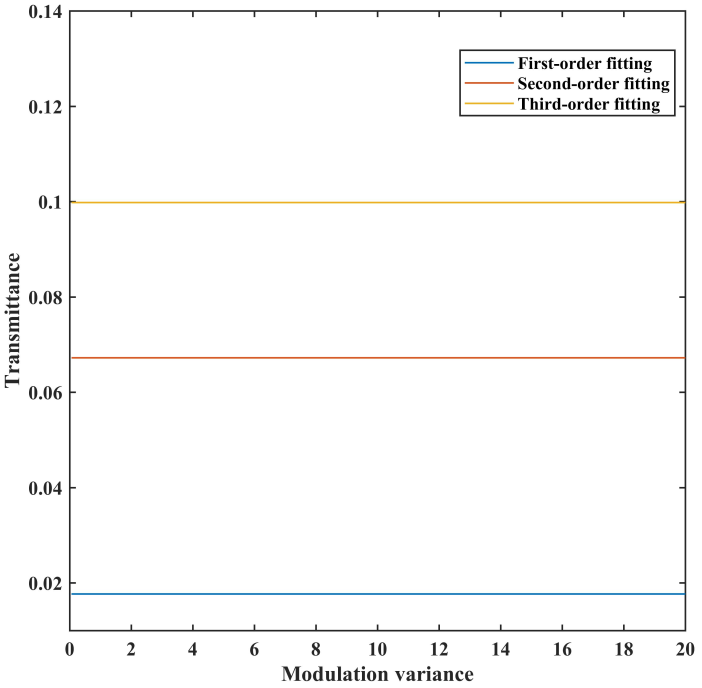

**Figure 5.** The relationship between transmittance and modulation variance under different fitting orders. The blue line represents first–order fitting, the red line represents second–order fitting, and the yellow line represents third–order fitting. The ideal transmittance is set to 0.1.

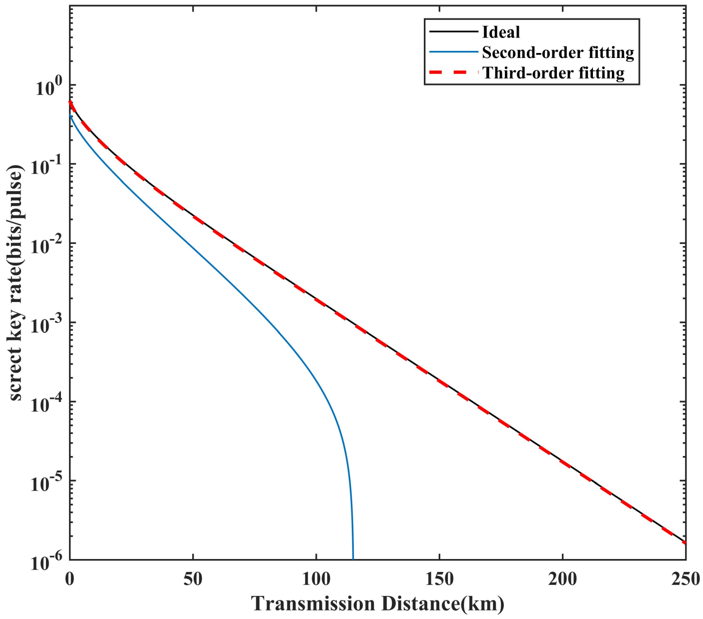

**Figure 6.** Under different fitting orders, the security key rate of CV–QKD. The blue solid line represents second–order fitting, the red dashed line represents third–order fitting, and the black solid line represents the ideal Gaussian distribution. $V_A = 4$, $V_{ele} = 0.01$, $\eta = 0.613$, and $\beta = 0.95$.

## 5. Conclusions

In a word, we analyzed the impact of non–ideal Gaussian modulation on the CV–QKD system. The non–ideality of Gaussian modulation is mainly caused by defects in the fitting of AM modulation curves. In addition, the parameter estimation error is related to the order of fitting and modulation variance. When the fitting order is low (first–order and second–order), the parameter estimation error is relatively large, while when the fitting order is high (above third–order), the parameter estimation error is relatively small (ignored). We further found that during the first–order and second–order fitting, excess noise linearly increases with $V_A$. During the first– order, the slope of change is 0.1853, and during the second–order, the slope of change is 0.0271. In addition, the transmittance does not vary with $V_A$. When fitting above the third–order, the transmittance and excess noise do not vary with $V_A$. Finally, during first–order fitting, the CV–QKD system cannot generate a secret key, and during second–order fitting, its transmission distance will decrease by half. The third–order or higher is consistent with the ideal transmission distance. Therefore, in practical applications, we need to use at least third–order fitting to achieve a CV–QKD system. Our work thoroughly analyzed the impact of non–ideal modulation curve fitting on the performance of CV–QKD systems from multiple perspectives, providing theoretical guidance for the practical application of CV–QKD. However, our work did not take into account other non–ideal factors, such as the bias point of the intensity modulator.

**Author Contributions:** Conceptualization, Z.L., X.W., Z.C. and B.X.; Methodology, Z.L.; Software, Z.L.; Formal analysis, Z.L. and X.W.; Investigation, Z.L.; Resources, X.W. and S.Y.; Writing—original draft, Z.L.; Writing—review and editing, X.W., Z.C., B.X. and S.Y.; Visualization, Z.C. and B.X.; Supervision, X.W.and S.Y.; Project administration, X.W. and Z.Chen.; Funding acquisition, X.W., Z.C.and B.X. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported by the National Natural Science Foundation of China under Grant Nos. 62001041 and 62201012, the Fundamental Research Funds of BUPT under Grant No. 2022RC08, the Fund of State Key Laboratory of Information Photonics and Optical Communications under Grant No. IPOC2022ZT09, and the stability Program of Science and Technology on Communication Security Laboratory (2022).

**Data Availability Statement:** Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

**Conflicts of Interest:** All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

## References

1. Laudenbach, F.; Pacher, C.; Fung, C.H.F.; Poppe, A.; Peev, M.; Schrenk, B.; Hentschel, M.; Walther, P.; Hübel, H. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. *Adv. Quantum Technol.* **2018**, *1*, 1800011.
2. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236.
3. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002.
4. Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum Cryptography—A Simplified Undergraduate Experiment and Simulation. *Physics* **2022**, *4*, 104–123. [CrossRef]
5. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **2015**, *114*, 070501. [CrossRef] [PubMed]
6. Leverrier, A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. *Phys. Rev. Lett.* **2017**, *118*, 200501. [CrossRef] [PubMed]
7. Lin, J.; Upadhyaya, T.; Lütkenhaus, N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Phys. Rev. X* **2019**, *9*, 041064. [CrossRef]
8. Ghorai, S.; Grangier, P.; Diamanti, E.; Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **2019**, *9*, 021059. [CrossRef]

9. Wang, X.; Xu, M.; Zhao, Y.; Chen, Z.; Yu, S.; Guo, H. Non-Gaussian reconciliation for continuous-variable quantum key distribution. *Phys. Rev. Appl.* **2023**, *19*, 054084. [CrossRef]
10. Chen, Z.; Wang, X.; Yu, S.; Li, Z.; Guo, H. Continuous-mode quantum key distribution with digital signal processing. *NPJ Quantum Inf.* **2023**, *9*, 28. [CrossRef]
11. Laudenbach, F.; Schrenk, B.; Pacher, C.; Hentschel, M.; Fung, C.H.F.; Karinou, F.; Poppe, A.; Peev, M.; Hübel, H. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum* **2019**, *3*, 193.
12. Roumestan, F.; Ghazisaeidi, A.; Renaudier, J.; Vidarte, L.T.; Diamanti, E.; Grangier, P. High-rate continuous variable quantum key distribution based on probabilistically shaped 64 and 256-QAM. In Proceedings of the 2021 European Conference on Optical Communication (ECOC), IEEE, Bordeaux, France, 13–16 September 2021; pp. 1–4.
13. Pan, Y.; Wang, H.; Shao, Y.; Pi, Y.; Li, Y.; Liu, B.; Huang, W.; Xu, B. Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. *Opt. Lett.* **2022**, *47*, 3307–3310. [PubMed]
14. Wang, X.; Wang, H.; Zhou, C.; Chen, Z.; Yu, S.; Guo, H. Continuous-variable quantum key distribution with low-complexity information reconciliation. *Opt. Express* **2022**, *30*, 30455–30465.
15. Tian, Y.; Wang, P.; Liu, J.; Du, S.; Liu, W.; Lu, Z.; Wang, X.; Li, Y. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. *Optica* **2022**, *9*, 492–500.
16. Sarmiento, S.; Etcheverry, S.; Aldama, J.; López, I.; Vidarte, L.; Xavier, G.B.; Nolan, D.; Stone, J.; Li, M.; Loeber, D.; et al. Continuous-variable quantum key distribution over a 15 km multi-core fiber. *New J. Phys.* **2022**, *24*, 063011.
17. Wang, T.; Xu, Y.; Zhao, H.; Li, L.; Huang, P.; Zeng, G. Multi-rate and multi-protocol continuous-variable quantum key distribution. *Opt. Lett.* **2023**, *48*, 719–722.
18. Aldama, J.; Sarmiento, S.; Etcheverry, S.; Valivarthi, R.; Grande, I.L.; Vidarte, L.T.; Pruneri, V. Small-form-factor Gaussian-modulated coherent-state transmitter for CV–QKD using a gain-switched DFB laser. *Opt. Express* **2023**, *31*, 5414–5425.
19. Huang, D.; Huang, P.; Li, H.; Wang, T.; Zhou, Y.; Zeng, G. Field demonstration of a continuous-variable quantum key distribution network. *Opt. Lett.* **2016**, *41*, 3511–3514. [PubMed]
20. Huang, Y.; Shen, T.; Wang, X.; Chen, Z.; Xu, B.; Yu, S.; Guo, H. Realizing a downstream-access network using continuous-variable quantum key distribution. *Phys. Rev. Appl.* **2021**, *16*, 064051.
21. Milovančev, D.; Vokić, N.; Laudenbach, F.; Pacher, C.; Hübel, H.; Schrenk, B. High rate CV–QKD secured mobile WDM fronthaul for dense 5G radio networks. *J. Light. Technol.* **2021**, *39*, 3445–3457.
22. Wang, X.; Chen, Z.; Li, Z.; Qi, D.; Yu, S.; Guo, H. Experimental upstream transmission of continuous variable quantum key distribution access network. *Opt. Lett.* **2023**, *48*, 3327–3330. [PubMed]
23. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 839–894.
24. Ridene, S. Novel T-shaped GaSb/InAsN quantum wire for mid-infrared laser applications. *Phys. Lett. A* **2017**, *381*, 3324–3331.
25. Ridene, R.; Mastour, N.; Gamra, D.; Bouchriha, H. Energetic behavior of excitons in hybrid organic–inorganic parabolic quantum dots and its electric field dependence. *Int. J. Mod. Phys. B* **2015**, *30*, 1550211.
26. 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]
27. 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.
28. 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]
29. 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]
30. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.
31. Gehring, T.; Händchen, V.; Duhme, J.; Furrer, F.; Franz, T.; Pacher, C.; Werner, R.F.; Schnabel, R. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nat. Commun.* **2015**, *6*, 8795.
32. Walk, N.; Hosseini, S.; Geng, J.; Thearle, O.; Haw, J.Y.; Armstrong, S.; Assad, S.M.; Janousek, J.; Ralph, T.C.; Symul, T.; et al. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. *Optica* **2016**, *3*, 634–642.
33. Liu, W.; Wang, X.; Wang, N.; Du, S.; Li, Y. Imperfect state preparation in continuous-variable quantum key distribution. *Phys. Rev. A* **2017**, *96*, 042312.
34. Li, Z.; Wang, X.; Chen, Z.; Shen, T.; Yu, S.; Guo, H. Impact of non-orthogonal measurement in Bell detection on continuous-variable measurement-device-independent quantum key distribution. *Quantum Inf. Process.* **2023**, *22*, 236.
35. Wang, T.; Huang, P.; Wang, S.; Zeng, G. Polarization-state tracking based on Kalman filter in continuous-variable quantum key distribution. *Opt. Express* **2019**, *27*, 26689–26700. [PubMed]
36. Jain, N.; Derkach, I.; Chin, H.M.; Filip, R.; Andersen, U.L.; Usenko, V.C.; Gehring, T. Modulation leakage vulnerability in continuous-variable quantum key distribution. *Quantum Sci. Technol.* **2021**, *6*, 045001.
37. Shen, T.; Huang, Y.; Wang, X.; Tian, H.; Chen, Z.; Yu, S. Strengthening practical continuous-variable quantum key distribution against measurement angular error. *Opt. Express* **2021**, *29*, 30978–30990.

38. Muralekrishnan, R.; Venkatasubramani, L.N.; Mir, S.A.; Venkitesh, D. Influence of sub-system non–idealities on the performance of Gaussian modulated CV–QKD. In Proceedings of the 2022 Workshop on Recent Advances in Photonics (WRAP), IEEE, Mumbai, India, 4–6 March 2022; pp. 1–2.
39. Hajomer, A.A.; Jain, N.; Mani, H.; Chin, H.M.; Andersen, U.L.; Gehring, T. Modulation leakage-free continuous-variable quantum key distribution. *NPJ Quantum Inf.* **2022**, *8*, 136.
40. Scott, D.W. Box–muller transformation. *Wiley Interdiscip. Rev. Comput. Stat.* **2011**, *3*, 177–179. [CrossRef]

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.