mathematics

IMPACT FACTOR 2.4

CITESCORE 3.5

Article

Practical Security of Continuous Variable Quantum Key Distribution Ascribable to Imperfect Modulator for Fiber Channel

Shengzhe Xu, Zicheng Zhou and Ying Guo

Special Issue
Quantum Cryptography and Encryption

Edited by
Prof. Dr. Qiong Li and Dr. Ziyang Chen

MDPI

https://doi.org/10.3390/math12091356

mathematics

MDPI

Article

Practical Security of Continuous Variable Quantum Key Distribution Ascribable to Imperfect Modulator for Fiber Channel

Shengzhe Xu [1,2], Zicheng Zhou [2,3] and Ying Guo [2,4,*]

[1] School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China; alpaca@bupt.edu.cn
[2] School of Automation, Central South University, Changsha 410083, China; 2023201648@qdu.edu.cn
[3] School of Mathematics and Statistics, Qingdao University, Qingdao 266071, China
[4] School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
* Correspondence: guoying@bupt.edu.cn

Abstract: An amplitude modulator plays an essential role in the implementation of continuous-variable quantum key distribution (CVQKD), whereas it may bring about a potential security loophole in the practical system. The high-frequency modulation of the actual transmitter usually results in the high rate of the system. However, an imperfect amplitude modulator (AM) can give birth to a potential information leakage from the modulation of the transmitter. To reveal a potential security loophole from the high-frequency AM embedded in the transmitter, we demonstrate an influence on the practical security of the system in terms of the secret key rate and maximal transmission distance. The results indicate the risk of this security loophole in the imperfect AM-embedded transmitter. Fortunately, the legal participants can trace back the potential information leakage that has been produced from the imperfect transmitter at high frequencies, which can be used for defeating the leakage attack in CVQKD. We find the limitations of the imperfect AM-embedded transmitter of the high-frequency quantum system, and hence, we have to trade off the practical security and the modulation frequency of the AM-embedded transmitter while considering its implementation in a practical environment.

Keywords: continuous-variable; quantum key distribution; practical security

MSC: 81Pxx

Citation: Xu, S.; Zhou, Z.; Guo, Y. Practical Security of Continuous Variable Quantum Key Distribution Ascribable to Imperfect Modulator for Fiber Channel. *Mathematics* **2024**, *12*, 1356. https://doi.org/10.3390/math12091356

Academic Editor: Jonathan Blackledge

Received: 6 March 2024
Revised: 31 March 2024
Accepted: 11 April 2024
Published: 29 April 2024

1. Introduction

Quantum key distribution (QKD), which makes two distant parties Alice and Bob share a set of secret key, may be manipulated by a potential eavesdropper, Eve. Security of QKD has been proved on the basis of quantum mechanics. Discrete-variable QKD (DVQKD) has tended to be developed maturely, but it still faces challenges in the source preparation, the detection cost, and the secret key rate. Continuous-variable quantum key distribution (CVQKD) provides an approach to distilling the secret key among legal participants based on quantum mechanics [1]. There are several methods offered to improve the performance of the CVQKD system. For example, some operation schemes are performed in CVQKD, such as the local oscillator [2], photon subtraction, quantum photon catalysis [3], and so on. However, these CVQKD schemes require practical security proofs before being implemented. Others focus on increasing the frequency of the practical system, such as the modulation frequency of the transmitter, which has been usually proven to be a useful approach in the traditional CVQKD [4]. For QKD in discrete variables (DV), it can be brought down to finite dimensionality by compressed mappings or tagged state squarers. However, for QKD in continuous variables (CV), there is not an accurate modulation model to increase the performance of the transmitter in the practical system. Actually, the high-frequency transmitter has been employed for the performance improvement of the

CVQKD system. However, an imperfect pulse generation from the amplitude modulator (AM) embedded in the transmitter with high modulation frequencies can lead to a potential information leakage from the practical CVQKD system, which reveals a potential security loophole from the high-frequency AM embedded CVQKD system.

Currently, the security of the CVQKD system has been strictly proved in theoretics and experiments, whereas there are still potential vulnerabilities for practical implementations. The powerful eavesdropper called Eve may make use of some loopholes and perform attack strategies to steal the secret key from legal participants [5]. In addition, an eavesdropper can achieve the secret key from vulnerable channels while performing the known attack strategies, such as an intercept–resend attack [6], photon number splitting attacks [7], imperfect state preparation [8], and so on. The success of the above attack strategies depends much on imperfections of the channels deployed in CVQKD. These attacks are performed so as not to attack the actual device itself, avoiding the production of abnormal characteristics of the transmitted quantum signals. While performing the above-mentioned attack strategies, there usually exist some information leakages from the practical CVQKD system. Consequently, the potential security loopholes resulting from these attack strategies weaken the practical security of the CVQKD system. Moreover, an eavesdropper can directly perform attacking strategies on the devices themselves, such as a laser seeding attack [9], laser damage attack [10], wavelength attack [11], and the homodyne blinding attack [12], which weaken the practical security of the system itself. For example, when an eavesdropper injects the attacking light into the imperfect devices, he disrupts the regular signals of the devices and intercepts the transmitted photons from which the secret key can be extracted. Correspondingly, there exist several countermeasures that can be validly carried out to resist against these attack strategies, including a machine learning-based strategy [13], and so on. These countermeasures usually offer protection to some extent since attacking operations cause irregular features of the transmitted quantum signals, allowing us to carry out several effective countermeasure strategies.

Currently, there have been a number of imperfect devices embedded in the CVQKD system, such as the AM. In this paper, we consider the potential security loophole caused by the imperfect AM embedded in transmitter for the high-frequency modulation system. The main highlight of this work can be described as follows. We find that the high-frequency AM in transmitter sometimes generates imperfect light pulses in the high-frequency modulation, which initially provides a feasibility of information leakage in quantum communications. In addition, we find that the challenge of the AM-caused information leakage loophole be expanded with the increase of the maximal transmission distance.

This paper is organized as follows. In Section 2, we demonstrate the information leakage of the imperfect AM embedded in the high-frequency modulation CVQKD system. In Section 3, we evaluate the effects of the imperfect transmitter on the practical security of the CVQKD system. Finally, we draw a conclusion in Section 4.

2. AM-Embedded CVQKD

The frequency of the AM embedded in transmitter in the CVQKD system is crucial because it has an influence on performance of quantum information distilled from Alice and Bob. Before demonstrating the effect of the modulation frequencies on the CVQKD system, we have to describe the structure of the CVQKD system for design of AM-embedded modulation scheme, as follows.

In the initial stage, the modulator embedded in the transmitter generates the pulse light for quantum signals, as shown in Figure 1a. Fortunately, we find the appearance of the red pulse light for the high-frequency modulation at high frequencies, which brings out the imperfect signals and hence gives birth to a potential loophole of information leakage.

In the modulation stage, Alice selects the frequencies of the high-frequency transmitter. For frequencies less than 500 MHz, the output pulses are smooth and there exists only a single peak. Unfortunately, for the frequency of more than 1 GHz, there are two adjacent pulses, as illustrated in experiments and shown in Figure 1a, where the energy of the red

pulse is approximately half of the energy of the green one, which can be illustrated in experimental results of the imperfect transmitter with the modulation frequencies 100 MHz, 200 MHz, 400 MHz, 600 MHz, 800 MHz, 1 GHz, and 1.5 GHz respectively.

Motivated by characteristics above-mentioned, we suggest an attacking approach while taking into account the high-frequency modulator. We note that the AM-embedded transmitter, which is an actual gain adjustment of the avalanche photo-diode (APD), can be used for resisting this attack, based on the feedback of the response of detection that results in saturation. It can even be used for evaluating the practical security of the CVQKD system.

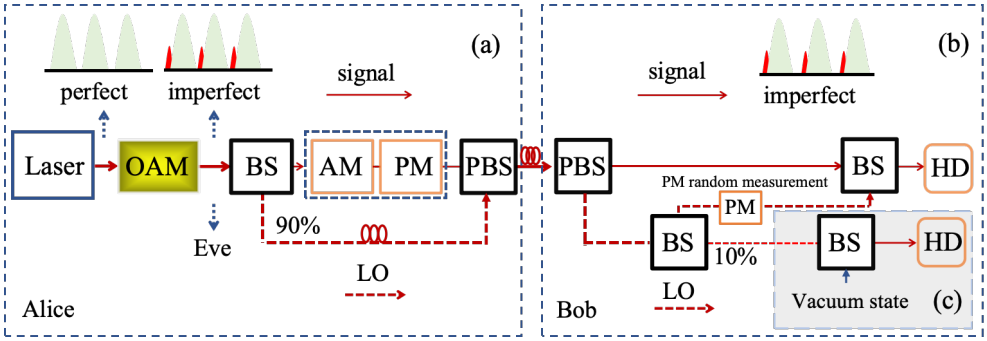

Figure 1. The implementation scheme of the CVQKD system embedded with the high-frequency AM. LO, local oscillator; BS, beam splitter; HD, homodyne detector; PM, phase modulator; OAM, imperfect amplitude modulator; AM, amplitude modulator; PBS, polarization beam splitter. (**a**) The transmitter, (**b**) the receiver, and (**c**) real-time short-noise measurement.

In the encoding stage, the sender Alice generates a series of Gaussian modulated-coherent states $|\alpha_A\rangle$ based on amplitude a and phase θ, where the state $|\alpha_A\rangle$ can be described as

$$|\alpha_A\rangle = ae^{i\theta} = x_A + ip_A. \tag{1}$$

Here, the notations $x_A = a\cos\theta$ and $p_A = a\sin\theta$ are both quadrature variables with the variance V and a mean of zero. Alice can regulate the values of x_A and p_A with the amplitude modulator (AM) and phase modulator (PM). Let x_A and p_A be two perfect quadrature variables of quantum signal A, and then, we obtain the output of the coherent state $|\alpha_A\rangle = x_A + ip_A$ with Gaussian modulation. The variance V of the quadrature variables x_A or p_A can be described by $V = 2\langle n\rangle$, which is the average number of photons for quantum signal A.

Normally, the variance V is achieved from the perfect green pulse light, whereas imperfections of the high-frequency transmitter are detected in experiments for a frequency of more than 1 GHz. In order to describe this process, we consider the parameter g, defined by $g = (I_{\text{red}} + I_{\text{green}})/I_{\text{green}}$, where I_{green} denotes the intensity of quantum signals and I_{red} is the intensity of the leaked light of the imperfect transmitter, respectively.

Due to the effects of the imperfect transmitter, the variations of the initial parameters x_A and p_A, and V can be described as

$$x'_A = \sqrt{g}x_A, p'_A = \sqrt{g}p_A, V' = gV, \tag{2}$$

where x'_A and p'_A are quadrature variables of the imperfect signal A' with the resulting variance V'. After that, the results' noisy signals are transmitted to the receiver Bob at the destination.

In the key-distillation stage, Bob receives the transmitted signals and performs the detection operation. Finally, the secret key can be generated after performing data post-processing. Due to the effects of the light leakage on the imperfect transmitter, the intensity of the local oscillator (LO) light deviates from its optimal value. Fortunately, the impact of optical attenuation on the LO light can be elegantly eliminated through using the real-time shot-noise measurement, as shown in Figure 1c, where Bob initially splits a part of the LO light into a balanced homodyne detector. The interference of the separated LO light and

the vacuum mode can be efficiently used for assessments of the variance of scattered noise. Furthermore, calibrating the linear relationship between the variance of scattered noise and the intensity of the LO light makes it feasible to evaluate the variance of scattered noise, while monitoring the intensity of the LO light at the receiver in real time.

We note that in the practical CVQKD, the AM-embedded transmitter is usually vulnerable and attackable. For example, the information leakage attack has been suggested for eavesdropping imperfect electronics in the homodyne detector. It can be used for attacking the actual devices of Gaussian-modulated coherent-state (GMCS)-involved CVQKD and discrete-modulation(DM)-involved CVQKD. The information leakage attack is feasible to resist the existing CVQKD because the coherent detector has a finite linearity domain that could be driven (if not being monitored) outside by displacing the mean value of the received quadratures. In addition, Eve can make use of heterodyne detection to measure both quadratures X and P intercepted, and subsequently prepare a fake coherent state according to her measurement results with displacements, which can be used for an amplification to compensate for the loss of heterodyne detection.

3. Performance Analysis

In what follows, we consider the performance of the proposed CVQKD system in terms of the derived secret key rate and the maximal transmission distance. After that, we demonstrate the practical security with numerical simulations.

3.1. Derivation of the Secret Key Rate

In order to show the performance of AM-embedded CVQKD with the high-frequency modulation, we describe the characteristics of the secret key rate. Then we show effects of excess noise on the secret key rate.

In what follows, we show the imperfectness of the high-frequency AM-embedded transmitter that has a negative effect on the practical security of the CVQKD system. Traditionally, we can derive the secret key rate with the given parameters [1], such as variance V, transmission efficiency T, reconciliation efficiency β, excess noise ε, detector efficiency η, detector noise v_{el}, and so on. Here, we take into account the reverse reconciliation for the practical security analysis because it usually offers an advantage in the performance analysis of the CVQKD system. According to the finite-size effect with respect to the traditional collective attacks [2], we obtain the secret key rate K, described as

$$K = \frac{n}{N}[\beta I_{AB} - S_{EB} - \Delta(n)], \tag{3}$$

where $n = N - m$ represents the number of the received quantum signals, S_{EB} denotes the maximum value of the Holevo information of an eavesdropper Eve and Bob, and I_{AB} represents the mutual information of Alice and Bob given by

$$I_{AB} = \frac{1}{2}\log_2 \frac{V + \chi_{tot} + 1}{\chi_{tot} + 1}, \tag{4}$$

where χ_{tot} denotes the total quantum channel noise. The parameter S_{EB}, which denotes the mutual information between Bob and Eve, can be derived from the covariance matrix Γ as follows:

$$\Gamma = \begin{bmatrix} aI_2 & c\sigma_Z \\ c\sigma_Z & bI_2 \end{bmatrix}, \tag{5}$$

where the parameters a, b, and c are described as $a = V + 1$, $b = T_{min}(V + \varepsilon_{max}) + 1$, and $c = \sqrt{T_{min}(V^2 + 2V)}$, respectively. The Pauli matrices I_2 and σ_Z are diagonal matrices defined by $diag\{1, 1\}$ and $diag\{1, -1\}$. The parameter T_{min} is the lower bound of transmission efficiency T, and the parameter ε_{max} denotes the upper bound of the excess noise ε.

When considering the simplified analysis, we let $m = N/2$. For the large value of m, the above two parameters T_{min} and ε_{max} can be derived as

$$T_{\min} = \frac{(t+\Delta t)^2}{\eta}, \epsilon_{\max} = \frac{\hat{\sigma}^2 + \Delta\sigma^2 - N_0(1+\nu_{el})}{N_0 t^2}, \tag{6}$$

where the parameters t, Δt, σ^2, and $\Delta\sigma^2$ are described as

$$t = \sqrt{\eta T}, \Delta t = \sqrt{\frac{\sigma^2}{mV}}, \sigma^2 = \eta T\xi + \nu_{el} + 1, \Delta\sigma^2 = \frac{\sigma^2\sqrt{2}}{\sqrt{m}}. \tag{7}$$

Consequently, the Holevo information S_{EB} can be calculated by

$$S_{EB} = \sum_{i=1}^{2} h\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} h\left(\frac{\lambda_i - 1}{2}\right), \tag{8}$$

where $h(x)$ can be defined by a function $h(x) = (x+1)\log_2(x+1) - x\log_2 x$. The parameters λ_i with $i \in \{1,2,3,4,5\}$ are the symplectic of Γ. In addition, the parameter $\Delta(n)$ is related to the security of privacy amplification given by

$$\Delta(n) = \sqrt{\frac{\log_2(1/\bar{\varepsilon})}{n} + \frac{2}{n}\log_2\frac{1}{\varepsilon_{PA}}}, \tag{9}$$

where $\bar{\varepsilon}$ denotes the smoothing parameter, and ε_{PA} represents the failure probability of privacy amplification for the distillation of the secret key.

3.2. Numerical Simulations

For the practical security analysis, the secret key rate of the CVQKD system with Gaussian modulation can be described as $K_G = K(V, T, \varepsilon, v_{el})$. Since the detection efficiency increases as the raised optical intensity of the AM-embedded transmitter, we obtain the transformed parameter $T' = gT$ caused by the imperfect transmitter. The additional noise decreases with the increase in optical intensity of the high-frequency transmitter, leading to $\varepsilon' = \varepsilon/g$ at the receiver.

Subsequently, there are two scenarios for consideration in the practical CVQKD system. According to the imperfections in the transmitter without being detected, Alice achieves the perfect variance V from the green pulse light, while Bob determines two resulting parameters T' and ε' from the measurement of the received imperfect signals. Then, we obtain the untrusted secret key rate $K_e = K(V, T', \varepsilon', v_{el})$. However, when the imperfection of the transmitter is detected, Alice obtains the imperfect variance V' combined with the green and red pulse lights, as shown in Figure 1. The numerical simulations show that the proposed scheme is sensitive to the AM-involved excess noise, and the transmission distance decreases as the the AM-involved excess noise increases. Consequently, we obtain the trusty secret key rate $K_p = K(V', T', \varepsilon', v_{el})$.

In numerical simulations, we make use of parameters, including attenuation coefficient 0.2 dB/km, detection efficiency 0.6, and so on, which can be usually used performance evaluation of the traditional quantum communication system. As shown in Figure 2, we have the relationship of the secret key rate and transmission distance when considering the leaked lights of the imperfect transmitter. In numerical simulations, the parameters are set as $V = 4$, $\eta = 0.5$, $v_{el} = 0.01$, $\beta = 95\%$, $\epsilon = 10^{-10}$, $N = 7 \times 10^9$, and $g = 1.44$, respectively. The yellow region is obtained from the difference described as $K_e - K_p$. The derived secret key rate falls within this region only when the leaked light cannot be undetected. This implies that the leaked light has resulted in a potential security loophole, which can be employed by Eve to steal the secret key while performing the intercept–resend attack strategy. As for the red region determined by K_e, the security of the derived secret key rate is not ensured, irrespective of the existence of the AM-involved light leakage.

Consequently, we find the limitations of the high-frequency AM embedded in the transmitter of the CVQKD system. In addition, the green region is achieved from the derived secret key rate K_p. When the secret key rate falls within this region, it is trustworthy, even in the presence of half the information leakage of the imperfect transmitter. As a result, the legal participants can trace back the information leakage that was produced by the imperfect transmitter at a high frequency from the above analysis, which can be used for defeating the leakage attack in the CVQKD system. In implementations, we have to trade off the practical security and the transmission efficiency while considering its deployment in a practical environment.

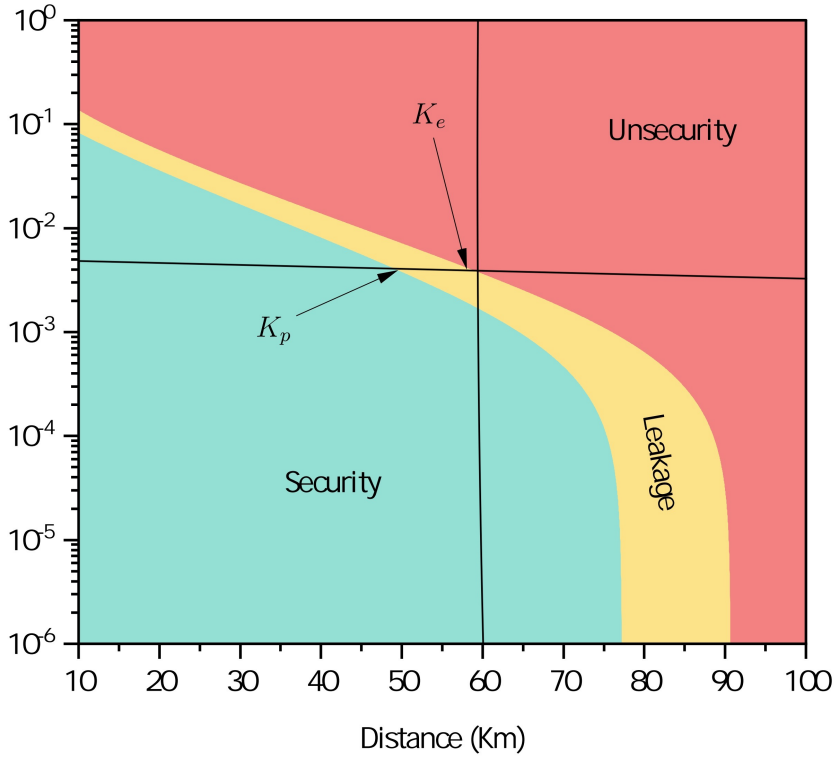

Figure 2. The secret key rate (bit/pulse) as a function of the transmission distance.

In the practical CVQKD system, Eve can perform the AM-involved attack strategies. According to the above analysis, we demonstrate the secret key rate of the practical CVQKD system when taking into account the information leakage attack. The evaluated secret key rate is overestimated in the absence of the protection of the high-frequency transmitter. Simulation results show that if the system has the ability to detect the AM-involved attacks, the practical secret key rate will be made smaller than that of the initial system. Therefore, the AM-involved attack will result in being untrustworthy of the estimated secret key rate.

In addition, we demonstrate the secret key rate of the the high-frequency AM embedded in the transmitter of the CVQKD system as a function of the transmission while illustrating the effect of the tunable parameter $g \in \{1.34, 1.44, 1.54\}$ on performance, as shown in Figure 3. We find that there is a decline in the secret key rate with the decreased parameter g. Moreover, the range of the difference region of K_p and K_e, which is called the leakage region, can be extended as the parameter g is enlarged. Namely, the larger parameter g results in the broader difference region for the light leakage. In addition, we find that the smaller parameter g means less information leakage, which leadss to a small security loophole from the high-frequency AM embedded in the transmitter.

According to the above analysis, we note that the aforementioned loophole can be solved by using the suitable frequencies of less than 500 MHz for the CVQKD system with high-frequency modulations, where the eavesdropper has no access to the unsolved loop-

hole. Given the lower sampling frequency of the transmitter, it is of practical significance to apply the frequency-tunable transmitter to a practical system.

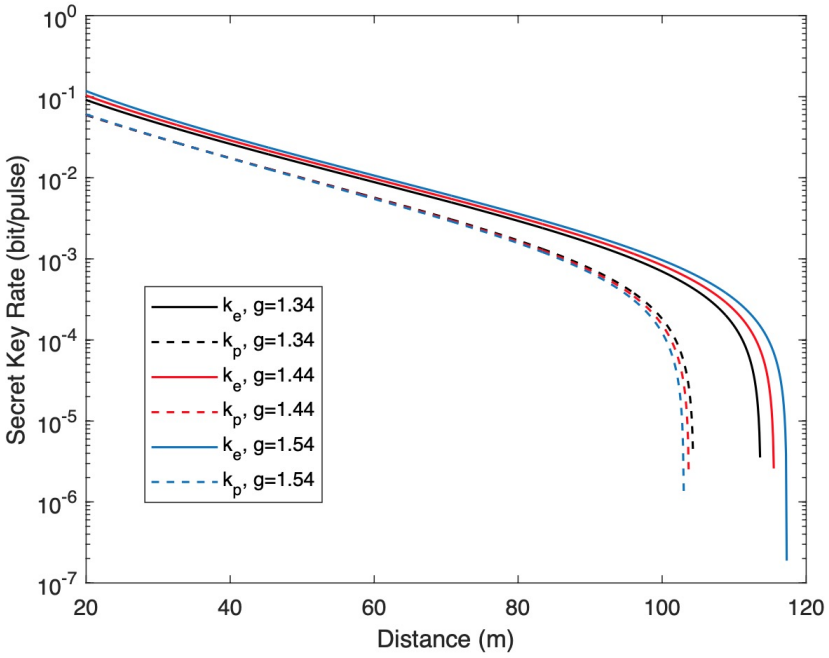

Figure 3. The secret key rate (bit/pulse) as a function of the transmission distance for the tunable parameter $g \in \{1.34, 1.44, 1.54\}$.

4. Conclusions and Discussion

We have demonstrated the feasibility of information leakage from a high-frequency AM-embedded transmitter in the practical CVQKD system. The light leakage from an imperfect transmitter results in deviations of the transmitted Gaussian-modulated coherent states, and thus, it makes us underestimate the channel excess noise when distilling the secret key at the receiver. This loophole causes an overestimation of the secret key rate, leading to a vulnerability of the practical security of the CVQKD system. The reason is that an eavesdropper may perform an intercept–resend attack strategy on the imperfect transmitter, from which the secret key can be potentially pilfered without being detected. We focus on revealing the forgotten imperfectness of the high-frequency AM, which contributes to the practical security of the CVQKD system. Assessment of the light leakage from the transmitter allows us to precisely evaluate the channel parameters, enabling the performance improvement of the practical CVQKD system. Meanwhile, there might exist other useful approaches to counteracting such a passive attack, such as the self-adapting detection of eavesdroppers with quantum artificial intelligence, which will be explored in future research.

We focus on revealing the imperfectness of a transmitter for high modulation frequencies at the transmitter, which compromise the practical security of the related system. Actually, an assessment of the AM-involved light leakage allows us to precisely evaluate the channel parameters, which have effects on the security of the practical CVQKD system. Moreover, several approaches have been suggested for counteracting these passive attack strategies. However, there are few works on high-frequency transmitters in the CVQKD system. As for the practical security when taking into account the high-frequency AM-embedded transmitter, we will think over its exact effects on the practical CVQKD system implemented in the future.

Author Contributions: Writing—original draft preparation, S.X.; writing—revising and editing, Z.Z.; supervisor, Y.G. All authors have read and agree to the published version of the manuscript.

Funding: This work was supported by the key research and development project in Hunan Province (Grant No. 2022GK2016), the Scientific Research Fund of Hunan Provincial Education Department (Grant No. 22C0446), Key project of Scientific Research of Hunan Provincial Education Department (Grant Nos. 21A0470, 22A0669), and the Natural Science Foundation of Hunan Province (Grant Nos. 2023JJ50268, 2023JJ50269).

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

Acknowledgments: We thanks Qingquan Peng for his constructive mention on the motivation of this paper.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **2013**, *7*, 378–381. [CrossRef]
2. 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]
3. Hu, L.; Al-Amri, M.; Liao, Z.; Zubairy, M.S. Continuous-variable quantum key distribution with non-Gaussian operations. *Phys. Rev. A* **2020**, *102*, 012608. [CrossRef]
4. 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. [CrossRef]
5. Qin, H.; Kumar, R.; Alléaume, R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Phys. Rev.* **2016**, *94*, 012325. [CrossRef]
6. Ferreyrol, F.; Blandino, R.; Barbieri, M.; Tualle-Brouri, R.; Grangier, P. Experimental realization of a nondeterministic optical noiseless amplifier. *Phys. Rev.* **2011**, *83*, 063801. [CrossRef]
7. Beveratos, A.; Brouri, R.; Gacoin, T.; Villing, A.; Poizat, J.-P.; Grangier, P. Single photon quantum cryptography. *Phys. Rev. Lett.* **2002**, *89*, 187901. [CrossRef] [PubMed]
8. Derkach, I.; Usenko, V.C.; Filip, R. Continuous-variable quantum key distribution with a leakage from state preparation. *Phys. Rev.* **2017**, *96*, 062309. [CrossRef]
9. Zheng, Y.; Huang, P.; Huang, A.; Peng, J.; Zeng, G. Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack. *Opt. Express* **2019**, *27*, 27369–27384. [CrossRef] [PubMed]
10. 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]
11. Li, H.-W.; Wang, S.; Huang, J.-Z.; Chen, W.; Yin, Z.-Q.; Li, F.-Y.; Zhou, Z.; Liu, D.; Zhang, Y.; Guo, G.-C.; et al. Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources. *Phys. Rev. A* **2011**, *84*, 062308. [CrossRef]
12. Tan, X.; Guo, Y.; Zhang, L.; Huang, J.; Shi, J.; Huang, D. Wavelength attack on atmospheric continuous-variable quantum key distribution. *Phys. Rev. A* **2021**, 103, 012417. [CrossRef]
13. Mao, Y.; Huang, W.; Zhong, H.; Wang, Y.; Qin, H.; Guo, Y.; Huang, D. Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New J. Phys.* **2020**, *22*, 083073. [CrossRef]