# Analysis of an injection-locking-loophole attack from an external source for quantum key distribution

Xiao-Xu Zhang,[1,2,3,*] Mu-Sheng Jiang,[1,2] Yang Wang,[1,2] Yi-Fei Lu,[1,2] Hong-Wei Li,[1,2]
Chun Zhou,[1,2] Yu Zhou,[1,2] and Wan-Su Bao[1,2,†]

[1] *Henan Key Laboratory of Quantum Information and Cryptography, SSF IEU, Zhengzhou, Henan 450001, China*
[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*
[3] *Basic Department, SSF IEU, Zhengzhou, Henan 450001, China*

(Received 17 January 2022; accepted 30 November 2022; published 12 December 2022)

Many security loopholes exist in quantum key distribution (QKD) due to the imperfections of realistic devices. On the source side, the decoy-state method can defend against the most severe photon-number-splitting (PNS) attack and improve the performance of QKD. Measurement-device-independent QKD and twin-field QKD have further closed all loopholes on the detection side. In this paper, we propose a valuable optical injection-locking loophole for the case when the internal isolator inside the laser is removed. We first introduce the effects of the injection locking with different injection intensities on the source frequency. Through the successive responses of adjacent pulses from frequency ports of the dense wavelength division multiplexer, the decoy state and the signal state can be partially distinguished. The specific injection-locking-loophole analysis of the isolatorless decoy phase-encoding Bennet-Brassard 1984 QKD and decoy phase-matching QKD protocols with external optical injection has been deeply studied. Simulation results show that, if we maintain the same observed gain statistics as normal after an external optical injection locking, the loophole cannot be exploited for a PNS attack when the QKD distance is short. As the QKD distance increases, a PNS attack at a medium distance using the optical injection-locking loophole does not threaten the security; the security is still valid. With the further increase of the QKD distance, the lower-bound secure key rate is higher than the upper-bound secure key rate given by a PNS attack at a long distance, some of the keys must be insecure, and information will be leaked.

DOI: 10.1103/PhysRevA.106.062412

## I. INTRODUCTION

Quantum. key distribution (QKD) allows two distant parties to generate information-theoretic secure keys, which has been proven in theories [1,2] and demonstrated in experiments [3]. However, due to imperfect devices, QKD has many practical security loopholes [4–13]. On the source side, a weak coherent photon source (WCPS) is often used instead of a single-photon source. The multiphoton signals generated by WCPS open the door to powerful eavesdropping attacks, including the photon-number-splitting (PNS) attack, which can be addressed by the decoy-state method [14–16]. Meanwhile, many attacks [10–13] target the most vulnerable detection side of any QKD device. All security loopholes on the detection side are closed by measurement-device-independent QKD (MDI-QKD) [17–20] protocols by performing a two-photon Bell-state measurement in the intermediate node. However, the photons are inevitably lost in the fiber channel; then the key rate of most QKD protocols, including MDI-QKD, is rigorously limited by the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [21]. Fortunately, a novel twin-field QKD (TF-QKD) [22] protocol was proposed to surpass the linear PLOB bound. TF-QKD exploits single-photon interference and shows the superior relation between the key rate and channel transmittance, $R \propto \sqrt{\eta}$.

However, the security proof is imperfect in the original TF-QKD protocol [22]. In order to give a more rigorous security proof when considering practical issues, three main practical variant TF-QKD protocols have been proposed [23–26]. The phase-matching QKD (PM-QKD) protocol gives the first rigorous security analysis for coherent-state-based QKD protocols [23]. It employs a phase postcompensation technology and does not need the phase feedback precompensation, so it is easy to implement experimentally. The sending-or-not-sending TF-QKD (SNS-TF-QKD) protocol can tolerate large misalignment errors [24]. The key states are encoded as “sending” or “not sending” the coherent states, and interference is not required, so SNS-TF-QKD has strong antinoise capability and a long key distribution distance. The signal state of the no-phase-postselection TF-QKD (NPP-TF-QKD) protocol has no phase randomization [25,26], so the NPP-TF-QKD reestablishes the photon number channel and provides better key-rate performance. In addition, NPP-TF-QKD requires phase feedback precompensation, which makes the experiment more difficult.

With the development of TF-QKD theory protocols, a series of important advances has been made in experiments [27–37]. Experimentally, there are two main technical chal-

[*] zxx@qiclab.cn
[†] bws@qiclab.cn

lenges. One is the frequency locking of nonlocal lasers, and the other is the compensation of the fast phase drift. Common solutions for the frequency locking include the optical phase-locked loop (OPLL) [27–29], the Pound-Drever-Hall (PDH) [30,31] method, and optical injection locking [32,33]. The OPLL and PDH methods need feedback control technology, such as temperature, external cavity length, or external frequency modulation, so their experimental implementation is relatively complicated. The optical injection locking is generated by strong light injection from an external source which enforces stimulated radiation. This locking is easier to implement experimentally, but it can introduce some practical security loopholes because the internal isolator inside the laser needs to be removed and no isolator can be placed on the injection channel. For example, increasing the intensity of the injected light will increase the intensity of the light at the output of the transmitter [32,33].

A Trojan-horse attack is a common attack method, especially for plug-and-play systems. When Eve injects strong light into Alice and Bob, information leakage is detected by observing the back-reflected light of the intensity modulator or phase modulator on frequency [38,39]. If the internal isolator inside the laser is removed, the externally injected strong light will enter the laser and lock the output frequency of the laser, thus causing a different type of security loophole. This is the optical injection-locking security loophole proposed by us, which is inspired by the adoption of external optical injection in [32,33,40]. The core of the optical injection-locking loophole is the injection frequency locking (unlocking) of the laser by different injecting intensities rather than back-reflected light. Through the successive responses of adjacent pulses, which are from the same or different frequency ports of the dense wavelength division multiplexer (DWDM), Eve can partially distinguish the decoy state from the signal state.

In this paper, the optical injection-locking loophole is used for a PNS attack on the isolatorless decoy phase-encoding Bennet-Brassard 1984 QKD (BB84-QKD) to obtain perfect keys at a long distance without being discovered. The scheme has also been used for isolatorless decoy PM-QKD; because the discrete phase is not the global phase, it will inevitably increase the quantum bit error rate (QBER). Indeed, analyses of isolatorless decoy SNS-QKD and NPP-QKD would be better; the reason is that the signal state is encoded in intensity for SNS-QKD, and there is no phase randomization of the signal state for NPP-QKD. Further research is reserved for the future.

This paper is arranged as follows: In Sec. II, we introduce the effect of suitable externally injected light on the frequency. In Sec. III, the specific optical injection-locking-loophole analyses for the isolatorless decoy phase-encoding BB84-QKD and decoy PM-QKD protocols are depicted. Simulation results are presented and discussed in Sec. IV. Countermeasures are shown in Sec. V, and then we conclude in Sec. VI.

## II. THE OPTICAL INJECTION LOCKING

As shown in Fig. 1, the continuous master laser with a center frequency of $f_1$ is injected into the slave laser with a center frequency of $f_2$ through the circulator (CIR) and intensity modulator (IM); the angular frequency offset $\Delta\omega = 2\pi(f_1 - f_2)$. Suppose the intensity of the master laser passing through the IM is $I$ and the angular frequency offset satisfies the following formula [41]: $\Delta\omega < |-k_M\sqrt{1+\alpha^2}\sqrt{\frac{I}{I_0}}|$, where $\alpha$ is the linewidth enhancement factor, $I_0$ is the intensity of the slave laser, and $k_M$ is the injection strength; then the slave laser can be locked, and the central output frequency will be the same as that of the master laser. The reason is that injection photons suppress spontaneous radiation and enforce stimulated emission of the slave laser [42,43]. Yuan [44,45] proposed and experimentally demonstrated a similar direct phase-modulated light source which is suitable for diverse applications, such as coherent communications and quantum cryptography. If the intensity of the master laser does not satisfy the above formula, the slave laser will be unlocked and exhibit nonlinear characteristics.

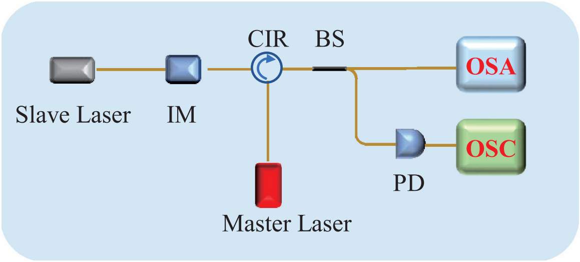


FIG. 1. Experimental setup of the single-optical-injection semiconductor laser. IM: intensity modulator, CIR: circulator, BS: beam splitter, PD: photodetector, OSA: optical spectrum analyzer, OSC: oscilloscope.

The experimental spectra from the master laser and the slave laser are shown in Fig. 2; $I_1$ and $I_2$ are intensities injected into the slave laser from the master laser. The black and pink solid lines are the experimental spectra of the slave laser with injection intensities $I_1$ and $I_2$. The black dashed line is the free-running master-laser spectrum with central frequency $f_1$. The red dashed line is the free-running slaver-laser spectrum with

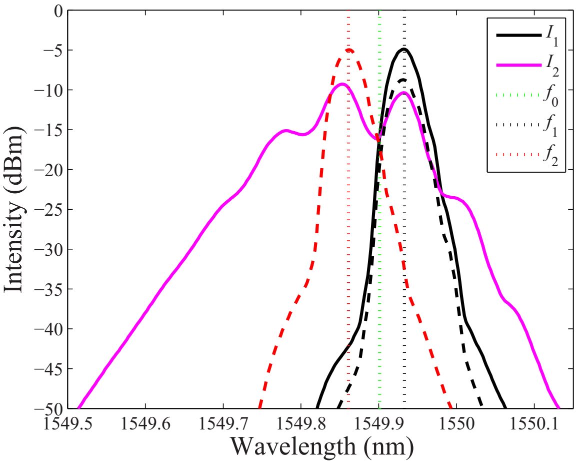


FIG. 2. The black and pink solid lines are the experimental spectra of the slave laser with injection intensities $I_1$ and $I_2$. The black and red dashed lines are the experimental spectra of the free-running master and slave lasers. The middle green, right black, and left red dotted lines represent the reference frequencies $f_0$, $f_1$, and $f_2$.

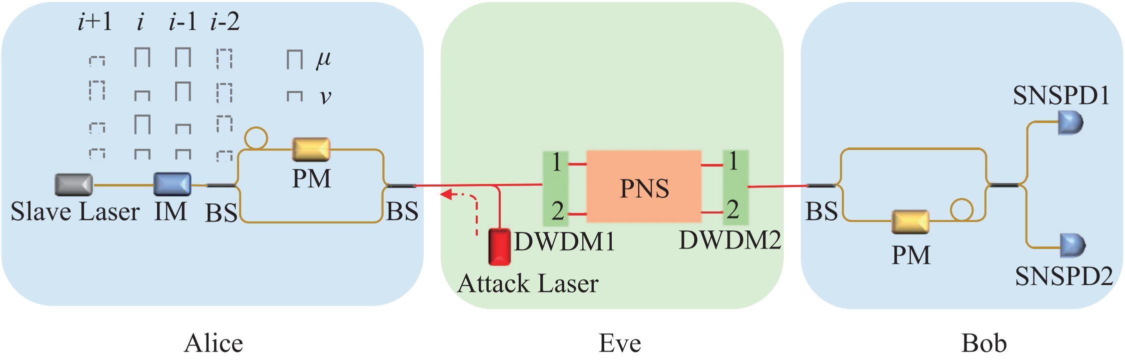


FIG. 3. The optical injection-locking-loophole analysis scheme for isolatorless decoy phase-encoding BB84-QKD. IM: intensity modulator, PM: phase modulator, BS: beam splitter, DWDM: dense wavelength division multiplexer, SNSPD: superconducting-nanowire single-photon detector.

central frequency $f_2$; in other words, the injection intensity $I = 0$. The black solid line is the spectrum of the slave laser locked by the injection intensity $I_1$, which satisfies the above formula, and then the center frequency $f_1$ is consistent with the master laser. The pink solid line is the slave-laser spectrum unlocked by the injection intensity $I_2$ (the injection intensity $I_2 \neq 0$); the spectrum is broadened and exhibits complex dynamic characteristics. Further research has shown that when the slave laser is unlocked, the spectrum of the slave laser varies with the injection intensity. See Appendix A for more details on the intensity time series.

We take the green dotted line in the middle as the reference frequency $f_0$. When the injection intensity is $I_1$, $\xi_{f_1|I_1}$ ($\xi_{f_2|I_1}$) is defined as the frequency of the slave laser whose output frequency component is greater (less) than $f_0$; the purpose of this definition is to facilitate the subsequent optical injection-locking-loophole attack. When the injection intensity is $I_2$, a similar definition can be given by $\xi_{f_1|I_2}$ ($\xi_{f_2|I_2}$). Meanwhile, we use $I_2{:}I_1 = 1{:}2.25$ in the experiment; then the calculation of experimental data shows that $\xi_{f_1|I_1} = 99.2\%$ and $\xi_{f_2|I_2} = 69.6\%$.

It is worth noting that there is also an inevitable intensity fluctuation of the slave laser when the injection intensity is $I_2$, and the period of the intensity fluctuation is roughly the same as that of the relaxation oscillation; see Appendix A for more details.

Through studies of optical injection locking, we can partially judge the signal state and decoy state of some QKD protocols by detecting the spectral components; details are given in Sec. III.

## III. THE OPTICAL INJECTION-LOCKING-LOOPHOLE ANALYSIS

### A. The optical injection-locking-loophole analysis of isolatorless decoy phase-encoding BB84-QKD

The isolatorless decoy phase-encoding BB84-QKD with the asymmetric Mach-Zehnder interferometer is single-photon interference, which can make use of the loophole of optical injection locking for security analysis; this scheme is shown in Fig. 3. Suppose a weak coherent-state pulse source without the internal isolator is prepared by Alice, the center frequency of Alice's pulse laser is $f_2$, and the center frequency of Eve's continuous laser is $f_1$. For the convenience of analysis, only one decoy state is used; the intensities of the signal state and decoy state are $\mu$ and $v$, respectively.

The details of the security analysis using the optical injection-locking loophole are as follows:

(1) When the light from the attack laser is injected into Alice's laser through the IM, the attack light passing through the $i$th pulse will affect the center frequency of Alice's $(i+1)$th pulse in the opposite direction; one precondition is that Alice's pulse period must match the time interval between the slave laser and IM. In other words, the preceding pulse will affect the after pulse due to Eve's attack. Then the affected $(i+1)$th pulse light from Alice's laser passes through the interferometer into DWDM1. The frequencies of the light coming from port 1 and port 2 are greater and smaller than the reference frequency $f_0$. When only one port contains multiple photons, we can use a PNS attack because the signal state and decoy state of the $i$th pulse can be partially distinguished.

(2) If the $i$th pulse does not contain photons, we cannot attack even if we correctly judge that the $i$th pulse is a signal state or a decoy state by the $(i+1)$th pulse. Similarly, if the $i$th pulse contains photons but the $(i+1)$th pulse does not, we still cannot judge whether the $i$th pulse is a signal state or a decoy state. That is to say, the specific attack needs to take into account the case that both the $i$th pulse and the $(i+1)$th pulse contain photons while discarding the other cases; then a PNS attack on the $i$th pulse can be executed.

(3) As shown in Table I, when the $i$th pulse of Alice via the IM is a signal state, we can get the photon probability of the $(i+1)$th pulse from port 1 or port 2; the photon probability from port 1 (port 2) is that we correctly judge (misjudge) the $i$th pulse as a signal state. Similarly, when the $i$th pulse of Alice via the IM is a decoy state, the photon probability from port 1 (port 2) is that we misjudge (correctly judge) the $i$th pulse as a decoy state.

(4) It is worth noting that, with the output from port 1 and port 2, there is a probability that we will misjudge the signal state and decoy state of the $i$th pulse, but it does not affect our PNS attack. To illustrate the point, we further consider the QBER with Eqs (C1a) and (C1b).

(5) In an actual attack scheme, we just have to satisfy the conditions that the detection statistics on the receiver's side are not disturbed and let the remaining photons prop-

TABLE I. The distinction between the signal state and decoy state on the *i*th pulse of decoy BB84-QKD.

| | $(i+1)$th pulse | | $i$th pulse | |
|---|---|---|---|---|
| Intensity | Photon probability from port 1 | Photon probability from port 2 | Intensity | Photon probability |
| $\mu$ | $P_{\mathrm{S}}(1-P_{0\|\mu})P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_1}$ | $P_{\mathrm{S}}(1-P_{0\|\mu})P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{S}}(1-P_{0\|\mu})$ |
| $\nu$ | $P_{\mathrm{S}}(1-P_{0\|\mu})P_{D}(1-P_{0\|\nu})\xi_{f_1\|I_1}$ | $P_{\mathrm{S}}(1-P_{0\|\mu})P_{D}(1-P_{0\|\nu})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{S}}(1-P_{0\|\mu})$ |
| $\mu$ | $P_{\mathrm{D}}(1-P_{0\|\nu})P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_2}$ | $P_{\mathrm{D}}(1-P_{0\|\nu})P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{D}}(1-P_{0\|\nu})$ |
| $\nu$ | $P_{\mathrm{D}}(1-P_{0\|\nu})P_{\mathrm{D}}(1-P_{0\|\nu})\xi_{f_1\|I_2}$ | $P_{\mathrm{D}}(1-P_{0\|\nu})P_{\mathrm{D}}(1-P_{0\|\nu})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{D}}(1-P_{0\|\nu})$ |

agate at yields of $Z_i^{\mu}$ and $Z_i^{\nu}$; see Appendix B for more details.

The key-rate lower bound of decoy BB84-QKD is

$$R_{\mathrm{BB84}}^{l} = P_1 Y_1^s\left[1 - H\left(E_1^s\right)\right] - f Q_\mu H(E_\mu), \tag{1}$$

where $Q_\mu$ and $E_\mu$ are the overall gain and QBER, $f$ is the error-correction efficiency, and $Y_1^s$ and $E_1^s$ are the yield and the phase error rate of the single-photon signal state, respectively, we can estimate using the decoy-state method. $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

A PNS attack is carried out by using the optical injection-locking loophole; then the upper bound of the BB84-QKD secure key rate is

$$R_{\mathrm{BB84\_E}}^{u} = e^{-\mu}\mu Z_{1\_\mathrm{BB84}}^{s}, \tag{2}$$

where $Z_{1\_\mathrm{BB84}}^{s}$ is the best optimum single-photon yield of the signal state sent to Bob when Eve uses the optical injection-locking loophole to carry out a PNS attack; see Appendix B for more details.

It should be noted that Eve can successfully steal the keys only if the upper bound of the secure key rate after an attack is smaller than the lower bound of the secure key rate [46]. Since the lower bound represents the key rate at which Alice and Bob generate a new key that they think is secure, if the lower-bound secure key rate is higher than the upper-bound secure key rate given by our PNS attack, some of the keys must be insecure, and Eve will steal some keys from them.

Overall, we can use the optical injection-locking loophole to carry out a PNS attack on the isolatorless decoy phase-encoding BB84-QKD scheme; the critical assumptions we need are that there is no isolator at the output of the transmitter and that Alice's pulse laser lacks the internal isolator. Meanwhile, the pulse width is wider than the relaxation oscillation period to ensure that the intensity fluctuation is smaller. The pulse period of the slave laser must match the time interval between the slave laser and IM. It is worth mentioning that we do not need to consider the effect of the phase modulator on the injection because the randomized phase of the BB84-QKD protocol is the global phase.

### B. The optical injection-locking-loophole analysis of isolatorless decoy PM-QKD

TF-QKD requires phase locking of the source, and strong light injection locking is a simple way to achieve phase locking. It must be noted that the laser removing the internal isolator is an essential precondition for optical injection. At the same time, because the time jitter caused by long-distance transmission is significant, to meet the interference between pulses, the pulse width is generally set to be large, so the pulse width is wider than the relaxation oscillation period to ensure that the intensity fluctuation is smaller, which was discussed above. Therefore, the injection-locking loophole is a natural threat to decoy TF-QKD when it uses external injection locking. The remaining conditions need to ensure only that the pulse period of the slave laser matches the time interval between the slave laser and IM and the modulation period of the IM must not match the time interval between the IM and PM. We focus on optical injection-locking-loophole analysis of PM-QKD. This scheme is shown in Fig. 4; Alice and Bob prepare a weak coherent-state pulse source without the internal isolator. As the master laser, Charlie emits strong continuous light, amplified by the erbium-doped optical fiber amplifier and then injected into Alice and Bob. The injection-locking (-unlocking) light from Alice and Bob is modulated by IMs and PMs. The IMs are used to modulate the intensity of the signal state and decoy state; for the convenience of analysis, only one decoy state is used. The PMs are used for encoding and discrete phase randomization and then go through the quantum channel into Charlie's terminal and cause interference. The details of security analysis using the optical injection-locking loophole are as follows:

(1) To maintain the consistency of frequency, Eve divides light from the classical channel and injects it into the attack laser; that is to say, the attack laser can be regarded as the slave laser of the master laser, so it can be locked by the master laser. Theoretically, the master laser and the attack laser are a twin field.

(2) The light injected from the master laser into the slave laser of Alice (Bob) is cut off in the middle. The attack laser is set as the master laser with center frequency $f_1$; then the slave laser of Alice (Bob) is injected through PMs and IMs in the opposite direction. As discussed below, the analysis is more complicated than in Sec. III A because the type of frequency (as shown in Fig. 2 by the pink line) will modify the phase of the emitted pulses and hence scramble the interference at Charlie, which does not affect BB84-QKD.

(3) As seen in Table II, when the $(i-1)$th pulse of the salve laser via the IM is a signal state, the preceding pulse will affect the after pulse due to Eve's attack; we can get the photon probability of the $i$th pulse from port 1, and the photon probability from port 1 is that we correctly judge the $(i-1)$th pulse as a signal state. Meanwhile, we discard the case from port 2; the photon probability from port 2 is that we misjudge the $(i-1)$th pulse as a signal state. Similarly, from the $(i+1)$th pulse, we can also judge with a certain probability whether the $i$th pulse is a signal state or a decoy state. In brief, we can judge with a certain probability whether the $i$th pulse is a decoy state or a signal state from the $(i+1)$th pulse; at the

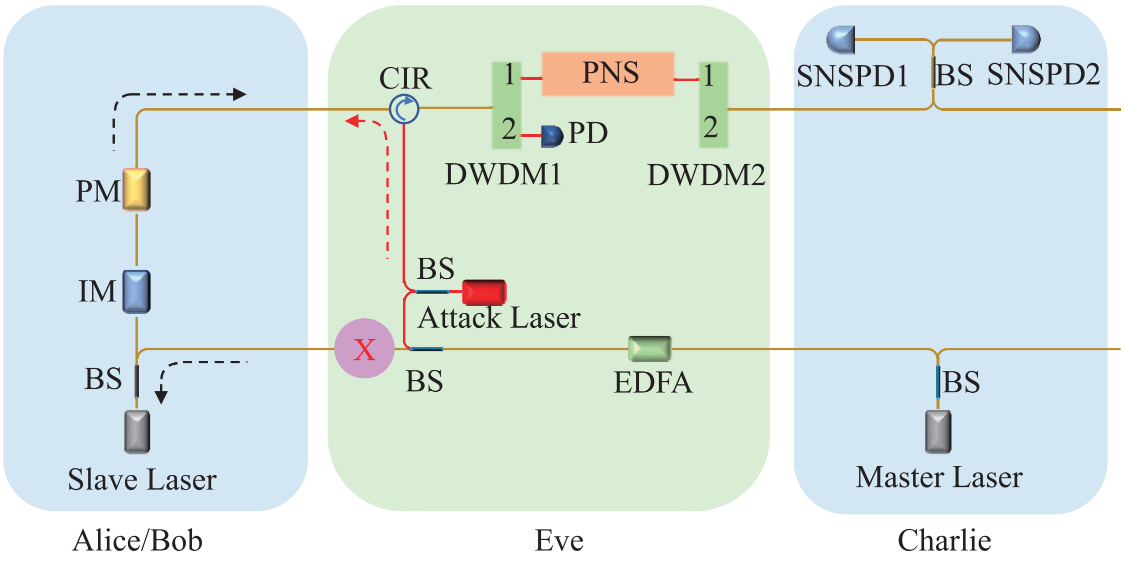


FIG. 4. The optical injection-locking-loophole analysis scheme for isolatorless decoy PM-QKD. IM: intensity modulator, PM: phase modulator, BS: beam splitter, DWDM: dense wavelength division multiplexer, EDFA: erbium-doped optical fiber amplifier, PD: photodetector, SNSPD: superconducting-nanowire single-photon detector.

same time, as long as the $(i-1)$th pulse is a signal state, the $i$th pulse and the $(i+1)$th pulse contain photons, and then a PNS attack on the $i$th pulse can be executed.

(4) Similarly, as can be seen from Table II, when the $(i-1)$th pulse of the slave laser via the IM is a decoy state, the weak optical injection will affect the phase and intensity. It even causes the phase randomization of the $i$th pulse; then phase locking is not satisfied, and errors will occur. We need to discard the photons from port 2 of the $i$th pulse and treat the photons from port 1 of the $i$th pulse as errors. Indeed, they will inevitably increase the QBER and be identified by authorized users. Combining the experimental values $\xi_{f_2|I_2} = 69.6\%$ and the proportion of decoy states (10%), the QBER will increase by about 1.52% in both the signal state and the decoy state. To illustrate the point, we further consider the QBER with Eqs. (C2a) and (C2b). It is worth noting that this loophole has no effect on BB84-QKD. We do not need to discard the photons after the decoy state because the randomized phase of the BB84-QKD protocol is the global phase.

(5) A PNS attack is carried out on the $i$th pulse from port 1, where the signal state and decoy state can be judged to optimize the yields of $Z_i^{\mu}$ and $Z_i^{v}$. The conditions that the detection statistics on the receiver's side are not disturbed need be satisfied; see Appendix B for more details.

The key-rate lower bound of decoy PM-QKD is

$$R_{\mathrm{PM}}^{l} = \frac{2}{D} Q_{\mu}[1 - H(E_X) - fH(E_Z)], \tag{3}$$

where $D$ is the phase slice, $Q_{\mu}$ and $E_Z$ are the overall gain and QBER, and $E_X$ is the phase error rate, which we can also estimate using the decoy-state method [47].

After a PNS attack is carried out by using the optical injection-locking loophole, the upper bound of the PM-QKD secure key rate is

$$R_{\mathrm{PM\_E}}^{u} = e^{-\mu} \mu Z_{1\_\mathrm{PM}}^{s}, \tag{4}$$

where $Z_{1\_\mathrm{PM}}^{s}$ is the best optimum single-photon yield of the signal state sent to Charlie by Alice and Bob when Eve uses the optical injection-locking loophole to carry out a PNS attack; see Appendix B for more details.

Eve's attack aims to let the upper bound of the secure key rate be small so as not to exceed the lower bound of the secure key rate [46]; then Eve is able to trick Alice and Bob into accepting an insecure key.

TABLE II. The distinction between the signal state and dec e on the $i$th pulse of decoy PM-QKD.

| | $(i+1)$th pulse | | $i$th pulse | | $(i-1)$th pulse |
|---|---|---|---|---|---|
| Intensity | Photon probability from port 1 | Photon probability from port 2 | Intensity | Photon probability from port 1 | Intensity |
| $\mu$ | $P_{\mathrm{S}}^2 P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_1}(1-P_{0\|\mu})\xi_{f_1\|I_1}$ | $P_{\mathrm{S}}^2 P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_1}(1-P_{0\|\mu})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{S}} P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_1}$ | $\mu$ |
| $\nu$ | $P_{\mathrm{S}}^2 P_D(1-P_{0\|\mu})\xi_{f_1\|I_1}(1-P_{0\|v})\xi_{f_1\|I_1}$ | $P_{\mathrm{S}}^2 P_D(1-P_{0\|\mu})\xi_{f_1\|I_1}(1-P_{0\|v})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{S}} P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_1}$ | $\mu$ |
| $\mu$ | $P_{\mathrm{S}}^2 P_D(1-P_{0\|v})\xi_{f_1\|I_1}(1-P_{0\|\mu})\xi_{f_1\|I_2}$ | $P_{\mathrm{S}}^2 P_D(1-P_{0\|v})\xi_{f_1\|I_1}(1-P_{0\|\mu})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{S}} P_D(1-P_{0\|v})\xi_{f_1\|I_1}$ | $\mu$ |
| $\nu$ | $P_{\mathrm{S}} P_D^2(1-P_{0\|v})\xi_{f_1\|I_1}(1-P_{0\|v})\xi_{f_1\|I_2}$ | $P_{\mathrm{S}} P_D^2(1-P_{0\|v})\xi_{f_1\|I_1}(1-P_{0\|v})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{S}} P_D(1-P_{0\|v})\xi_{f_1\|I_1}$ | $\mu$ |
| $\mu$ | $P_{\mathrm{D}} P_{\mathrm{S}}^2(1-P_{0\|\mu})\xi_{f_1\|I_2}(1-P_{0\|\mu})\xi_{f_1\|I_1}$ | $P_{\mathrm{D}} P_{\mathrm{S}}^2(1-P_{0\|\mu})\xi_{f_1\|I_2}(1-P_{0\|\mu})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{D}} P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_2}$ | $\nu$ |
| $\nu$ | $P_{\mathrm{D}}^2 P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_2}(1-P_{0\|v})\xi_{f_1\|I_1}$ | $P_{\mathrm{D}}^2 P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_2}(1-P_{0\|v})\xi_{f_2\|I_1}$ | $\mu$ | $P_{\mathrm{D}} P_{\mathrm{S}}(1-P_{0\|\mu})\xi_{f_1\|I_2}$ | $\nu$ |
| $\mu$ | $P_{\mathrm{D}}^2 P_{\mathrm{S}}(1-P_{0\|v})\xi_{f_1\|I_2}(1-P_{0\|\mu})\xi_{f_1\|I_2}$ | $P_{\mathrm{D}}^2 P_{\mathrm{S}}(1-P_{0\|v})\xi_{f_1\|I_2}(1-P_{0\|\mu})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{D}} P_{\mathrm{D}}(1-P_{0\|v})\xi_{f_1\|I_2}$ | $\nu$ |
| $\nu$ | $P_{\mathrm{D}}^2 P_{\mathrm{D}}(1-P_{0\|v})\xi_{f_1\|I_2}(1-P_{0\|v})\xi_{f_1\|I_2}$ | $P_{\mathrm{D}}^2 P_{\mathrm{D}}(1-P_{0\|v})\xi_{f_1\|I_2}(1-P_{0\|v})\xi_{f_2\|I_2}$ | $\nu$ | $P_{\mathrm{D}} P_{\mathrm{D}}(1-P_{0\|v})\xi_{f_1\|I_2}$ | $\nu$ |

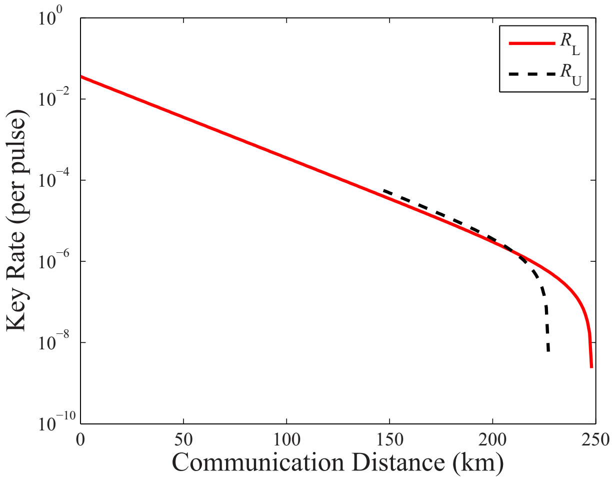


FIG. 5. The secure key rate of the isolatorless decoy phase-encoding BB84-QKD. The red solid line is the lower bound without a PNS attack. The black dashed line is the upper bound under the optical injection-locking loophole with a PNS attack.

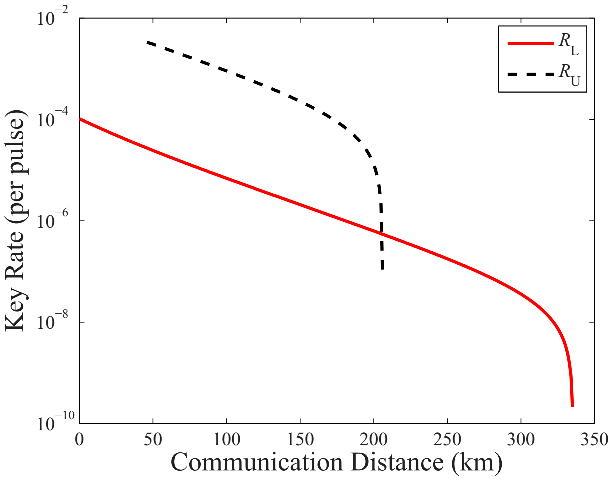


FIG. 6. The secure key rate of the isolatorless decoy PM-QKD. The red solid line is the lower bound without a PNS attack. The black dashed line is the upper bound under the optical injection-locking loophole with a PNS attack.

## IV. RESULTS AND DISCUSSION

From isolatorless decoy phase-encoding BB84-QKD to PM-QKD, the optical injection-locking loophole is used to carry out a PNS attack. First, we use the optical injection-locking loophole to simulate a PNS attack on the isolatorless decoy phase-encoding BB84-QKD. Simulation results can be seen in Fig. 5. Before 145 km, because retaining the same observed gain statistics as normal after an external optical injection locking cannot be guaranteed, Alice and Bob can deduce the disturbance of an attack, and the optical injection-locking loophole cannot be used for a PNS attack. Between 145 and 210 km, Alice and Bob cannot detect the attack; Eve can use the optical injection-locking loophole for a PNS attack, but the key rate is safe. The reason is the upper bound of the secure key rate is higher than the lower bound of the secure key rate. That is to say, the security is still valid before 210 km. After 210 km, Alice and Bob cannot judge the existence of the attack, and the lower bound of the secure key rate is higher than the upper bound under the attack because the lower bound represents the key rate at which Alice and Bob generate a key that they think is secure; therefore, the key is not insecure, Eve can successfully steal the key. In a similar way, we use the same mean number of photons and the optical injection-locking loophole to simulate a PNS attack on the isolatorless decoy PM-QKD. As can be seen in Fig. 6, before 46 km, when Eve uses the loophole to carry out a PNS attack, Alice and Bob can deduce the existence of an attack from the different gain statistics observed in a normal situation, so the optical injection-locking loophole cannot be used for a PNS attack. Between 46 and 207 km, Eve can optimize the yields to get the key rate without being detected by Alice and Bob; a PNS attack using the optical injection-locking loophole does not threaten the security, and the security is still valid. After 207 km, our attack succeeds in stealing the final secret keys because the upper-bound secure key rate drops sharply to zero. Further research showed that, with the increase of the average photon number, the secure key distance would be shorter and shorter regardless of whether it was BB84-QKD or PM-QKD; the reason for this is that, as the mean number of photons increases, the probability of successive responses of adjacent pulses increases.

Moreover, for SNS-QKD and NPP-QKD, when we use lasers without internal isolators for experimental implementation, the secure key distance will be shorter; the reason is that the securities of these two protocols completely depend on the guarantee of the decoy-state method. The signal state is encoded in intensity for SNS-QKD, and there is no phase randomization of the signal state for NPP-QKD.

## V. COUNTERMEASURES

The effects of using the optical injection-locking loophole to carry out a PNS attack on isolatorless decoy phase-encoding BB84-QKD and PM-QKD were analyzed above. One straightforward countermeasure that we can think of is to lock nonlocal lasers by abandoning the optical injection locking. However, the optical injection locking is feasible and straightforward, which can significantly reduce the complexity of the experiment, so we still advocate using it while ensuring safety.

The other straightforward countermeasure that we can think of is to add more isolation at the end of the source side to block Eve's injection. Previous papers showed that the external isolator can be damaged by an ultrastrong light attack, and the degree of isolation is effectively reduced [48]. As a solution, not only do we need to add the external isolator at the end of the source side, but we can also install an opposite-intensity monitoring device to detect whether strong optical injection damages the external isolator. Meanwhile, a high-precision optical spectrum analyzer is required to monitor other frequencies of optical injection locking.

Indeed, the most effective countermeasure is to strictly control the pulse period of the laser, so that it cannot match the time interval between the laser and IM.

## VI. CONCLUSIONS

Optical injection locking is a simple way to lock nonlocal lasers, but it may bring security risks. Reasonable countermeasures are needed to ensure security. In this paper, from the principle of optical injection locking, we first introduced the effects of different injection intensities on the source frequency. Then we found that the successive responses of adjacent pulses can distinguish the signal state from the decoy state of the preceding pulse. Finally, the optical injection-locking loophole was used to carry out a PNS attack on isolatorless decoy phase-encoding BB84-QKD and PM-QKD. One issue to note is that when the injection strength is not large enough, the slave laser will be unlocked and exhibit nonlinear characteristics; the phase of the emitted pulses can be modified to scramble the interference at the receiver. The optical injection unlocking has no effect on BB84-QKD because the randomized phase of the BB84-QKD protocol is the global phase, but it will increase the QBER on PM-QKD.

Simulation results showed that, if we maintain the same observed gain statistics as normal after an external optical injection locking, the loophole cannot be exploited at a short distance. Increasing the distance of the QKD, the optical injection-locking loophole does not threaten the security at a medium distance, and the security is still valid. At a long distance, the lower-bound secure key rate is higher than the upper-bound secure key rate given by our PNS attack because the lower bound represents the key rate at which Alice and Bob generate a key that they think is secure; then some of the keys must be insecure, and Eve will steal some keys from them. Further research showed that with the increase of the average photon number, the probability of successive responses of adjacent pulses will increase, and the secure key distance will become shorter and shorter.

## ACKNOWLEDGMENTS

This work is supported by the National Key Research and Development Program of China (Grants No. 2020YFA0309702 and No. 2020YFA0309701), the National Natural Science Foundation of China (Grants No. 62101597, No. 61605248, No. 61675235, and No. 61505261), the China Postdoctoral Science Foundation (Grant No. 2021M691536), the Natural Science Foundation of Henan (Grants No. 202300410534 and No. 202300410532), and the Anhui Initiative in Quantum Information Technologies.

## APPENDIX A: DYNAMICS OF THE SEMICONDUCTOR LASER WITH OPTICAL INJECTION LOCKING

Based on the well-known Lang-Kobayashi rate equations, we simulate the dynamics of the semiconductor laser with a single optical injection [49]:

$$\frac{dE(t)}{dt} = \frac{1}{2}(1+i\alpha)\left[\frac{g(N(t)-N_0)}{1+\varepsilon|E(t)|^2} - \frac{1}{\tau_p}\right]E(t) + k_{\mathrm{M}}E_{\mathrm{M}}(t)e^{-i2\pi(f_2\tau_{\mathrm{M}}-\Delta f t)}, \tag{A1a}$$

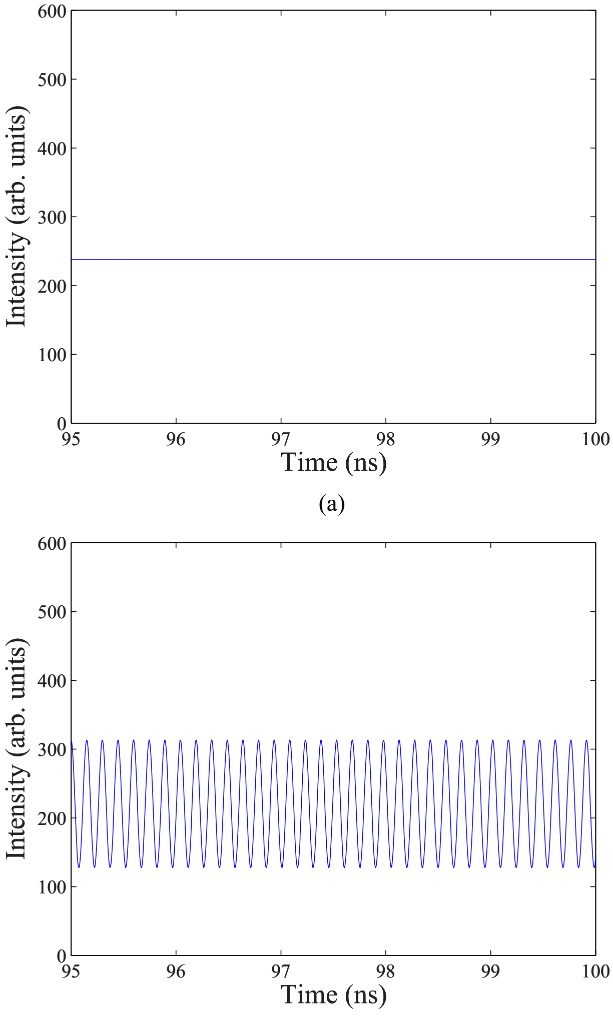
$$\frac{dN(t)}{dt} = j_0 J_{th} - \frac{N(t)}{\tau_N} - \frac{g(N(t)-N_0)}{1+\varepsilon|E(t)|^2}|E(t)|^2, \tag{A1b}$$

TABLE III. Parameters of the semiconductor laser used in the simulation.

| Parameter | Symbol | Value |
|---|---|---|
| Linewidth enhancement factor | $\alpha$ | 4.5 |
| Gain saturation coefficient | $\varepsilon$ | $1 \times 10^{-7}$ |
| Differential gain coefficient | $g$ | $8.4 \times 10^4/\mathrm{s}^{-1}$ |
| Carrier density at transparency | $N_0$ | $1.25 \times 10^8\ \mathrm{m}^3$ |
| Photon lifetime | $\tau_p$ | 1.927/ps |
| Carrier lifetime | $\tau_N$ | 2.04/ns |
| Optical frequency offset | $\Delta f$ | 5/GHz |
| Normalized injection current | $j_0$ | 1.44 |
| Injection current at threshold | $J_{th}$ | $9.892 \times 10^{32}\ \mathrm{m}^{-3}\ \mathrm{s}^{-2}$ |

where $E(t)$ and $E_{\mathrm{M}}(t)$ are the slowly varying electric field amplitudes of the slave laser and the master laser, $N(t)$ is the carrier density, and $k_{\mathrm{M}}$ is the injection strength.

The typical simulation parameters are listed in Table III. As shown in Fig. 7, when the injection strength of the master laser is large enough, the slave laser will be locked, a steady



(a)

(b)

FIG. 7. Intensity time series of optical injection locking. (a) $k_{\mathrm{M}} = 90$ GHz and (b) $k_{\mathrm{M}} = 40$ GHz.

intensity will be generated, and so is the phase. Otherwise, the slave laser will be unlocked, the intensity exhibits nonlinear periodic states and even more complex nonlinear chaotic states, and the phase also exhibits nonlinear characteristics.

The relaxation oscillation frequency of a solitary semiconductor laser can be calculated by the following equation [50]:

$$f_r = \frac{1}{2\pi}\sqrt{gJ_{\rm th}(j_0 - 1)}. \tag{A2}$$

So we can adjust the relaxation oscillation frequency by changing the injection current.

## APPENDIX B: PHOTON-NUMBER-SPLITTING ATTACK AND KEY-RATE UPPER BOUND

The gains $Q_\mu$ and $Q_v$ are the probabilities that the receiver obtains the detection event when the transmitter sends the signal state and the decoy state:

$$Q_\mu = \sum_{j=1}^{\infty} Y_j^s P_j^s, \tag{B1a}$$

$$Q_v = \sum_{j=1}^{\infty} Y_j^d P_j^d, \tag{B1b}$$

where $Y_j^s$ ($Y_j^d$) is the yield of the signal state (decoy state) and $P_j^s = e^{-\mu}\frac{\mu^j}{j!}$ ($P_j^d = e^{-v}\frac{v^j}{j!}$) is the probability following the Poisson distribution.

Meanwhile, the core assumption of the decoy state is

$$Y_j^s = Y_j^d, \tag{B2a}$$

$$E_j^s = E_j^d. \tag{B2b}$$

In our attack strategy, after making a partial distinction between the signal state and decoy state, Eqs. (B2a) and (B2b) are violated. Eve can choose $Y_j^s$ and $Y_j^d$ smartly by performing a PNS attack, with the aim of maintaining $Q_\mu$ and $Q_v$ as in the normal channel.

For a normal channel, Alice and Bob can get

$$Q_\mu = 1 - e^{-\eta\mu}, \tag{B3a}$$

$$Q_v = 1 - e^{-\eta v}, \tag{B3b}$$

where $\eta$ is the given overall efficiency between Alice and Bob.

Under a PNS attack, the yields $Y^\mu_{j\_{\rm PNS}}$ and $Y^v_{j\_{\rm PNS}}$ can be given by

$$Y^\mu_{j\_{\rm PNS}} = \varsigma_{\mu r} Z_j^\mu + \varsigma_{vw} Z_j^v, \tag{B4a}$$

$$Y^v_{j\_{\rm PNS}} = \varsigma_{vr} Z_j^v + \varsigma_{\mu w} Z_j^\mu, \tag{B4b}$$

where $Z_j^\mu$ ($Z_j^v$) is the best optimum single-photon yield of the signal state (decoy state) sent to the receiver. When Eve gets a vacuum state, $Z_0^\mu$ ($Z_0^v$) is set to zero to avoid errors. $\varsigma_{\mu r}$ ($\varsigma_{\mu w}$) is the probability of correctly judging (misjudging) the signal state of the $i$th pulse when both the $i$th pulse and the $(i+1)$th pulse have photon responses, and $\varsigma_{vr}$ ($\varsigma_{vw}$) is the probability of correctly judging (misjudging) the decoy state of the $i$th pulse when both the $i$th pulse and the $(i+1)$th pulse have photon responses; therefore, $\varsigma_{\mu r} = \frac{P_{f_1|\mu}}{P_{f_1|\mu}+P_{f_1|v}}$, $\varsigma_{vw} = \frac{P_{f_1|v}}{P_{f_1|\mu}+P_{f_1|v}}$, $\varsigma_{vr} = \frac{P_{f_2|v}}{P_{f_2|\mu}+P_{f_2|v}}$, and $\varsigma_{\mu w} = \frac{P_{f_2|\mu}}{P_{f_2|\mu}+P_{f_2|v}}$. $P_{f_1|\mu}$ ($P_{f_1|v}$) is the probability from port 1 when the $i$th pulse is the signal state (decoy state) and when both the $i$th pulse and the $(i+1)$th pulse have photon responses. $P_{f_2|\mu}$ ($P_{f_2|v}$) is the probability from port 2 when the $i$th pulse is the signal state (decoy state) and when both the $i$th pulse and the $(i+1)$th pulse have photon responses. $P_{f_1|\mu}$, $P_{f_1|v}$, $P_{f_2|\mu}$, and $P_{f_2|v}$ can be directly obtained from Tables I and II.

Then the gains of the signal state and decoy state under a PNS attack are given by

$$Q_{\mu\_{\rm PNS}} = \sum_{j=1}^{\infty} \left(\varsigma_{\mu r} Z_j^\mu + \varsigma_{vw} Z_j^v\right) e^{-\mu}\frac{\mu^j}{j!}, \tag{B5a}$$

$$Q_{v\_{\rm PNS}} = \sum_{j=1}^{\infty} \left(\varsigma_{vr} Z_j^v + \varsigma_{\mu w} Z_j^\mu\right) e^{-v}\frac{v^j}{j!}. \tag{B5b}$$

Since the secure key comes from only the single-photon component, Eve aims to make the upper bound of the secure key rate of the signal state as small as possible, $R_{\rm E}^\mu = Z_1^s e^{-\mu}\mu = (\varsigma_{\mu r} Z_1^\mu + \varsigma_{vw} Z_1^v) e^{-\mu}\mu$. For BB84-QKD, $Z_1^s$ is the best optimum single-photon yield of the signal state sent to Bob. For PM-QKD, $Z_1^s$ is the best optimum single-photon yield of the signal state sent to Charlie by Alice and Bob.

Therefore, under the premise that the detection statistics on the receiver's side are not disturbed, as described above, Eve should optimize $Z_j^\mu$ and $Z_j^v$ to minimize the upper bound of the secure key rate. All these optimum $Z_j^\mu$ and $Z_j^v$ are in the regime [0,1] and are not related to the quantities in Tables I and II, except for the condition that Eqs. (B3a) and (B3b) and (B5a) and (B5b) must be equal.

## APPENDIX C: ATTACK ERROR STATISTICS ANALYSIS

Here, we analyze in detail the more rigorous results when Eve strictly maintains the gain statistics and the error statistics simultaneously. Further considering the QBER, the following equations need to be satisfied for BB84-QKD:

$$E_\mu Q_\mu \geqslant 0.5 Z_0^\mu + \sum_{j=1}^{\infty} 0.5 \varsigma_{vw} Z_j^v e^{-\mu}\frac{\mu^j}{j!}, \tag{C1a}$$

$$E_v Q_v \geqslant 0.5 Z_0^v + \sum_{j=1}^{\infty} 0.5 \varsigma_{\mu w} Z_j^\mu e^{-v}\frac{v^j}{j!}. \tag{C1b}$$

The QBER is set to the maximum value of 0.5 when we misjudge the signal state or decoy state of the preceding pulse.

For PM-QKD, QBER is inevitably increased due to the phase confusion, since the weak optical injection affects the phase. We need to add one more term to the formula above:

$$E_\mu Q_\mu \geqslant 0.5 Z_0^\mu + \sum_{j=1}^{\infty} 0.5 \varsigma_{vw} Z_j^v e^{-\mu}\frac{\mu^j}{j!} + \sum_{j=1}^{\infty} 0.5 P_d (1 - \xi_{f_2|I_2}) Z_j^\mu e^{-\mu}\frac{\mu^j}{j!}, \tag{C2a}$$

$$E_vQ_v \geqslant 0.5Z_0^v + \sum_{j=1}^{\infty} 0.5\varsigma_{\mu w} Z_j^{\mu} e^{-v}\frac{v^j}{j!} + \sum_{j=1}^{\infty} 0.5P_d(1-\xi_{f_2|I_2})Z_j^{v} e^{-v}\frac{v^j}{j!}, \tag{C2b}$$

where $P_d = 10\%$ is the proportion of the decoy state.

When the $(i-1)$th pulse is a decoy state, the subsequent measured responses are all regarded as errors; regardless of whether the correct judgment or a misjudgment is made, the QBER is set as $0.5P_d(1-\xi_{f_2|I_2})$. The reason is that the phase after a decoy state will be randomized, which does not meet the condition of phase locking.

[1] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[2] R. Renner, N. Gisin, and B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Phys. Rev. A **72**, 012332 (2005).

[3] Y. Liu, T. Y. Chen, L. J. Wang, H. Liang, G. L. Shentu, J. Wang, K. Cui, H. L. Yin, N. L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C. Z. Peng, Q. Zhang, and J. W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[4] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett. **85**, 1330 (2000).

[5] 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).

[6] 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).

[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[8] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[9] S. Sun and F. Xu, Security of quantum key distribution with source and detection imperfections, New J. Phys. **23**, 023011 (2021).

[10] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, After-gate attack on a quantum cryptosystem, New J. Phys. **13**, 013043 (2011).

[11] V. Makarov, Controlling passively quenched single photon detectors by bright light, New J. Phys. **11**, 065003 (2009).

[12] 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).

[13] V. Makarov and D. R. Hjelme, Faked states attack on quantum cryptosystems, J. Mod. Opt. **52**, 691 (2005).

[14] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[15] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[16] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).

[17] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[18] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[19] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw, Phys. Rev. A **85**, 042307 (2012).

[20] G.-J. Fan-Yuan, F.-Y. Lu, S. Wang, Z.-Q. Yin, D.-Y. He, Z. Zhou, J. Teng, W. Chen, G.-C. Guo, and Z.-F. Han, Measurement-device-independent quantum key distribution for nonstandalone networks, Photonics Res. **9**, 1881 (2021).

[21] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[22] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[23] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[24] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[25] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[26] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum Key Distribution without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[27] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[28] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[29] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[30] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).

[31] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field

Quantum Key Distribution through Sending or Not Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[32] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L.-X. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[33] H. Liu *et al.*, Field Test of Twin-Field Quantum Key Distribution through Sending-or-Not-Sending over 428 km, Phys. Rev. Lett. **126**, 250502 (2021).

[34] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).

[35] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics **15**, 570 (2021).

[36] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution, Phys. Rev. Lett. **123**, 100506 (2019).

[37] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses, npj Quantum Inf. **7**, 8 (2021).

[38] A. Vakhitov, V. Makarov, and D. R. Hjelme, Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography, J. Mod. Opt. **48**, 2023 (2001).

[39] 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).

[40] 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).

[41] E. K. Lau, L. J. Wong, and M. C. Wu, Enhanced modulation characteristics of optical injection-locked lasers: A tutorial, IEEE J. Sel. Top. Quantum Electron. **15**, 618 (2009).

[42] A. Gavrielides, V. Kovanis, and T. Erneux, Analytical stability boundaries for a semiconductor laser subject to optical injection, Opt. Commun. **136**, 253 (1997).

[43] A. Murakami, K. Kawashima, and K. Atsuki, Cavity resonance shift and bandwidth enhancement in semiconductor lasers with strong light injection, IEEE J. Quantum Electron. **39**, 1196 (2003).

[44] Z. L. Yuan, B. Fröhlich, M. Lucamarini, G. L. Roberts, J. F. Dynes, and A. J. Shields, Directly Phase-Modulated Light Source, Phys. Rev. X **6**, 031044 (2016).

[45] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, A direct GHz-clocked phase and intensity modulated transmitter applied to quantum key distribution, Quantum Sci. Technol. **3**, 045010 (2018).

[46] Y.-L. Tang, H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[47] P. Zeng, W. Wu, and X. Ma, Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound Over a Noisy Channel, Phys. Rev. Appl. **13**, 064013 (2020).

[48] 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).

[49] R. Lang and K. Kobayashi, External optical feedback effects on semiconductor injection laser properties, IEEE J. Quantum Electron. **16**, 347 (1980).

[50] T. Wu, W. Sun, X. Zhang, and S. Zhang, Concealment of time delay signature of chaotic output in a slave semiconductor laser with chaos laser injection, Opt. Commun. **381**, 174 (2016).