




Defending against a laser-seeding attack on continuous-variable quantum key distribution using an improved optical power limiter

Qingquan Peng ^{1,2}, Binwu Gao,² Dongyang Wang,² Qin Liao ^{3,*}, Zhiyue Zuo,¹ Hai Zhong,¹
Anqi Huang,^{2,†} and Ying Guo ^{1,4,‡}

¹*School of Automation, Central South University, Changsha 410083, China*

²*Institute for Quantum Information and State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, China*

³*College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*

⁴*School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China*



(Received 10 June 2023; accepted 8 November 2023; published 27 November 2023)

Laser-seeding attack enables an attacker to control the source output and eavesdrops on the key information, compromising the security of the continuous-variable (CV) quantum key distribution (QKD) system. In this paper, we suggest an improved optical power limiter (OPL) to defend against a laser-seeding attack on CV QKD systems. The proposed OPL utilizes a temperature monitor to detect Eve's attacks through temperature changes, providing an effective optical component for improving the security and reliability of the CV QKD system in practical environments, which is called an OPL-T scheme. In particular, we consider the security threats of a laser-seeding attack on two common CV QKD systems and prove their theoretical security degradation. Experiments are conducted to verify the effective OPL-T, and the results show that this defense scheme has an advantage in resisting the laser-seeding attack. Numerical simulations demonstrate the security analysis on CV QKD equipped with an OPL-T, which further confirms the effectiveness of our scheme. This work provides a practical solution for the security enhancements of continuous-variable quantum communication in practical applications.

DOI: [10.1103/PhysRevA.108.052616](https://doi.org/10.1103/PhysRevA.108.052616)

I. INTRODUCTION

Continuous-variable (CV) quantum key distribution (QKD) provides secure communications between two remote parties (Alice and Bob) by sharing a string of secret keys [1–4], whose theoretical security is guaranteed by the principle of quantum physics [5–7]. In particular, Gaussian-modulated coherent state (GMCS) CV QKD has been proven to be secure against both collective and coherent attacks [7–9] and it can be implemented with existing coherent optical communication technologies and devices, rendering CV QKD a cost-effective solution for short-distance secure communication [10].

One of the fundamental prerequisites for achieving theoretical unconditional security in original CV QKD protocols is the assurance that both the sender and receiver nodes are physically and technologically isolated from potential eavesdroppers [11,12]. However, the practical security still could be compromised by Eve due to the imperfect devices in implementations of the QKD system [13–15]. In fact, attackers have devised several methods to exploit the imperfection of a system's detection side and then eavesdrop on security keys, for instance, a detector efficiency mismatch attack [16–21],

a time-shift attack [22,23], and a wavelength attack [24,25]. In addition, a local oscillator (LO) calibration attack [26] exploits calibration errors in the LO phase that generate a stable interference signal, allowing the attacker to gather critical information about quantum signals. A homodyne-detector-blinding attack [27] aims to saturate the detector's electronics by shining a bright light, rendering it temporarily inoperative. On the other hand, a polarization attack [28] exploits the polarization dependence of the detectors and other components to intercept the quantum signal. To mitigate the risk of these CV QKD systems' detection-side attacks, researchers have proposed various countermeasures, including wavelength filters [29], proper monitors [30], passive CV QKD [31], measurement-device-independent (MDI) CV QKD systems [32,33], and preventive measures for intelligent feature extraction [34,35].

However, despite the significant progress made in defending against detection-side attacks, attackers have also found ways to exploit vulnerabilities on the source side of QKD systems such as a phase-remapping attack [36,37], a bright illumination attack [38–40], a laser damage attack [41–43], a Trojan-horse attack [44,45], and a laser-seeding attack [46,47]. The Trojan-horse and laser-seeding attacks are particularly insidious as they are difficult to detect. An attacker can use a Trojan-horse light to send a probe signal into Alice's or Bob's apparatus and analyze the backscattered signal to infer their modulation or measurement settings [48,49]. The laser-seeding attack is another

*llqqlq@hnu.edu.cn

†angelhuang.hn@gmail.com

‡guoying@bupt.edu.cn

source-side attack that compromises the security of discrete-variable (DV) quantum key distribution and CV QKD, including chip-based implementation. Eve injects photons into the source of Alice’s laser, which can increase the optical intensity of the laser’s emitted pulses. This means that Eve’s laser-seeding attack broke the basic assumption that the QKD system’s light intensity must be maintained at a certain value. It should be noted that if she wants to eavesdrop on security keys, then she must combine the laser-seeding attack with others, such as intercept-resend [50] and photon-number-splitting attacks [51,52]. Fortunately, an optical power limiter (OPL) has been suggested to successfully limit the injected light from Eve [53,54].

Inspired by countermeasures to defend against such attacks in DV QKD, this paper proposes an improved OPL scheme to defend against a laser-seeding attack in the CV QKD system. The proposed OPL-T scheme utilizes the thermal defocusing effect of acrylic prisms to scatter the seeding light from the attacker and detects the attack by monitoring the temperature. The experimental results show that the proposed OPL-T scheme can limit the injected seeding light to the microwatt level, coordinating the temperature monitor in the scheme to defend against the laser-seeding attack in both GMCS CV QKD and MDI CV QKD systems. Moreover, the OPL-T can be easily integrated into the existing CV QKD systems, enhancing the security of quantum communication in practical applications.

This paper is organized as follows. In Sec. II we briefly recap the laser-seeding attack in a CV QKD system, followed by proposals of equipping an OPL-T in CV QKD implementations. We demonstrate the performance of the OPL-T in Sec. III and analyze the security of the proposed scheme in Sec. IV. We conclude in Sec. V with a summary of our study and suggestions for future work.

II. DEFENDING AGAINST A LASER-SEEDING ATTACK USING AN OPL-T

In this section, we briefly recap the principle of laser-seeding attack in the CV QKD system [46] and then suggest the OPL-T scheme for the application scenarios in CV QKD systems.

A. Laser-seeding attack in CV QKD

As shown in Fig. 1, Eve injects light into the laser diode of the CV QKD system through the quantum channel, resulting in more photons generated by the laser diode. These extra photons are also modulated and sent to Bob. Unfortunately, Eve can intercept and detect some photons here to obtain Alice’s encoded information. It is worth noting that Eve can maximize injection efficiency by adjusting the polarization of the injected optical signal using a polarization controller.

To figure out how the laser-seeding attack works in the CV QKD system, it is necessary to review the coherent state preparation process. Alice modulates the random key information to the pulse signal A_0 and generates a GMCS. After optical attenuation, transmitted coherent states are expressed in phase space as

$$|\alpha_{A_0}\rangle = x_{A_0} + ip_{A_0}, \quad (1)$$

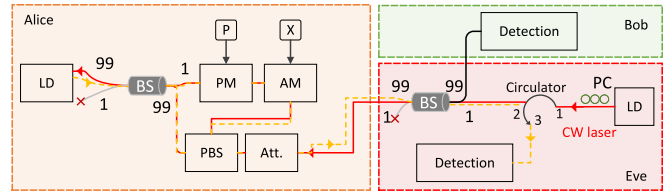


FIG. 1. Diagram illustrating the laser-seeding attack on the CV QKD system. The red solid line represents the propagation path of the laser-seeded light attack, while the yellow dashed line illustrates the path of photons with increased laser gain following a successful attack. Alice’s quantum signal is split into two by Eve’s optical beam splitter (BS): One is intercepted and the other is transmitted to Bob, as depicted by the black solid line. The following denotations are used: LD, laser diode; cw laser, continuous-wave laser; PC, polarization controller; PM, phase modulator; AM, amplitude modulator; PBS, polarization beam splitter; and Att., adjustable attenuator.

where $x_{A_0} = |\alpha_{A_0}| \cos \theta$ and $p_{A_0} = |\alpha_{A_0}| \sin \theta$. The amplitude and phase of the Gaussian modulated optical signal A_0 are denoted by $|\alpha_{A_0}|$ and θ , respectively. Here x_{A_0} and p_{A_0} are two independent quadratures variables with the same variance V_{A_0} and zero mean [4]. A laser-seeding attack affects the optical signal’s amplitude and phase modulation A_0 . As shown in Fig. 2, the optical signal generated by a semiconductor laser after being attacked undergoes significant changes. The blue solid line represents the ideal optical signal generated by a semiconductor laser. In contrast, the orange dashed line represents the optical signal generated after the laser-seeding attack of the semiconductor laser. It can be seen from the graph that the peak value of the orange dashed line appears earlier than the blue solid line and the average optical power becomes higher. This indicates that the injected light triggers stimulated emission, which is faster than the spontaneous emission in Alice’s laser diode. Consequently, Alice’s pulse reaches its peak earlier in time. At the same time, we should also take note of the prolonged emission time of Alice’s laser, resulting in an ultimate increase in the overall light intensity [47]. The orange open marker (A'_0) and the blue open marker (A_0) on the right-hand side of Fig. 2 represent the optical signals received by Bob with and without an attack, respectively. A comparison reveals that the deviation occurring during an attack is more noticeable. Therefore, the values of x_{A_0} , p_{A_0} , and V_{A_0} experience deviations due to the effects of the attack.

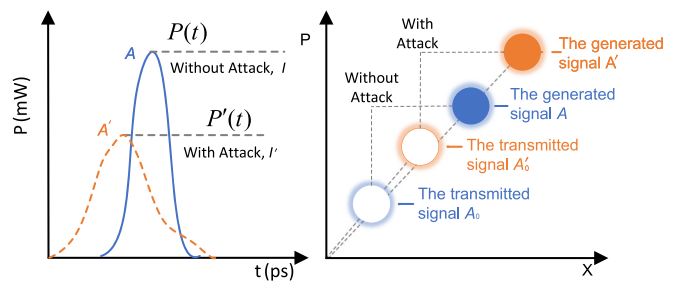


FIG. 2. Shift of the GMCS in phase space under laser-seeding attack. Here $P(t)$ and $P'(t)$ are the powers of the optical signal emitted by a LD without attack and with attack, respectively, and A and A' are the generated signals without attack and with attack, respectively.

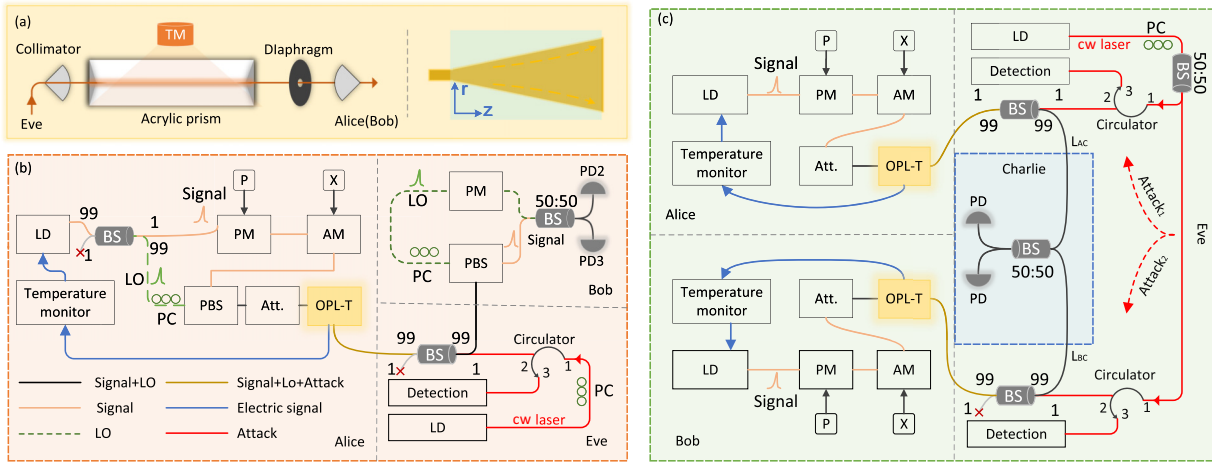


FIG. 3. Schematic of the OPL-T and diagram of its use in the CV QKD system. (a) Schematic of the OPL-T. Eve's laser enters from the left, is emitted by a collimator, irradiates the left section of an acrylic prism, and then exits from the right section. Finally, the collimator collects the laser light after passing through the aperture of a diaphragm. The transmission paths of Alice's and Bob's optical signals are exactly the opposite. (b) Design of the GMCS CV QKD system using the OPL-T to defend against a laser-seeding attack. (c) Design of the MDI CV QKD system using the OPL-T to defend against the laser-seeding attack. The following denotations are used: TM, temperature monitor; LO, local oscillator; BS, beam splitter; PD, pin photodiode; PM, phase modulator; AM, amplitude modulator; PC, polarization controller; PBS, polarization beam splitter; and Att., adjustable attenuator.

This phenomenon becomes evident through the phase-space depiction shown in Fig. 2. In the context of variable $I \propto |\alpha_{A_0}|$, the modifications in variables x'_{A_0} , p'_{A_0} , and V'_{A_0} unfold as

$$x'_{A_0} = \sqrt{g}x_{A_0}, \quad p'_{A_0} = \sqrt{g}p_{A_0}, \quad V'_{A_0} = gV_{A_0}, \quad (2)$$

where g is the light magnification after a laser-seeding attack and x'_{A_0} and p'_{A_0} are two independent quadrature variables of the transmitted quantum signal A'_0 with the attack involving the variance V'_{A_0} .

Eve can manipulate the CV QKD system by injecting approximately 100-nW seed light into Alice's laser [55], increasing the transmitted GMCS's intensity. This attack has the effect of causing the system to underestimate the excess noise present in the quantum channel. Consequently, an inadvertent overestimation of the secure key rate creates a vulnerability. This vulnerability allows Eve to potentially conduct interception-resend attacks on the CV QKD system without being detected. Furthermore, in a laser-seeding attack, the wavelength of Eve's light must align with the output wavelength of the QKD system's laser to effectively stimulate the laser's emission of additional photons. It should be noted that the laser-seeding attacks can affect both the optical power and phase of Alice's light. However, the phase variations of Alice's light do not affect the security of the CV QKD system. This is because Alice splits the laser's light into signal and LO parts, as shown in Fig. 4(b). The phase of the signal light will be modulated by Alice and that of the LO light will not be. After Bob receives the signal and LO lights, he measures the phase difference between them to extract the information of Alice's modulation.

B. CV QKD embedded with an OPL-T

The OPL-T consists of passive and active components. The component responsible for constraining Eve's optical emissions operates passively. While the temperature monitor

qualifies as an active device, it is a noncontact approach to monitor temperature changes in the acrylic prisms. This insulation structure protects the temperature monitor for Eve's attack.

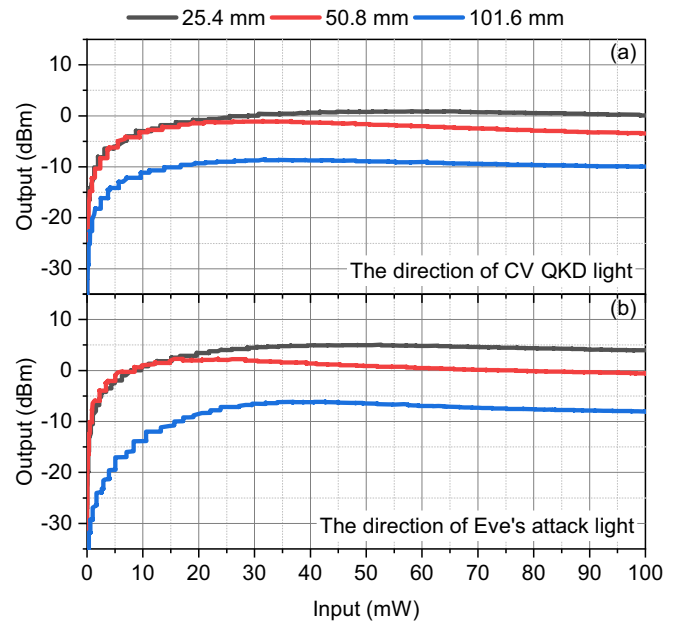


FIG. 4. (a) Insertion loss calibration of the OPL-T. The direction of light is opposite that in Fig. 3(a). The light is coming in from the right-hand side and going out on the left-hand side. The input represents the laser power sent into the OPL-T by the CV QKD source. (b) Power limit calibration of the OPL-T. The light's transmitted direction is shown in Fig. 3(a). The light is coming in from the left-hand side and going out on the right-hand side. The input represents the laser power sent into the OPL-T by the Eve source. The black, red, and blue solid lines represent 25.4-, 50.8-, and 101.6-mm acrylic prisms, respectively.

The overall configuration is depicted in Fig. 3(a). It comprises two collimators, a temperature monitoring module, and an acrylic prism, involving a small diaphragm hole. Eve's attack light enters the acrylic prism through the left collimator. Light diffuses and propagates through an acrylic prism, as shown in the green area on the right-hand side in Fig. 3(a). A small diaphragm hole is placed to the right of the acrylic prism to ensure that only a small portion of light can pass through and eventually be collected by the right collimator. An acrylic prism is used as the active medium and plays an important role in the power-limiting process. When an acrylic prism absorbs energy and produces an internal temperature gradient, the incident light beam will diverge due to the thermal defocusing effect. Therefore, the temperature of the acrylic prism will rise sharply if Eve launches a laser-seeding attack with a high-power laser. To detect this attack, we place a temperature monitor around the acrylic prism to record real-time temperature changes. Once the temperature exceeds room temperature, a signal is triggered to stop the CV QKD's laser to prevent information leakage. Moreover, when the injected light exceeds 4 W, the acrylic prism undergoes dissolution, at a maximum temperature of about 50 °C [54]. Following dissolution, the acrylic prism blocks the transmission of light. Therefore, other devices of the CV QKD system can be protected at the expense of an acrylic prism.

We note that the proposed OPL-T can be applied to both GMCS CV QKD and MDI CV QKD systems. Figure 3(b) shows the GMCS CV QKD system embedded with the OPL-T. The CV QKD system uses a 1:99 beam splitter to split the coherent state pulsed light into a weak signal and a strong local oscillator. The signal is randomly modulated according to a Gaussian distribution with variance V_{A_0} and zero mean in both quadratures and then sent to Bob after passing through a polarization beam splitter, an adjustable attenuator, and an OPL-T. Eve can intercept some information from the public quantum channel to reconstruct the secure key shared between Alice and Bob. The more information Eve intercepts, the easier it is for her to recover the key. However, this will draw the attention of Alice and Bob since Bob's information will decrease. Therefore, the best strategy for Eve is to intercept more information without significantly affecting Bob's information. Eve can use a laser-seeding attack to inject a laser into Alice's system, which increases the amount of information Alice sends. Alice must use the OPL-T to limit the attacker's injected light. However, using the OPL-T also limits Alice's output light, so adjusting the variable attenuator appropriately ensures that the number of photons output from the OPL-T satisfies the modulation variance. Additionally, if the temperature of the OPL-T exceeds room temperature, it will send feedback signals to turn off the laser, ensuring the safety of the equipment.

In MDI CV QKD, the transmitted state is not measured by Bob. Instead, he and Alice send their own states to an untrusted relay, which performs the measurement. The relay then announces the measurement results to Alice and Bob, who use them to generate a secret key. In a way, MDI CV QKD is more secure than GMCS CV QKD because it does not require a trusted detection end. However, from another perspective, the separate laser sources of Alice and Bob may provide Eve with more opportunities for attack. For example, Eve can

use a laser-seeding attack to hack Alice or Bob individually or launch such an attack on both Alice and Bob simultaneously. Figure 3(c) shows a schematic diagram of Eve launching laser-seeding attacks on Alice and Bob simultaneously, with Attack_1 and Attack_2 representing the attacks on Alice and Bob, respectively. To defend against this attack, we deploy an OPL-T for Alice and Bob to limit Eve's laser power, as highlighted in yellow in Fig. 3(c). To be clear, the OPL-T will monitor its own real-time temperature change to sense Eve's presence, whether it is in GMCS CV QKD or MDI CV QKD. Also, when faced with a strong light attack, the OPL-T will sacrifice itself to protect Alice's and Bob's components [54].

III. EFFECTS OF AN OPL-T ON PRACTICAL SECURITY

The insertion loss of the OPL-T is the lost optical power caused by inserting the OPL-T into the CV QKD system. A high insertion loss reduces the system's performance by reducing the optical power available for Bob to detect. The power-limiting performance of the OPL-T shows the ability to reduce the amount of optical power that is received by Eve. A weak power-limiting performance cannot effectively defend against the laser-seeding attack. Eve can inject a great deal of optical power into the system and obtain the secret key.

A. Calibration

Calibration of the OPL-T is essential to ensure its stable operation in a CV QKD system. The first step is calibrating the light source direction, the opposite direction in Fig. 3(a). The next step is to calibrate the Eve attack light direction, which is the same as that in Fig. 3(a). During the calibration process, the length of the acrylic prisms affects the power-limiting performance of the OPL-T. For this reason, we show calibration data for three different lengths of acrylic prisms. From Fig. 4 we can easily find that the output power of the OPL-T is increased as a function of increasing injected optical power when injecting cw light between 0 and 20 mW. This phenomenon can be called the power pass unconstrained effect, occurring in both directions. It is essential to mention that through our experimental investigations, we have uncovered that the transmission performance of the OPL-T is not entirely uniform in both directions. In principle, one would anticipate that, due to the presence of the diaphragm, injecting light from the left-hand side in Fig. 3(a) would encounter more difficulty passing the OPL-T than injecting from the right-hand side. However, our experimental result shown in Fig. 4 deviated from the anticipated theoretical outcomes because the acrylic prism surface is nonideal. To accurately depict the OPL-T's capabilities, we conducted subsequent experiments on the OPL-T under the condition that transmission loss is minimized for Eve by adjusting component coupling, allowing maximal injecting light.

In CV QKD, the average number of pulse photons varies from a few to tens depending on the modulation variance, which means that the OPL-T does not limit the output light. When the laser injected into the OPL-T is 20–100 mW, the output power begins to stabilize within a range and no longer increases with the increase of the injected power. This shows that the OPL-T can effectively limit the laser power injected

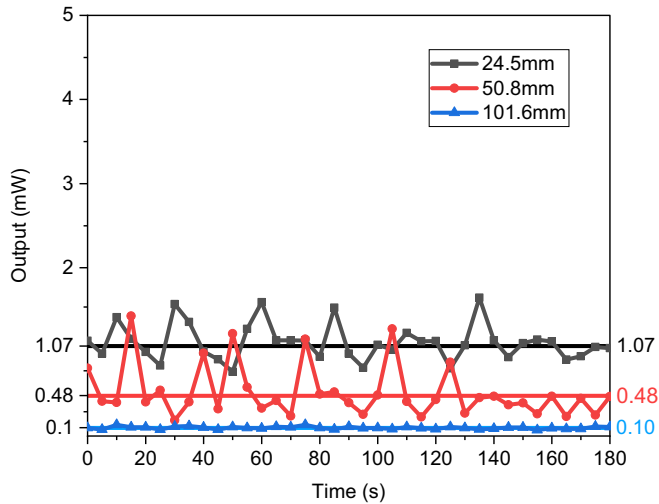


FIG. 5. Variation of output power during the OPL-T operation in 20 min. The laser power injected into the OPL-T by Eve is 217 mW. The light direction is shown in Fig. 3(a), coming in from the left-hand side and going out on the right-hand side.

into the CV QKD system if the laser power adopted by Eve is in the range of 0–100 mW. In addition, the longer the acrylic prism is, the lower its output power is, which makes it more difficult for Eve to attack successfully.

B. Stability

The long-term stability of the OPL-T is also an important factor to consider when evaluating its ability to resist a laser-seeding attack. A continuous laser-seeding attack is simulated to the OPL-T for up to 20 min to assess its performance. The output power is monitored at 5-s intervals. The cw laser power injected into the OPL-T is 217 mW. As shown in Fig. 5, black, red, and blue solid lines represent the output power of OPL-Ts with acrylic prism lengths of 25.4, 50.8, and 101.6 mm, respectively. Solid lines with markers represent experimental records, while horizontal lines with the same color represent the average output power. It can be found that the fluctuation of the output power of the OPL-T with an acrylic prism length of 101.6 mm is minimal, while the fluctuation of the output power of the other two OPL-Ts is significant. The experimental results also show that the 101.6-mm acrylic prism offers even better stability, power-limiting capabilities, and higher minimum insertion loss than the 25.4-mm acrylic prism. At the same time, we should also be aware that the higher insertion loss can reduce the transmission performance of CV QKD. To resolve this issue, Alice can adjust the variable attenuators to compensate for reducing the impact of increased insertion loss caused by the OPL-T on the CV QKD system. It should be noted that Alice can only compensate for the minimum insertion loss by calibrating the OPL-T. If the insertion loss increases by Eve's attack, then it cannot be offset. Therefore, balancing protection and limitation capacity is paramount when considering the length of the acrylic prism for OPL-T integration. Furthermore, the prerequisite for adjusting the attenuator to compensate for insertion loss is that the OPL-T is regarded as a trusted component of Alice or

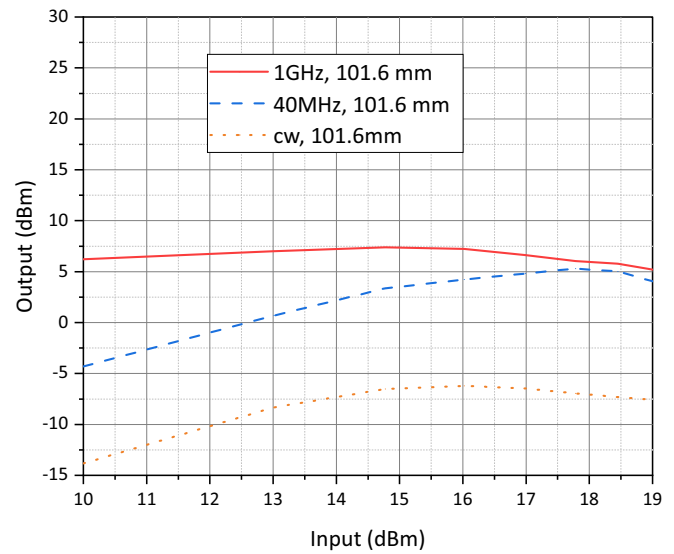


FIG. 6. Experimental diagram of the input power and output power of the OPL-T under cw light and pulsed light. The length of the acrylic prism assembled by the OPL-T is 101.6 mm. The duty cycle of the pulsed light is 24%. In the pulsed-light experiment, the output power is the peak power collected by an oscilloscope, while the input power is the average optical power.

Bob. If the OPL-T is untrusted, we cannot arbitrarily adjust the attenuator.

In summary, when utilizing the OPL-T in a CV QKD system, Alice needs to consider factors such as the trustworthiness of the OPL-T and usage environment. This paper cannot estimate which length is optimal before understanding the actual environment. However, once the CV QKD system has ensured the OPL-T is a trusted component, Alice can only compensate for the minimum insertion loss by calibrating the OPL-T. Otherwise, excessive compensation will compromise the security of CV QKD.

C. Optical power limitation

Pulsed-light attacks are typically characterized by high instantaneous power and short duration, making it difficult for CV QKD systems to detect them. Therefore, it is necessary to conduct pulsed-light experiments on the OPL-T to evaluate its ability to defend against these attacks. Figure 6 shows the relationship between the input and output power of the OPL-T with an acrylic prism length of 101.6 mm under pulsed light and cw light. The red solid and blue dashed lines show pulsed-light results with repetition frequencies of 1 GHz and 40 MHz, respectively. The yellow dotted line represents the results of cw light. The results show that the output optical power initially increases with the rise in input power and eventually stabilizes. This means that the OPL-T can limit the seed light. On the other hand, the experimental results also demonstrate that the output power at a pulse frequency of 1 GHz is higher than that at 40 MHz for the same input power. In addition, when the OPL-T is attacked by a laser with an optical power of 10 dBm, the output power of pulsed light is greater than that of cw light and increases with the repetition frequency of the pulsed light. This means it is easier to use

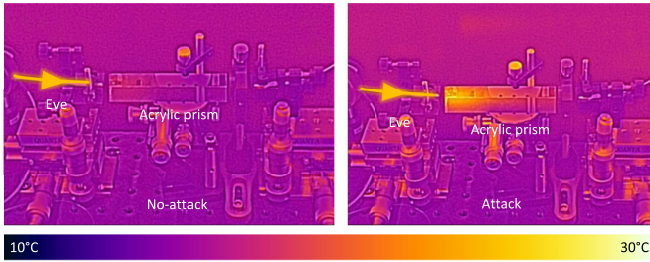


FIG. 7. Using thermal imaging to observe the temperature changes of the OPL-T under attack and no-attack conditions. The acrylic prism length is 101.6 mm. The optical power of the attack light is 217 mW.

pulsed light than cw light to eavesdrop on the information. A maximum output of only 7.3 dBm for the OPL-T when Eve uses pulsed light at 1 GHz indicates that an OPL-T with an acrylic prism length of 101.6 mm is sufficient to resist Eve's laser-seeding attack.

Reference [54] presents an experiment about the OPL-T's passive component at a lower pulse frequency, precisely, a 0.5-Hz experiment. By contrasting the experiments involving cw and 0.5-Hz lights, we obtain that, after passing the OPL-T, the output power of the pulsed light is higher than that of the cw light. Also, compared to the 40-MHz and 1-GHz light experiments, we verified that the limiting performance of the OPL-T passive component reduces with increasing pulse frequency. To address the issue of limiting performance degradation in pulsed light, the OPL-T identifies Eve's attack through a dual component to improve the security of the CV QKD system. In scenarios where Eve employs the weak power of pulsed light for an attack, even if temperature variation is undetected, the OPL-T's passive component constrains her attack light. If Eve employs the more substantial power of pulsed light for an attack, the OPL-T's passive component will limit her light intensity and the temperature monitor will discover the thermal effects of the OPL-T by sending a warning to the CV QKD system.

D. Attack identification by temperature

The low optical power levels used in CV QKD make it challenging to induce significant thermal effects within the OPL-T. The thermal imaging on the left-hand side of Fig. 7 illustrates this phenomenon. In a laser-seeding attack, Eve cannot successfully attack if she uses seeding light at the same level because introducing such seeding light makes it difficult to overcome the attenuation of various components within the CV QKD system to reach the source laser. Therefore, Eve needs to increase her optical energy. Once Eve's laser power increases, a hot spot is generated inside the OPL-T. This hot spot is located towards the rear of the acrylic prism injection side, as shown on the right-hand side of Fig. 7. At this point, the OPL-T detects an abnormal temperature and issues a warning to the CV QKD system, making it difficult for Eve to perform a laser-seeding attack on a CV QKD system equipped with an OPL-T without being detected.

The above-mentioned experiment indicates that the OPL-T performs best at power limiting when assembled with a

101.6-mm acrylic prism. However, it still needs to be verified whether using the OPL-T in the CV QKD system can effectively resist a laser-seeding attack. Therefore, based on existing experimental results, we perform a security analysis of the CV QKD system embedded with the OPL-T in what follows.

IV. SECURITY ANALYSIS AND DISCUSSION

In this section, we detail the security analysis of the OPL-embedded CV QKD system in both GMCS and MDI constructions.

A. GMCS CV QKD embedded with an OPL-T

In a GMCS CV QKD system, Alice's laser is the only place where Eve can perform a laser-seeding attack. Therefore, an effective way to defend against Eve's attack is to prevent it from entering Alice's laser cavity as much as possible. In the designed GMCS CV QKD system that can counteract a laser-seeding attack, as shown in Fig. 3(b), the OPL-T is used to limit the amount of optical power that is available for Eve to attack. The analysis of the secret key rate is usually used to verify the feasibility of GMCS CV QKD (Appendix A).

Assuming the cumulative attenuation of various components within Alice's setup is 70 dB and Eve uses a 200-mW cw laser to launch an attack, the attack light power reaching Alice's laser is about 20 nW, which will result in Alice's output light increasing by about two times ($g = 2$) [55]. However, if an OPL-T is used to protect the GMCS CV QKD system, only about 0.01 nW of the attack light can be injected into Alice's laser under the same conditions. Additionally, based on the experimental results shown in Fig. 6, pulses with higher repetition frequency are less constrained by the OPL-T when using the same duty cycle. This is because the pulse with a higher repetition rate results in a shorter pulse width in each cycle, thus reducing the thermal defocusing effect of the OPL-T. According to the thermal defocusing effect of the acrylic prism within the OPL-T, there is a positive correlation between internal heat accumulation and the power limitation capability of the OPL-T. Therefore, Eve's optimal attack strategy is to use the high-repetition-frequency pulse width to allow more seed light to pass through the OPL-T and induce stronger light pulses from the CV QKD system's laser. For example, if Eve employs a pulsed-light source with a power of 31.62 mW and a frequency of 1 GHz to inject into the OPL-T, she obtains a maximum output optical power of 5.73 mW, as shown in Fig. 6. Based on this observation, we assume Eve employs the above attacking method, and all other parameters remain unchanged. The seeding light with an approximate power of 0.57 nW is injected into Alice's laser diode, whose output power is increased to 1.01 times ($g = 1.01$) [55].

Figure 8 depicts the relationship between secret key rate and transmission distance for a practical GMCS CV QKD system with or without the protection of the OPL-T. The given parameters for the simulation are set to $V_{A_0} = 4$, $g = 1.01$ or 2.0, $\eta = 0.5$, $\epsilon = 0.01$, $\bar{\epsilon} = 10^{-10}$, $Z_{\epsilon_{PE}/2} = 6.5$, $\nu_{el} = 0.01$, $m = 0.5N$, $N = 10^{10}$, and $\beta = 0.95$. When Alice and Bob discover that the CV QKD system was attacked by laser

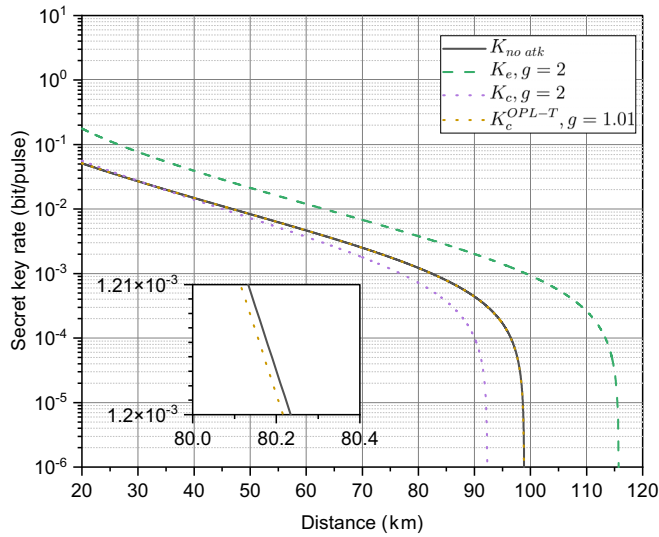


FIG. 8. Secret key rate as a function of the transmission distance from Alice to Bob. The solid line represents the secret key rate without attack $K_{no\ atk}$. The dashed line represents the estimated secret key rate K_e . The dotted lines K_c and K_c^{OPL-T} represent the correct key rates with and without the OPL-T in the CV QKD system, respectively.

seeding they will use the actual light intensity values to calculate the variance value V_{A_0} and estimate the security key rate. This means that the V_{A_0} employed for the secure key rate calculation is not optimized, leading to performance degradation in the secure key rate. From Fig. 8 it can be seen that Alice and Bob's estimated secret key rate K_e is overestimated compared to $K_{no\ atk}$, which is without attack. More precisely, the security proof in Refs. [7,8] cannot guarantee the security of the secret key obtained by Alice and Bob. If the GMCS CV QKD system can detect the laser-seeding attack, the correct value of K_c will be less than that of $K_{no\ atk}$. This shows that the laser-seeding attack on the GMCS CV QKD system will make the estimated secret key rate untrustworthy. In other words, the estimated key rate under a laser-seeding attack either does not guarantee communication security or leads to the reduction of the transmission distance.

Fortunately, when Eve launches an optimal attack on the GMCS CV QKD system with OPL-T protection, it only results in an increase in Alice's laser intensity by 1.01 times. This is a very small increase and has a negligible impact on the secret key K_{OPL-T} , as shown in Fig. 8. Therefore, in practical applications, the OPL-T should be used to enhance the security of CV QKD by limiting the amount of information Eve can eavesdrop on.

B. MDI CV QKD embedded with an OPL-T

The MDI CV QKD system is a type of QKD system immune to attacks on measurement devices. The reason is that the quantum signal is measured by an untrusted third party, Charlie. However, this system might be more sensitive to the laser-seeding attack. This is because Alice and Bob possess laser diodes in the MDI CV QKD system, enabling Eve to target both of them with laser-seeding attacks, whereas Eve can only perform a laser-seeding attack on Alice in a prepare-and-measure CV QKD system. To resist a laser-seeding attack, we

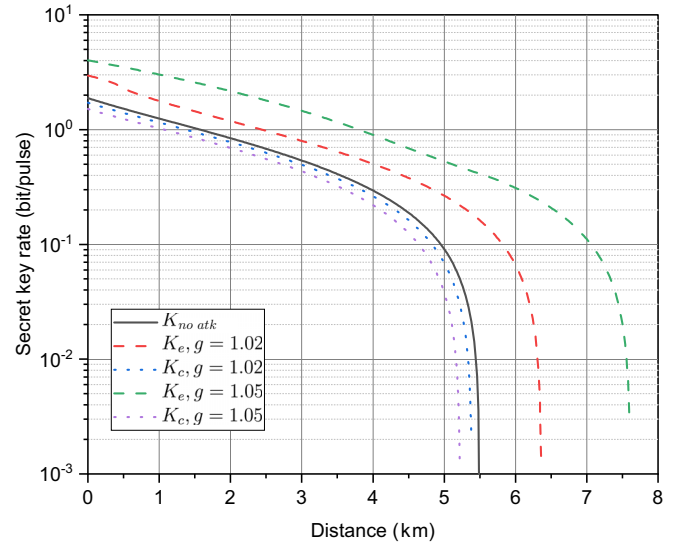


FIG. 9. Secret key rate as a function of the transmission distance from Alice to Bob in the symmetric case. The solid line represents the secret key rate without attack $K_{no\ atk}$. The dashed line represents the estimated secret key rate K_e . The dotted line represents the correct secret key rate K_c . Here g is the light magnification after the laser-seeding attack. The experimental parameters are $L_{AC} = L_{BC}$, $V_{A_0} = V_B = 40$, $g = 1.02$ or 1.05 , $\eta = 0.5$, $\epsilon_{AC} = \epsilon_{BC} = 0.01$, $g_A = g_B = g$, and $\beta = 0.95$.

can add an OPL-T device at the exit of each laser source, as shown in Fig. 3(c). An OPL-T device limits the power of the laser signal, making it more difficult for Eve to inject her laser signal. The following analysis assumes Eve simultaneously attacks Alice's and Bob's laser sources.

Figures 9 and 10 show the relationship between key rate and transmission distance under symmetric and asymmetric conditions, respectively. Eve uses a laser-seeding attack on Alice and Bob to obtain gains of g_A and g_B , respectively. Assuming that $g_A = g_B = g$, the numerical simulation shows a gap between the secret key rate estimated by Alice and Bob and the correct secret key rate, even with small gain values g . This means Eve can perform an intercept-resend attack in MDI CV QKD to eavesdrop on the secret key. Importantly, the difference of the estimated secret key rate and the correct secret key rate means that the shared information between Alice and Bob is not secure. In addition, the MDI CV QKD system is more sensitive to multiple photons than the GMCS CV QKD system. The slightly increased light intensity of Eve in the communication may result in a major impact on the evaluative value of the secret key rate of the MDI CV QKD systems, especially in the extreme asymmetric case. Therefore, in MDI CV QKD, it becomes essential to minimize the likelihood of laser-seeding light entering the laser diode, in order to counteract this form of attack. To take a countermeasure regarding this attack, we assume that the attack light power reaching Alice's (Bob's) laser will be about 0.01 nW [55]. Based on this, we have provided a set of values that can be used for the internal attenuation values of MDI CV QKD with the OPL-T, as shown in Table I.

This paper has derived the following conclusions through an analysis of simulations of GMCS CV QKD and MDI CV

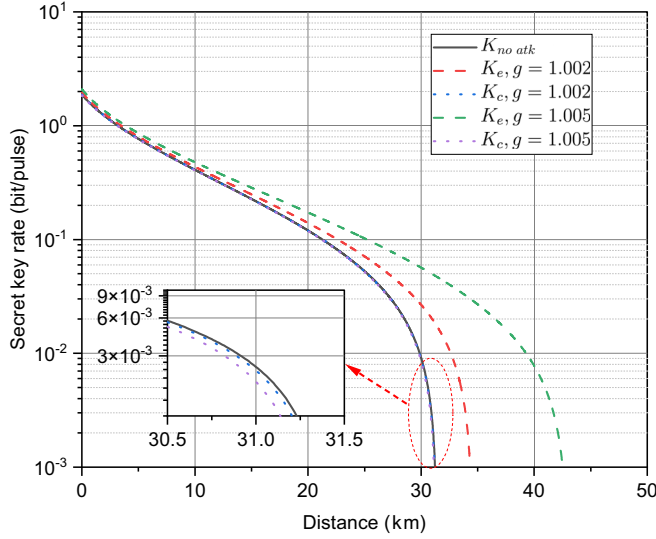


FIG. 10. Secret key rate as a function of the transmission distance from Alice to Bob in the asymmetric case. The solid line represents secret key rate without attack $K_{\text{no atk}}$. The dashed line represents the estimated secret key rate K_e . The dotted line represents the correct secret key rate K_c . Here g is the light magnification after the laser-seeding attack. The experimental parameters are $L_{AC} = 0.001$, $V_{A_0} = V_B = 40$, $g = 1.002$ or 1.005 , $\eta = 0.5$, $\epsilon_{AC} = \epsilon_{BC} = 0.01$, $g_A = g_B = g$, and $\beta = 0.95$.

QKD systems. First, the simulation results replicate the adverse effects of laser-seeding attacks on CV QKD, specifically manifesting as overestimating secret key rates or reducing transmission performance. Second, the simulation results also show that with the assistance of the OPL-T, the performance of the CV QKD system, while not entirely eliminating the harm caused by laser-seeding attack, approaches the optimal performance achievable without an attack. Therefore, defending against the laser-seeding attack in the MDI CV QKD system requires the selection of an appropriate OPL-T and the coordination of other components, such as variable attenuators.

V. CONCLUSION

Focusing on the security of the CV QKD system, this paper proposed a countermeasure against the laser-seeding attack. Specifically, we improved an optical power limiter and named

TABLE I. Recommended configuration choices for Alice's setup for a MDI CV QKD system equipped with an OPL-T to provide a comprehensive defense against laser-seeding attacks, for three typical attack strategies.

Type ^a	Power ^b (mW)	Length ^c (mm)	Attenuation ^d (dB)
cw	217	101.6	>70
40 MHz	31.6	101.6	>87
1 GHz	63	101.6	>85

^aThe frequency at which Eve attacks the light.

^bEve's average optical power for a laser-seeding attack.

^cThe length of the acrylic prism.

^dAttenuation within Alice or Bob of the MDI CV QKD system.

it the OPL-T to limit the seed light reaching Alice's laser diode and detect Eve's attack by using a temperature monitor. In the experimental demonstration, we validated the OPL-T limitation performance effect and were able to detect its high-power attack capability. Furthermore, we analyzed the feasibility of the OPL-T countermeasure scheme in applying GMCS CV QKD and MDI CV QKD systems by stimulating the security key rate. This study provides an approach to enhance the security and reliability of the CV QKD systems. We hope our work will provide support and reference to build robust and practically secure quantum communication systems.

ACKNOWLEDGMENTS

This work was funded by the National Natural Science Foundation of China (Grants No. 62101180, No. 61901483, No. 62371459, and No. 62061136011), National Key Research and Development Program of China (Grant No. 2019QY0702), Research Fund Program of State Key Laboratory of High Performance Computing (Grants No. 202001-02 and No. 202101-25), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300704), Aid Program for Science Technology Innovative Research Team in Higher Educational Institutions of Hunan Province, Fundamental Research Funds for the Central Universities (Grant No. 531118010371), Key Research and Development Program of Hunan Province (Grant No. 2022GK2016), Key Project of Scientific Research of Hunan Provincial Education Department (Grants No. 21A0470, No. 22A0669, and No. 22C0446), and Hunan Provincial Natural Science Foundation of China (Grants No. 2022JJ30163, No. 2023JJ50268, and No. 2023JJ50269).

Q.P. and A.H. conducted the experiment. Q.P. and A.H. analyzed the data. Q.P., Q.L., Z.Z., H.Z., and A.H. wrote the paper with input from all authors. A.H. and Y.G. supervised the project.

APPENDIX A: SECRET KEY RATE OF GMCS CV QKD

In the case of a collective attack, the secret key rate K with n received pulses used for establishing the key for reverse coordination is expressed as [8]

$$K = \frac{n}{N} [\beta I_{AB} - \epsilon_{BE} - \Delta(n)], \quad (\text{A1})$$

where $n = N - m$ and β is the reconciliation efficiency. The Shannon mutual information between Alice and Bob becomes

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2} \log_2 \frac{V_{A_0} + \chi_{\text{tot}} + 1}{\chi_{\text{tot}} + 1}. \quad (\text{A2})$$

The total noise at the input of the reference channel represents $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T$, where T is the transmission efficiency, $\chi_{\text{line}} = 1/T - 1 - \epsilon$, and $\chi_{\text{hom}} = (1 + v_{el} - \eta)/T$. The covariance matrix between Alice and Bob can be written as

$$\Gamma = \begin{bmatrix} aI_2 & c\sigma_Z \\ c\sigma_Z & bI_2 \end{bmatrix} \times \begin{bmatrix} (V_{A_0} + 1)I_2 & \sqrt{T_{\min}(V_{A_0}^2 + 2V_{A_0})}\sigma_Z \\ \sqrt{T_{\min}(V_{A_0}^2 + 2V_{A_0})}\sigma_Z & [T_{\min}(V_{A_0} + \epsilon_{\max}) + 1]I_2 \end{bmatrix}, \quad (\text{A3})$$

where $I_2 = \text{diag}[1, 1]$, $\sigma_Z = \text{diag}[1, -1]$, and T_{\min} and ϵ_{\max} correspond to the lower bound of T and the upper bound of ϵ , respectively. When m is large enough ($m > 10^6$), T_{\min} and ϵ_{\max} are expressed as [56]

$$T_{\min} = \frac{(t + \Delta t)^2}{\eta}, \quad \epsilon_{\max} = \frac{\sigma^2 + \Delta\sigma^2 - N_0 - N_0 v_{el}}{N_0 t^2}, \quad (\text{A4})$$

where

$$t = \sqrt{\eta T}, \quad \Delta t = Z_{\epsilon_{PE}/2} \sqrt{\frac{\sigma^2}{m V_{A_0}}},$$

$$\sigma^2 = \eta T \xi + v_{el} + 1, \quad \Delta\sigma^2 = Z_{\epsilon_{PE}/2} \frac{\sigma^2 \sqrt{2}}{\sqrt{m}}. \quad (\text{A5})$$

Here χ_{BE} represents the maximum value of the Holevo information compatible with the statistics except with probability ϵ_{PE} , which can be calculated as

$$\chi_{BE} = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^5 G\left(\frac{\lambda_i - 1}{2}\right), \quad (\text{A6})$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$ and $\lambda_{1,2,3,4,5}$ are symplectic eigenvalues that can be written as

$$\lambda_{1,2}^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \quad \lambda_{3,4}^2 = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \quad (\text{A7})$$

where

$$A = a^2 + b^2 - 2c, \quad B = ab - c^2,$$

$$C = \frac{b + aB + A}{b + 1}, \quad D = \frac{B(a + B)}{b + 1}. \quad (\text{A8})$$

Moreover, $\Delta(n)$ is a linear function of n in Eq. (A1), which is related to the security of privacy amplification. In a practical CV QKD, it is expressed as

$$\Delta(n) = 7 \sqrt{\frac{\log_2(1/\bar{\epsilon})}{n} + \frac{2}{n} \log_2 \frac{1}{\epsilon_{PA}}}, \quad (\text{A9})$$

where $\bar{\epsilon}$ and ϵ_{PA} denote the smoothing parameter and the failure probability of privacy amplification, respectively. Usually, $\bar{\epsilon}$ and ϵ_{PA} take the same value as ϵ_{PE} because the value of $\Delta(n)$ mainly depends on n .

Based on the above equation, it can be concluded that the secret key rate is a function of the above parameters, $K_o = (V_{A_0}, T, \epsilon, v_{el})$. If CV QKD does not detect the modulation variance, then Alice and Bob cannot perceive the change of V_{A_0} . Therefore, when there is a laser-seeding attack, CV QKD evaluates the system secret key rate as $K_e = (V_{A_0}, T', \epsilon', v_{el})$. However, the practical secret key should be calculated as $K_P = (V'_{A_0}, T, \epsilon, v_{el})$. Here

$$V'_{A_0} = gV_{A_0}, \quad T' = gT, \quad \epsilon' = \epsilon/g. \quad (\text{A10})$$

APPENDIX B: SECRET KEY RATE OF MDI CV QKD

In this Appendix we focus on the secret key rate of the MDI CV QKD system under a one-mode collective Gaussian attack. The one-mode attack is generally considered to be the optimal attack [57], but this is based on the existence of a

correlation between the two quantum channels. However, in the MDI CV QKD system, the two quantum channels come from different directions, reducing their correlation. Therefore, the quantum channel of MDI CV QKD can be reduced to a one-mode channel. Eve can efficiently perform one-mode attacks.

Here we assume that the heterodyne detection is perfect and does not consider the finite-size effect. It should be noted that doing so did not affect our analysis results [58]. The Shannon mutual information between Alice and Bob becomes [59]

$$I_{AB} = 2 \frac{1}{2} \log_2 \frac{V_B}{V_{B|A}} = \log_2 \left(\frac{1 + T(V_{A_0} + \chi_{\text{line}} + 1)}{1 + T(1 + \chi_{\text{line}})} \right), \quad (\text{B1})$$

where $V_B = [T(\chi_{\text{line}} + 1) + 1]/2$. Furthermore, the covariance matrix between Alice and Bob can be written as

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

$$\times \begin{bmatrix} (V_{A_0} + 1)I_2 & \sqrt{T[(V_{A_0} + 1)^2 - 1]}\sigma_Z \\ \sqrt{T[(V_{A_0} + 1)^2 - 1]}\sigma_Z & [T(V_{A_0} + \epsilon_m) + 1]I_2 \end{bmatrix}, \quad (\text{B2})$$

where $T = k^2 T_{AC}/2$. In order to minimize excess noise ϵ , we adopt $k^2 = 2V_B/T_{BC}(V_{B+2})$; then

$$\epsilon = \frac{T_{BC}(\epsilon_{BC} - 2) + 2}{T_{AC}} + \epsilon_{AC}. \quad (\text{B3})$$

The Holevo bound can be obtained as $\chi_{BE} = G[(\lambda_1 - 1)/2] + G[(\lambda_2 - 1)/2] - G[(\lambda_3 - 1)/2]$, where

$$\lambda_1^2 = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}),$$

$$\lambda_3 = \frac{(T\epsilon + 2)(V_{A_0} + 1) - TV_{A_0}}{T(\epsilon + V_{A_0}) + 2}. \quad (\text{B4})$$

Finally, the secret key rate of MDI CV QKD can be written as

$$K_o(V_{A_0}, V_B, T, \epsilon) = \beta(I_{AB} - \chi_{BE}). \quad (\text{B5})$$

After the above analysis, we can already calculate the secret key rate of MDI CV QKD. However, in practice, the previous MDI CV QKD system may encounter the following two situations. First, Alice and Bob do not know that Eve has carried out a laser-seeding attack, so the evaluation secret key rate is denoted by $K_e(V_{A_0}, V_B, T, \epsilon')$. Second, Alice and Bob know that Eve has carried out a laser-seeding attack, so the correct secret key rate is denoted by $K_P(V'_{A_0}, V'_B, T', \epsilon)$. Here

$$V'_A = gV_{A_0}, \quad V'_B = gV_B, \quad T' = \frac{gT_{AC}V_B}{T_{BC}(gV_B + 2)},$$

$$\epsilon' = \frac{T_{BC}}{T_{AC}} \left(\frac{\epsilon_{BC}}{g} - 2 \right) + \frac{\epsilon_{AC}}{g} + \frac{2}{gT_{AC}}. \quad (\text{B6})$$

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using Gaussian-modulated coherent states, *Nature (London)* **421**, 238 (2003).
- [3] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, *Nat. Photon.* **7**, 378 (2013).
- [4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, *Rev. Mod. Phys.* **84**, 621 (2012).
- [5] A. K. Ekert, in *Quantum Measurements in Optics*, edited by P. Tombesi and D. F. Walls, NATO Advanced Studies Institute, Series B: Physics (Springer, New York, 1992), Vol. 282, pp. 413–418.
- [6] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [7] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, Security of continuous-variable quantum key distribution against general attacks, *Phys. Rev. Lett.* **110**, 030502 (2013).
- [8] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, *Phys. Rev. Lett.* **114**, 070501 (2015).
- [9] C. Li, L. Qian, and H.-K. Lo, Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources, *npj Quantum Inf.* **7**, 150 (2021).
- [10] B. Qi, Simultaneous classical communication and quantum key distribution using continuous variables, *Phys. Rev. A* **94**, 042340 (2016).
- [11] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Asymptotic security of continuous-variable quantum key distribution with a discrete modulation, *Phys. Rev. X* **9**, 021059 (2019).
- [12] K. Brádler and C. Weedbrook, Security proof of continuous-variable quantum key distribution using three coherent states, *Phys. Rev. A* **97**, 022310 (2018).
- [13] N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61**, 052304 (2000).
- [14] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, *Nat. Commun.* **2**, 349 (2011).
- [15] S. Sun and A. Huang, A review of security evaluation of practical quantum key distribution system, *Entropy* **24**, 260 (2022).
- [16] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, *Phys. Rev. A* **74**, 022313 (2006); **78**, 019905(E) (2008).
- [17] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Thermal blinding of gated detectors in quantum cryptography, *Opt. Express* **18**, 27938 (2010).
- [18] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, Superlinear threshold detectors in quantum cryptography, *Phys. Rev. A* **84**, 032320 (2011).
- [19] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch, *Phys. Rev. A* **91**, 062301 (2015).
- [20] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, *IEEE J. Quantum Electron.* **52**, 8000211 (2016).
- [21] P. Chaiwongkhot, J. Zhong, A. Huang, H. Qin, S.-c. Shi, and V. Makarov, Faking photon number on a transition-edge sensor, *EPJ Quantum Technol.* **9**, 23 (2022).
- [22] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, *Quantum Inf. Comput.* **7**, 73 (2007).
- [23] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, *Phys. Rev. A* **78**, 042333 (2008).
- [24] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack, *Phys. Rev. A* **87**, 062329 (2013).
- [25] H.-W. Li, S. Wang, J.-Z. Huang, W. Chen, Z.-Q. Yin, F.-Y. Li, Z. Zhou, D. Liu, Y. Zhang, G.-C. Guo, W.-S. Bao, and Z.-F. Han, Attacking a practical quantum-key-distribution system with wavelength-dependent beam-splitter and multiwavelength sources, *Phys. Rev. A* **84**, 062308 (2011).
- [26] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, *Phys. Rev. A* **87**, 062313 (2013).
- [27] Z. He, Y. Wang, and D. Huang, Wavelength attack recognition based on machine learning optical spectrum analysis for the practical continuous-variable quantum key distribution system, *J. Opt. Soc. Am. B* **37**, 1689 (2020).
- [28] Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, Polarization attack on continuous-variable quantum key distribution, *J. Phys. B* **52**, 015501 (2019).
- [29] D. Huang, S. Liu, and L. Zhang, Secure continuous-variable quantum key distribution with machine learning, *Photonics* **8**, 511 (2021).
- [30] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Homodyne-detector-blinding attack in continuous-variable quantum key distribution, *Phys. Rev. A* **98**, 012312 (2018).
- [31] C. Li, C. Hu, W. Wang, R. Wang, and H.-K. Lo, Passive continuous variable quantum key distribution, [arXiv:2212.01876](https://arxiv.org/abs/2212.01876).
- [32] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [33] Q. Liao, G. Xiao, C.-G. Xu, Y. Xu, and Y. Guo, Discretely modulated continuous-variable quantum key distribution with an untrusted entanglement source, *Phys. Rev. A* **102**, 032604 (2020).
- [34] Q. Liao, G. Xiao, H. Zhong, and Y. Guo, Multi-label learning for improving discretely-modulated continuous-variable quantum key distribution, *New J. Phys.* **22**, 083086 (2020).
- [35] Q. Liao, H. Liu, L. Zhu, and Y. Guo, Quantum secret sharing using discretely modulated coherent states, *Phys. Rev. A* **103**, 032410 (2021).
- [36] C. H. F. Fung, B. Qi, K. Tamaki, and H. K. Lo, Phase-remapping attack in practical quantum-key-distribution systems, *Phys. Rev. A* **75**, 032314 (2007).
- [37] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, *New J. Phys.* **12**, 113026 (2010).

- [38] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, *Nat. Photon.* **4**, 686 (2010).
- [39] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, Controlling a superconducting nanowire single-photon detector using tailored bright illumination, *New J. Phys.* **13**, 113042 (2011).
- [40] B. Gao, Z. Wu, W. Shi, Y. Liu, D. Wang, C. Yu, A. Huang, and J. Wu, Strong pulse illumination hacks self-differencing avalanche photodiode detectors in a high-speed quantum key distribution system, *Phys. Rev. A* **106**, 033713 (2022).
- [41] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography, *Phys. Rev. Lett.* **112**, 070503 (2014).
- [42] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Creation of backdoors in quantum communications via laser damage, *Phys. Rev. A* **94**, 030302(R) (2016).
- [43] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, and V. Makarov, Laser-damage attack against optical attenuators in quantum key distribution, *Phys. Rev. Appl.* **13**, 034017 (2020).
- [44] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, *New J. Phys.* **16**, 123030 (2014).
- [45] S. Sajeed, C. Minshull, N. Jain, and V. Makarov, Invisible Trojan-horse attack, *Sci. Rep.* **7**, 8403 (2017).
- [46] Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack, *Opt. Express* **27**, 27369 (2019).
- [47] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, Laser-seeding attack in quantum key distribution, *Phys. Rev. Appl.* **12**, 064043 (2019).
- [48] Y. Pan, L. Zhang, and D. Huang, Practical security bounds against Trojan horse attacks in continuous-variable quantum key distribution, *Appl. Sci.* **10**, 7788 (2020).
- [49] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* **73**, 022320 (2006).
- [50] M. Curty and N. Lütkenhaus, Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses, *Phys. Rev. A* **71**, 062301 (2005).
- [51] N. Lütkenhaus and M. Jahma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, *New J. Phys.* **4**, 44 (2002).
- [52] F.-Y. Lu, P. Ye, Z.-H. Wang, S. Wang, Z.-Q. Yin, R. Wang, X.-J. Huang, W. Chen, D.-Y. He, G.-J. Fan-Yuan *et al.*, Hacking measurement-device-independent quantum key distribution, *Optica* **10**, 520 (2023).
- [53] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, Securing practical quantum communication systems with optical power limiters, *PRX Quantum* **2**, 030304 (2021).
- [54] Q. Peng, B. Gao, K. Zaitsev, Y. Guo, A. Huang, and J. Wu, Security boundaries of an optical power limiter for protecting quantum key distribution systems, [arXiv:2303.12355](https://arxiv.org/abs/2303.12355).
- [55] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, Hacking quantum key distribution via injection locking, *Phys. Rev. Appl.* **13**, 034008 (2020).
- [56] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, *Phys. Rev. A* **81**, 062343 (2010).
- [57] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photon.* **9**, 397 (2015).
- [58] X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, and H. Guo, Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution, *Phys. Rev. A* **96**, 042334 (2017).
- [59] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Continuous-variable measurement-device-independent quantum key distribution with photon subtraction, *Phys. Rev. A* **97**, 042329 (2018).