Laser-Seeding Attack in Quantum Key Distribution

Anqi Huang,[1,2,*] Álvaro Navarrete,[3] Shi-Hai Sun,[4] Poompong Chaiwongkhot,[2,5] Marcos Curty,[3] and Vadim Makarov[6,7,8,5]

[1] *Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China*
[2] *Institute for Quantum Computing, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*
[3] *EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
[4] *School of Physics and Astronomy, Sun Yat-Sen University, Zhuhai 519082, People's Republic of China*
[5] *Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1*
[6] *Russian Quantum Center, Skolkovo, Moscow 121205, Russia*
[7] *Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*
[8] *NTI Center for Quantum Communications, National University of Science and Technology MISiS, Moscow 119049, Russia*

(Received 13 May 2019; revised manuscript received 5 November 2019; published 18 December 2019; corrected 25 February 2020)

Quantum key distribution (QKD) based on the laws of quantum physics allows the secure distribution of secret keys over an insecure channel. Unfortunately, imperfect implementations of QKD compromise its information-theoretical security. Measurement-device-independent quantum key distribution (MDI QKD) is a promising approach to remove all side channels from the measurement unit, which is regarded as the "Achilles' heel" of QKD. An essential assumption in MDI QKD is, however, that the sources are trusted. Here we experimentally demonstrate that a practical source based on a semiconductor laser diode is vulnerable to a laser-seeding attack, in which light injected from the communication line into the laser results in an increase of the intensities of the prepared states. The unnoticed increase of intensity may compromise the security of QKD, as we show theoretically for the prepare-and-measure decoy-state BB84 and MDI QKD protocols. Our theoretical security analysis is general and can be applied to any vulnerability that increases the intensity of the emitted pulses. Moreover, a laser-seeding attack might be launched as well against decoy-state-based quantum cryptographic protocols beyond QKD.

DOI: 10.1103/PhysRevApplied.12.064043

I. INTRODUCTION

The distribution of a secret key between two authorized parties, Alice and Bob, is a fundamental but challenging cryptographic task. Such a secret key is the essential resource of the one-time-pad algorithm [1], the only known encryption method that can offer unconditionally secure communications. Public key cryptography solves this problem by resorting to computational assumptions, for instance, the difficulty of factoring large numbers [2]. This approach is, however, vulnerable to technological advances in both hardware and software; indeed, it is well known that factoring is an easy problem on a quantum computer [3]. Quantum key distribution (QKD), on the other hand, provides a solution based on the laws of quantum physics, and thus, in theory, it can guarantee that the distributed keys are information-theoretically secure [4–6].

There is, however, a big gap between the theory and the practice of QKD because the behavior of real QKD devices typically deviates from that considered in the security proofs. Such a deviation could be exploited by an eavesdropper, Eve, to obtain information about the secret key without being detected in QKD implementations [7–27]. Most of the quantum hacking attacks realized so far exploit imperfections of the single-photon detectors (SPDs)—the "Achilles' heel" of QKD [7–15,18–20,22]. Indeed, in recent years there has been an enormous effort to try to close the detectors' security loopholes and restore the security of QKD realizations. Some solutions are based on hardware and software patches [28,29], whose drawback is, however, that each patch typically protects only against a specific loophole, i.e., the system might still be vulnerable to unknown attacks. Moreover, patches might

[*] angelhuang.hn@gmail.com

also be hacked [20,22]. A safer and more elegant solution is that of measurement-device-independent QKD (MDI QKD) [30,31]. Remarkably, this latter approach guarantees security independently of the behavior of the measurement device, which can be treated as a “black box” fully controlled by Eve. This is achieved by turning Bob’s receiver into a transmitter by means of a time-reversed Einstein-Podolsky-Rosen (EPR) protocol [32,33]. MDI QKD has been successfully demonstrated in several recent experiments [34–39] including an implementation over 404 km [40].

With the advent of MDI QKD all security loopholes from the measurement unit are closed, so the focus is now on how to protect the QKD transmitters. For instance, decoy-state QKD [41–43] is a practical solution to defeat the photon-number-splitting attack [44,45]. More recently, several works have considered other imperfections of the transmitter, and security proofs that guarantee security in the presence of such imperfections have been developed [46–53]. For example, Refs. [48–50] quantify the optical isolation that is needed in order to achieve a certain performance (i.e., a certain secret key rate over a given distance) in the presence of a Trojan-horse attack (THA), in which Eve injects bright light into the transmitter and then analyzes the back-reflected light to obtain information about the quantum signals emitted. Finally, a type of light injection attack that affects the operation of the laser diode in the transmitter has recently been introduced, allowing Eve to actively derandomize the source’s phase and even change other parameters [54]. Indeed, the use of non-phase-randomized signals has a severe effect on the security of QKD, as has been shown in the past decade [55–58].

While the results above are promising, there is still a long way to go to be able to ensure the security of QKD implementations. For instance, a fundamental assumption of QKD is that the intensity of the quantum states prepared by Alice is set at a single-photon level. This assumption is indeed vital for a QKD system. However, no study has investigated whether or not Eve could increase the mean photon number of the prepared states. Here we introduce, and experimentally demonstrate, a quantum hacking attack, which we call a “laser-seeding attack,” which can increase and control the intensity of the light emitted by the laser diode in the transmitter of a QKD system. This attack has been confirmed experimentally for two types of laser diodes. Different from the THA that analyzes the back-reflected light that is originally from an external independent source, the laser-seeding attack manipulates the functioning of the transmitter’s laser diode directly. In other words, while in a THA Eve tries to correlate her signals with the quantum states prepared by the legitimate users of the system, in a laser-seeding attack the goal of Eve is to directly increase the intensity of such quantum states. Most importantly, this attack seriously compromises the security of decoy-state-based QKD, which includes MDI QKD with practical light sources as a prominent example. More precisely, in the presence of this attack, current security analyses overestimate the resulting secret key rate and thus they do not guarantee security.

II. EXPERIMENTAL SETUP

To investigate to which extent Eve can increase the output optical power of a laser diode by injecting light into it, we conduct an experiment whose schematic is illustrated in Fig. 1. On Alice’s side, the laser diode, as a testing target, generates optical pulses. As a hacker, Eve employs a tunable laser (Agilent 8164B) to send cw bright light to Alice’s laser diode via a single-mode optical fiber. The tunable laser is able to adjust the wavelength and output power of the signals emitted so that Eve can inject photons with a proper wavelength into Alice’s laser. In so doing, the energy of each injected photon can match the energy difference between the excited state and the ground state of the laser, and thus satisfy the condition for stimulated emission.

In order to maximize the injection efficiency, a polarization controller is used to adjust the polarization of Eve’s laser such that it matches that of Alice’s laser. To separate Eve’s injected light from that emitted by Alice, we employ an optical circulator. Eve’s light enters port 1 of the circulator and exits through its port 2, while Alice’s light goes from port 2 of the circulator to its port 3 (see Fig. 1). We record Alice’s output pulses with an optical-to-electrical converter with 40-GHz bandwidth (Picometrix PT-40A) that is connected to a high-speed oscilloscope (Agilent DSOX93304Q) of 33-GHz bandwidth. The average pulse energy is then calculated by integrating the recorded averaged waveform. A cross-check using an optical power meter has confirmed that this method is accurate. We observe the energy of Alice’s laser pulses with and without Eve’s tampering laser. We test two ID300 short-pulse laser sources from ID Quantique and one LP1550-SAD2 laser diode (LD) from Thorlabs. They are triggered by an external signal. ID300 contains a factory preset pulsed

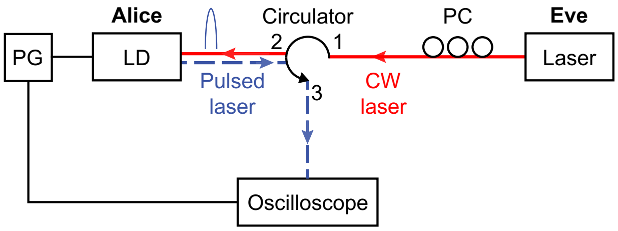

FIG. 1. Experimental setup. The red solid arrows represent Eve’s injected cw bright light, and the blue dashed arrows indicate the optical pulses emitted by Alice’s laser diode. PG, electronic pulse generator; LD, laser diode; PC, polarization controller.

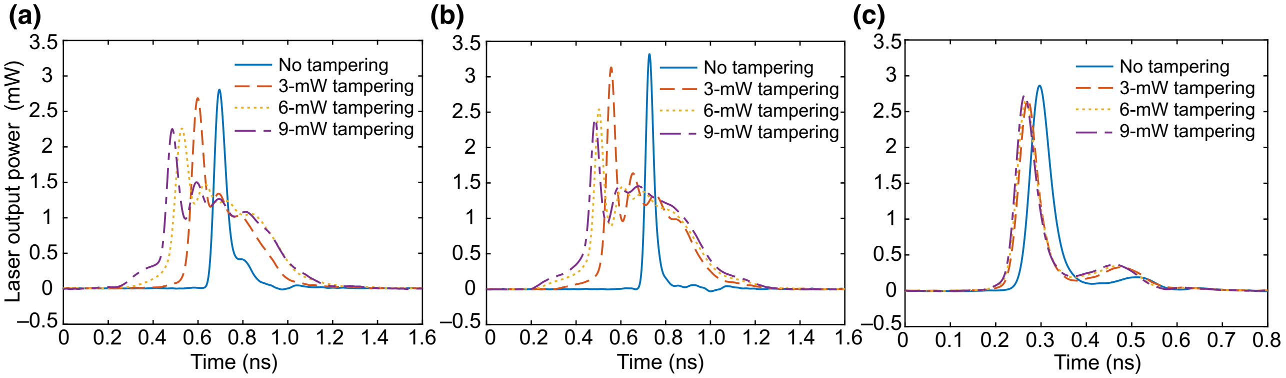

FIG. 2. Averaged waveforms of laser pulses measured from (a) ID300 sample 1, (b) ID300 sample 2, and (c) the laser diode LP1550-SAD2 from Thorlabs. Each oscillogram is an average over 2000 pulses.

driver electronics and produces 50–70-ps FWHM optical pulses, with their repetition rate controlled by our external electronic pulse generator (PG; Picosecond 12050). LP1550-SAD2's diode current is driven directly from the PG with pulse parameters set to obtain about 60-ps FWHM optical pulses from the LD. The pulse repetition rate for all samples is 1 MHz. The electronic pulse generator also acts as the external trigger of the oscilloscope as shown in Fig. 1.

III. EXPERIMENTAL RESULTS

Both samples of ID300 exhibit controllability of their output power by Eve. We first measure the center wavelength of each laser with a spectrum analyzer (Yokogawa AQ6370D). Then, in the experimental setup shown in Fig. 1, we dial the value of Alice's wavelength in Eve's laser. As a result, the output power of Alice's pulse suddenly increases. To obtain the maximum output power under Eve's control, we finely tune Eve's wavelength until the largest energy rise is observed, which is 1550.15 nm for sample 1 and 1550.44 nm for sample 2. This is the case we focus on. Additionally, we note that slightly different seed wavelengths result in different pulse shapes as shown in Appendix A.

When we gradually increase the power of Eve's cw laser, the energy of Alice's emitted pulses also increases. This is shown in Figs. 2(a) and 2(b), which illustrates the waveforms of Alice's pulses for various tampering light powers. If we compare these results with the original waveform of Alice's pulses (i.e., that in the absence of Eve's tampering laser), there are two main effects. First, as already mentioned, we see that the energy of the emitted optical pulses gets larger when we increase the tampering light power. In particular, Eve's injected light makes Alice's laser pulses wider with a much longer and higher tail as shown in Figs. 2(a) and 2(b). The tail contains more energy when higher power is injected into the diode. Second, under the laser-seeding attack, the main peak of Alice's pulse shifts to be earlier. This is because the injected light triggers the stimulated emission that happens quicker than the spontaneous emission in Alice's laser diode. Thus, Alice's pulse reaches the peak power earlier and is followed by a tail with two–four secondary oscillations under the attack.

We measure the energy of Alice's pulses for different tampering light powers. The results are shown in Fig. 3 as black curves. In particular, we find that when there is no attack, this energy is 0.232 pJ (0.169 pJ) for sample 1 (2). Then, we gradually increase the power of Eve's cw laser up to 9 mW, and obtain that the output energy of Alice's laser rises up to 0.712 pJ (0.773 pJ) for sample 1 (2). In other words, the pulse energy increases 3.07 (4.57) times for sample 1 (2).

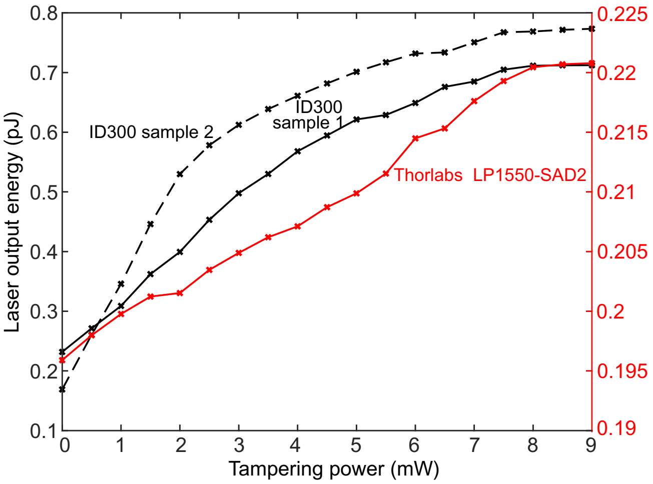

FIG. 3. Average energy of Alice's output pulses as a function of Eve's tampering power for two samples of the laser ID300 from ID Quantique (black curves) and the laser diode LP1550-SAD2 from Thorlabs (red curve). The energy of the pulse increases up to 3.07 times for ID300 sample 1, 4.57 times for ID300 sample 2, and 1.13 times for Thorlabs LP1550-SAD2.

Under the same experimental procedure done with ID300, a similar effect is observed in the laser LP1550-SAD2. The wavelength of the injected cw light is set to the center wavelength of the laser diode first, then tuned slightly to 1551.32 nm where we observe the maximum increase in Alice's pulse energy. Figure 2(c) shows the waveforms of Alice's pulses for the same tampering light powers as those in Figs. 2(a) and 2(b). Similarly to ID300 lasers, here the energy of the pulses increases with the tampering power as well. The rising edge of Alice's pulse also starts earlier in the presence of the attack. The increase of the pulse energy as a function of Eve's tampering power is shown in Fig. 3 as a red curve. If there is no attack, the average energy of Alice's laser pulses is 0.196 pJ, while it reaches 0.221 pJ when the tampering power is 9 mW. In other words, in this case the pulse energy increases 1.13 times.

We note that the commercial lasers under test in our experiment (ID300 and LP1550-SAD2) contain an internal optical isolator of the order of 30–40 dB. Thus, a few mW light that is applied in our experiment is first attenuated at the internal isolator of the laser, which means that only about 100-nW power actually reaches the laser cavity. This analysis indicates that an injection power in the order of 100 nW could be enough to control the intensity of Alice's pulses. Indeed, this value of injection power has been also confirmed recently by the experimental results shown in Ref. [59], in which Eve's injection power is in the 100–160 nW range. We also note that a real QKD system may use a laser diode without the internal isolator, then the injection power used in our laser-seeding attack may be reduced to the above level.

IV. EFFECT ON THE SECURITY OF QKD

Now we show theoretically how an unnoticed increase of the optical power emitted by a QKD transmitter, due to the attack described above, could seriously compromise the security of a QKD implementation. We assume that Alice's photon-number statistics is Poissonian and is not influenced by our attack. The former may not necessarily be the case [60], and investigating the validity of the latter assumption could be the topic of a future study. Based on this assumption, we shall consider the case of decoy-state-based QKD [41–43], which includes the most implemented QKD schemes today. We refer the reader to Appendix B for further details about decoy-state based QKD. For simplicity, in our analysis we assume the asymptotic scenario where Alice sends Bob an infinite number of pulses, i.e., we disregard statistical fluctuations due to finite size effects. Also, motivated by the experimental results presented in the previous section, we shall consider that Eve's attack increases all the intensities μ by the same factor $\kappa > 1$. That is, we assume that $\mu' = \kappa\mu$ for all μ.

Next, we quantitatively evaluate the effect that a laser-seeding attack has on the security of the standard decoy-state BB84 protocol and of MDI QKD for a typical channel model. For concreteness, we consider first the case of the standard decoy-state BB84 protocol with phase-randomized weak coherent pulses (WCPs); afterwards, we consider the case of MDI QKD.

A. Standard decoy-state BB84 protocol

Regarding the standard decoy-state BB84 protocol, we evaluate the typical implementation where Alice and Bob use three different intensities, μ_s, ν_1, and ν_2 that satisfy $\mu_s > \nu_1 > \nu_2$, and they generate a secret key only from those events where they employ the signal intensity μ_s in the Z basis, while they use the X-basis events for parameter estimation. In the asymptotic limit of an infinite number of transmitted signals, the secret key rate can be lower bounded by [61,62]

$$R_L = p_1^{\mu_s} Y_{1,L}^{Z}[1 - H_2(e_{1,U}^{X})] - f_e G_Z^{\mu_s} H_2(E_Z^{\mu_s}), \tag{1}$$

where we assume the efficient version of this protocol [63]. In Eq. (1), $Y_{1,L}^Z$ ($e_{1,U}^X$) denotes a lower (upper) bound on the single-photon yield Y_1^Z (phase error rate e_1^X), the parameter f_e is the error correction efficiency, $G_Z^{\mu_s}$ ($E_Z^{\mu_s}$) represents the overall experimentally observed gain (the overall experimentally observed QBER) when Alice sends to Bob a WCP of intensity μ_s in the Z basis, and $H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

To estimate $Y_{1,L}^Z$ and $e_{1,U}^X$ one can use analytical or numerical tools. Here we use the analytical method proposed in Ref. [61]. In particular, we have that

$$Y_{1,L}^{Z} \geq \frac{\mu_s}{\mu_s(\nu_1 - \nu_2) - \nu_1^2 + \nu_2^2} \times \left[G_Z^{\nu_1} e^{\nu_1} - G_Z^{\nu_2} e^{\nu_2} - \frac{\nu_1^2 - \nu_2^2}{\mu_s^2}(G_Z^{\mu_s} e^{\mu_s} - Y_{0,L}^{Z}) \right], \tag{2}$$

$$e_{1,U}^{X} \leq \frac{E_X^{\nu_1} G_X^{\nu_1} e^{\nu_1} - E_X^{\nu_2} G_X^{\nu_2} e^{\nu_2}}{(\nu_1 - \nu_2) Y_{1,L}^{X}}, \tag{3}$$

with $Y_{0,L}^Z$ being a lower bound on Y_0^Z given by

$$Y_{0,L}^{Z} \geq \frac{\nu_1 G_Z^{\nu_2} e^{\nu_2} - \nu_2 G_Z^{\nu_1} e^{\nu_1}}{\nu_1 - \nu_2}, \tag{4}$$

and where the parameter $Y_{1,L}^X$ represents a lower bound on Y_1^X. This last quantity can be obtained by using Eq. (2) but now referred to the X basis.

In the presence of a laser-seeding attack, Alice and Bob estimate $Y_{1,L}^Z$ and $e_{1,U}^X$ using Eqs. (2) and (3) but now with

TABLE I. Experimental parameters used in the simulations. The background rate and detection efficiency of the SPDs are taken from Ref. [38].

Channel loss coefficient (dB/km)	α	0.2
Background rate	Y_0	2.6×10^{-5}
Total misalignment error	e_d	1.5%
Detection efficiency of the SPDs	η_D	30%
Error correction efficiency	f_e	1.12

the experimentally observed quantities $G_\alpha^{\mu'}$ and $E_\alpha^{\mu'}$, with $\alpha \in \{Z, X\}$, $\mu' = \kappa\mu$ and $\mu \in \{\mu_s, \nu_1, \nu_2\}$ for a certain κ that depends on the attack.

In our analysis we also evaluate an ultimate upper bound on the secret key rate. More precisely, this upper bound holds for any possible postprocessing method that Alice and Bob could apply to their raw data. The only assumption here is that double-click events are randomly assigned to single-click events. For this, we use the technique introduced in Ref. [64]. More precisely, the upper bound on the key rate is given by

$$R_U \leq \sum_{n\geq 1} r_n (1 - \lambda_{\mathrm{BSA}}^n) I_n^{\mathrm{ent}}(A;B), \tag{5}$$

where $r_n \approx e^{-\mu_s}\mu_s^n/n!$ is the probability that Alice sends Bob an n-photon state with the signal intensity, λ_{BSA}^n is the maximum weight of separability among all the bipartite quantum states σ_{AB}^n that are compatible with Alice and Bob's observables, and $I_n^{\mathrm{ent}}(A;B)$ is the Shannon mutual information evaluated on the entanglement part of the state σ_{AB}^n that has the maximum weight of separability. See Ref. [64] and Appendix C for further details.

For simulation purposes we use the experimental parameters listed in Table I. The resulting lower and upper bounds on the secret key rate are shown in Fig. 4. The blue dotted line represents the lower bound R_L given by Eq. (1) in the absence of the attack. Here, for each given value of the distance, we select the optimal values of the intensities μ_s, ν_1, and ν_2 that maximize R_L. These optimized intensities are then fixed, and we use them to simulate the degradation of the security bounds due to Eve's laser-seeding attack.

More precisely, the red solid line in Fig. 4 shows the value of R_L that Alice and Bob would estimate in the presence of the attack when $\kappa = 2$. In other words, as explained above, here Alice and Bob estimate the parameters $Y_{1,L}^Z$ and $e_{1,U}^X$ with the observed quantities $G_\alpha^{\mu'}$ and $E_\alpha^{\mu'}$, with $\alpha \in \{Z, X\}$, $\mu' = \kappa\mu$, and $\mu \in \{\mu_s, \nu_1, \nu_2\}$, together with the original intensities μ_s, ν_1, and ν_2. The red dash-dotted line, on the other hand, illustrates the correct secure value of R_L in the presence of the attack. In other words, here $Y_{1,L}^Z$ and $e_{1,U}^X$ are estimated with the observed quantities $G_\alpha^{\mu'}$ and $E_\alpha^{\mu'}$, with $\alpha \in \{Z, X\}$, $\mu' = \kappa\mu$, and $\mu \in \{\mu_s, \nu_1, \nu_2\}$, together with the modified intensities μ'.

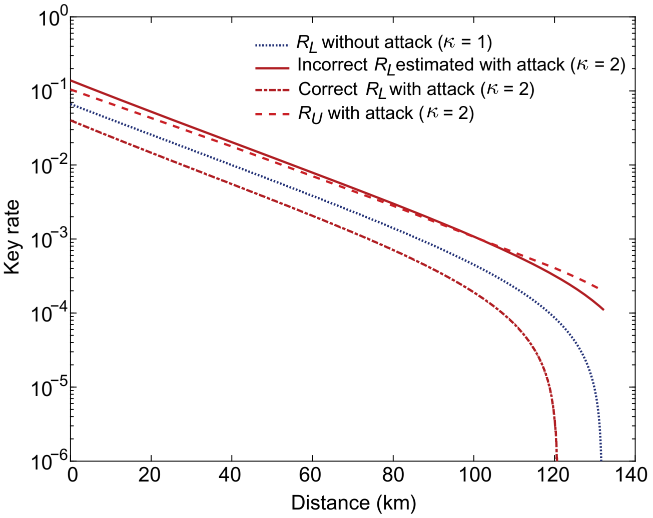

FIG. 4. Lower (R_L) and upper (R_U) bounds on the secret key rate as a function of the distance for the standard decoy-state BB84 protocol for two different values of the multiplicative factor $\kappa = \{1, 2\}$. The original intensity settings have been optimized previously for each distance. The parameters used in the simulations are given in Table I.

As we can see in Fig. 4, the secure R_L given by the red dash-dotted line is significantly below the R_L actually estimated by Alice and Bob. More precisely, in the presence of the attack, the security proof introduced in Refs. [61,62] cannot guarantee the security of the secret key obtained by Alice and Bob. Finally, the red dashed line illustrates the upper bound R_U given by Eq. (5) in the presence of the attack. Remarkably, this upper bound is below the R_L estimated by Alice and Bob for most of the distances, which demonstrates that the estimated secret key rate is actually insecure no matter what security proof is used.

Finally, in Fig. 5 we show the effect that the multiplicative factor κ has on the bounds on the secret key rate. For this, we now fix the transmission distance at a certain value, say 40 km. In this case, Fig. 5 shows that the incorrect lower bound R_L that Alice and Bob would estimate is always above its correct value whenever $\kappa > 1$. This is remarkable because it means that in the presence of a laser-seeding attack Alice and Bob always overestimate their secret key rate above that provided by the security proof. Moreover, if κ is large enough (around1.7 for the experimental parameters used in Fig. 5), it turns out that the upper bound R_U is below the estimated secret key rate, which confirms that there is no security proof, which can make the estimated secret key rate secure.

We remark that in practice Eve might need to throttle the key rate to roughly the original expected level in the absence of the attack. Indeed, a human operator of QKD

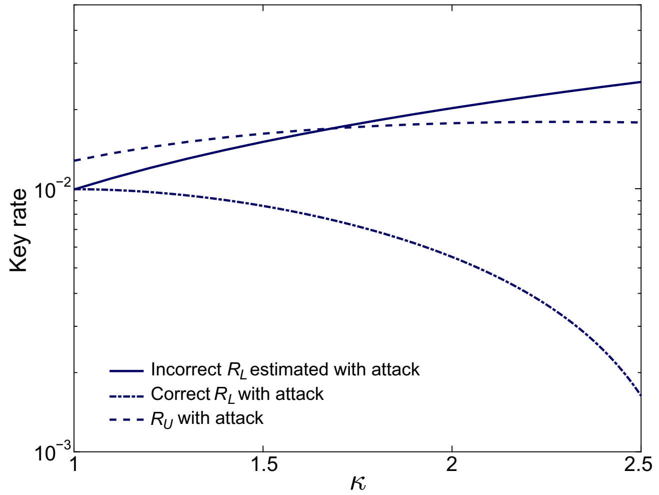

FIG. 5. Lower (R_L) and upper (R_U) bounds on the secret key rate as a function of the parameter κ for a fixed distance (40 km in this case), for decoy-state BB84 protocol. In these simulations, the original intensity settings have been optimized previously for the distance of 40 km assuming no attack. The parameters used in the simulations are given in Table I.

equipment may suspect something abnormal is happening if the key generation rate rises well above the expected level (blue dotted line in Fig. 4). To reduce the rate, Eve can simply introduce additional optical attenuation in the channel.

B. MDI QKD

Next we consider the case of MDI QKD with WCPs [30]. Similar to the previous example, we assume that each of Alice and Bob use three different intensities, μ_s, ν_1, and ν_2 that satisfy $\mu_s > \nu_1 > \nu_2$, and they generate the secret key from those events encoded with the signal intensity in the Z basis, while they use the X-basis events for parameter estimation. In the asymptotic limit of an infinite number of transmitted signals (and assuming for simplicity a sifting factor approximately equal to 1), the secret key rate is lower bounded by [30]

$$R_L = p_{11}^{\mu_s\mu_s} Y_{11,L}^{Z}[1 - H_2(e_{11,U}^{X})] - f_e G_Z^{\mu_s\mu_s} H_2(E_Z^{\mu_s\mu_s}), \quad (6)$$

where $p_{11}^{\mu_s\mu_s}$ is the probability that both Alice and Bob emit a single-photon pulse in the Z basis when they both use the signal intensity setting μ_s, $Y_{11,L}^{Z}$ is a lower bound on the yield associated to these single-photon events, $e_{11,U}^{X}$ is an upper bound on the phase error rate of these single-photon pulses, f_e is again the error correction efficiency, $G_Z^{\mu_s\mu_s}$ and $E_Z^{\mu_s\mu_s}$ are the gain and the QBER when both Alice and Bob send to the relay Charles WCPs of intensity μ_s in the Z basis, and $H_2(x)$ is the binary Shannon entropy function defined previously.

To evaluate Eq. (6), Alice and Bob need to calculate the parameters $Y_{11,L}^{Z}$ and $e_{11,U}^{X}$ based on the experimentally available data $G_\alpha^{\zeta\omega}$ and $E_\alpha^{\zeta\omega}$, with $\alpha \in \{Z, X\}$ and $\zeta, \omega \in \{\mu_s, \nu_1, \nu_2\}$, and their knowledge on the probability distribution $p_{nm}^{\zeta\omega}$ with $n, m \in \mathbb{N}$, where $\mathbb{N}$ is the set of the non-negative integers. Again, this estimation can be done analytically or numerically, and for simplicity here we use the analytical approach introduced in Ref. [65]. For completeness, below we include the expressions for $Y_{11,L}^{Z}$ and $e_{11,U}^{X}$:

$$\begin{aligned} Y_{11,L}^{Z} \geq{} & \frac{1}{(\mu_s - \nu_2)^2(\nu_1 - \nu_2)^2(\mu_s - \nu_1)^2} \\ & \times [(\mu_s^2 - \nu_2^2)(\mu_s - \nu_2)(G_Z^{\nu_1\nu_1} e^{2\nu_1} + G_Z^{\nu_2\nu_2} e^{2\nu_2} \\ & - G_Z^{\nu_1\nu_2} e^{\nu_1+\nu_2}) - (\nu_1^2 - \nu_2^2)(\nu_1 - \nu_2)(G_Z^{\mu_s\mu_s} e^{2\mu_s} \\ & + G_Z^{\nu_2\nu_2} e^{2\nu_2} - G_Z^{\mu_s\nu_2} e^{\mu_s+\nu_2} - G_Z^{\nu_2\mu_s} e^{\nu_2+\mu_s})], \quad (7) \end{aligned}$$

and

$$\begin{aligned} e_{11,U}^{X} \leq{} & \frac{1}{(\nu_1 - \nu_2)^2 Y_{11,L}^{X}} (e^{2\nu_1} G_X^{\nu_1\nu_1} E_X^{\nu_1\nu_1} + e^{2\nu_2} G_X^{\nu_2\nu_2} \\ & \times E_X^{\nu_2\nu_2} - e^{\nu_1+\nu_2} G_X^{\nu_1\nu_2} E_X^{\nu_1\nu_2} - e^{\nu_2+\nu_1} G_X^{\nu_2\nu_1} \\ & \times E_X^{\nu_2\nu_1}), \quad (8) \end{aligned}$$

where $Y_{11,L}^{X}$ represents a lower bound on the yield associated to those single-photon events emitted by Alice and Bob in the X basis. This last quantity can be estimated using Eq. (7) but now referred to the X basis.

To evaluate R_L in the presence of a laser-seeding attack we follow a methodology similar to that used in the previous subsection, and we omit it here for simplicity.

Also, to evaluate an upper bound R_U on the secret key rate, we extend the technique introduced in Ref. [64] to the case of MDI QKD. Here, for simplicity, we consider that Alice and Bob only distill the secret key from non-positive partial transposed entangled states [66,67], i.e., we disregard the key material, which could be obtained from positive partial transposed entangled states [68]. We refer the reader to Appendix D for further details about the upper bound R_U.

For simulation purposes, we use again the experimental parameters given in Table I. For simplicity, we assume that Eve performs a symmetric attack in which she injects light of the same intensity into both Alice's and Bob's transmitter devices, which moreover we assume are identical. The resulting lower and upper bounds on the secret key rate are shown in Fig. 6. For this example we consider three possible values for the multiplicative factor$\kappa = \{1, 1.5, 2.5\}$. The case $\kappa = 1$ corresponds to the scenario without attack. The results are analogous to those illustrated in Fig. 4. In particular, the incorrect value of R_L that Alice and Bob would estimate in the presence of the attack is well above

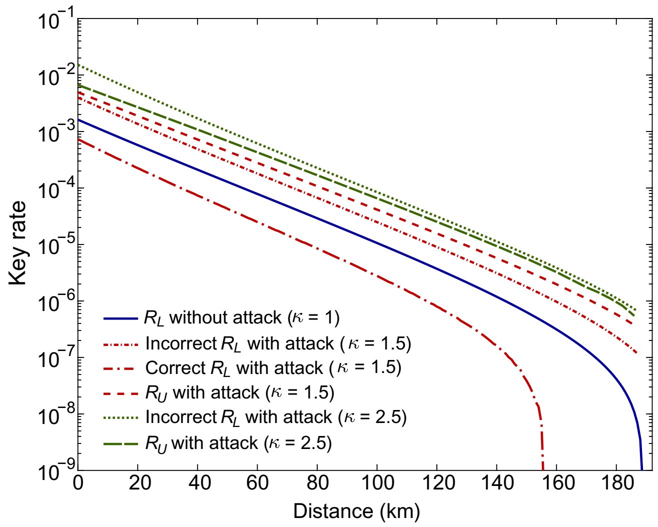

FIG. 6. Lower (R_L) and upper (R_U) bounds on the secret key rate as a function of the distance for MDI QKD with WCPs for three different values of the multiplicative factor $\kappa = \{1, 1.5, 2.5\}$. The correct value of R_L in the presence of the attack is zero when $\kappa = 2.5$. This shows that Alice and Bob significantly overestimate the secret key rate in the presence of the attack. The original intensity settings have been optimized previously for each distance for the case where there is no attack. The parameters used in the simulations are given in Table I.

the correct value of R_L delivered by a proper application of the security proof (i.e., for the case where one considers the correct values of the output intensities modified by the attack). This is particularly critical for the case where $\kappa = 2.5$, as the security proof provides no secure key rate in this scenario while Alice and Bob would incorrectly estimate a relatively high value for R_L. Also, in this case, the upper bound R_U is below the estimated R_L for all distances (see Fig. 6).

V. DISCUSSION AND COUNTERMEASURE

In this laser-seeding attack, the isolation present in a real QKD system may significantly affect Eve's injection power. Thus, we should analyze this effect in detail. The first factor that contributes to such isolation is the presence of an attenuator to attenuate Alice's signals to the single-photon level. If we assume that the power of Alice's laser is similar to the laser we tested, the required attenuation would be in the order of 60 dB to obtain single-photon-level pulses. This means that Eve's initial injection laser (before going through the attenuator) should be in the order of 100 mW (assuming that there is no internal isolator in the laser) such that about 100-nW power can enter the laser cavity. This value is reasonable and can be safely transmitted through optical fiber, which confirms that the laser-seeding attack is practical.

Furthermore, we note that the attenuation provided by optical attenuators can be decreased via a laser-damage attack [24]. Specifically, Eve can illuminate Alice's attenuator with a cw laser with power of several watts. The experimental results reported in Ref. [24] show that it is possible to permanently decrease the attenuation by more than 10 dB by the cw laser. Importantly, this can be done such that no connector or other components in the experiment are damaged. The attenuator is the only component that responds. Therefore, if Eve applies first the laser-damage attack against the attenuators to decrease their attenuation, then the injection power of the laser-seeding attack could be even lower than 100 mW. This strategy of combination attacks makes the laser-seeding attack easier to implement thanks to the laser-damage attack.

The second factor that could contribute to having more isolation is to include an external isolator. The isolator indeed makes Eve's attack more difficult. However, according to the working mechanism of an optical isolator, the isolation of the backward injection light is due to the polarization rotation inside the isolator, after which the rotated light is extinguished. The rotation is realized by a magneto-optic effect. It is notable that the magnets used in isolators are temperature dependent [69]. In other words, the higher temperature, the smaller rotation. Thus, the temperature is an important factor in practice to determine the real isolation value. From Eve's point of view, she may somehow hack the isolator by increasing the temperature. The quantitative study of the dependence between the optical isolation provided by an optical isolator and the temperature that Eve can achieve is beyond the scope of this Paper, but we have studied this topic in another manuscript [70].

It is clear that for a given power of Eve's injected light, the more effective isolation the users' transmitters have, the smaller the value of the multiplicative factor κ will be, and thus also the effectiveness of the attack. For example, according to Fig. 3, if the power of Eve's injected light is say 10 W, then an effective isolation > 80 dB would result in a multiplicative factor $\kappa < 2$ for ID300 sample 2. Importantly, however, as we see in Fig. 5, whenever $\kappa > 1$ (which in principle might happen even for very high isolation), Alice and Bob might always overestimate their secret key rate, unless, of course, they modify their security analysis to properly incorporate the effect of the laser-seeding attack.

For this, for instance, Alice and Bob could first bound the power of Eve's injected light to a reasonable value, as done for example in Refs. [24,48–50]. With this assumption in place, and for a given value of the isolation of their transmitters, as well as the behavior of their laser sources, Alice and Bob could in principle upper bound the maximum value, $\kappa_{\max}$, that the parameter κ can take. In so doing, and for given observed experimental data (i.e., gains and error rates associated to different values of the intensity settings), they could simply minimize their secret key rate by taking into account that now the intensities of the emitted light pulses might lay in an interval $[\mu, \kappa_{\max}\mu]$, where μ is the value of the original intensity setting. This way Alice and Bob consider the worst-case scenario and can guarantee that the resulting secret key rate is indeed secure.

Another alternative for Alice to determine the parameter $\kappa_{\max}$ might be to use an incoming-light monitor to detect the injection light. The main drawback of this approach is, however, that the classical monitor that detects the injected light is not a reliable device. For example, in Ref. [71], it has been shown that the classical monitor can be bypassed by Eve's pulses with high repetition rate, and thus the classical monitor cannot correctly quantify the amount of injected light. This is due to the limited bandwidth of the classical monitor. Furthermore, the classical monitor may even be damaged by Eve's light [22]. According to the experimental results in Ref. [22], the classical monitor is the first component in Alice that is damaged by Eve's laser. Therefore, the classical detector also may not be a reliable countermeasure to prevent Eve's injection of light.

In practice, it is important to note as well that Eve could in principle combine the laser-seeding attack with various attacks to enhance her hacking capability, for example, with the laser-damage attack [22,24] as mentioned above, with the THA analyzed in Refs. [48–50,53,72,73], and/or with the recently introduced injection-locking attack [59]. For instance, Eve could employ the fact that the laser seeding can be affected in real time by the state of Alice's modulator, changing the laser wavelength depending on the modulator setting [59] and/or modulating the intensity multiplication factor κ. Besides using her injected light to modify the internal functioning of the transmitter (as done in the laser-seeding attack), Eve could also simultaneously perform a THA and measure the back-reflected light to obtain information about the transmitter's settings for each emitted light pulse. This means that to properly evaluate the security of a QKD system, one should probably combine the techniques described in the previous paragraphs with the security analysis introduced in Refs. [48–50,53].

VI. CONCLUSION

This study has experimentally demonstrated that the laser-seeding attack is able to increase the intensity of the light emitted by the laser diode used in a QKD system, breaking the fundamental assumption about the mean photon number of a QKD protocol. Moreover, we show theoretically that such increase of the intensity might seriously compromise the security of QKD implementations. For this, we consider two prominent examples: the standard decoy-state BB84 protocol and MDI QKD, both implemented with phase-randomized WCPs. In both cases, we demonstrate that, in the presence of the attack, the legitimate users of the system might significantly overestimate the secret key rate provided by proper security proofs, even well above known upper bounds. This theoretical security analysis can be applied to any attack that increases the intensity of the emitted pulses. For instance, a laser-damage attack against the optical attenuators also shows that Eve can increase the intensity of Alice's pulses by decreasing the attenuation provided by the attenuators [24].

Although MDI QKD is immune to all detector side-channel attacks, our work shows Eve's capability of hacking the source of a QKD system and highlights that further research is needed to protect the system against source side-channel attacks. Moreover, we remark that the laser-seeding attack may compromise as well the security of other quantum decoy-state-based cryptographic systems beyond QKD, like, for instance, various two-party protocols with practical signals [74], quantum digital signatures [75,76], and blind quantum computing [77,78].

While preparing this Paper for publication, we learnt of another laser-seeding experiment that changes the wavelength of Alice's laser rather than its intensity [59].

ACKNOWLEDGMENTS

We thank Koji Azuma for very useful discussions. This work is funded by the Galician Regional Government (program atlanTTic), the Spanish Ministry of Economy and Competitiveness (MINECO), Fondo Europeo de Desarrollo Regional (FEDER; Grants No. TEC2014-54898-R and No. TEC2017-88243-R), the European Union's Horizon 2020 program under the Marie Skłodowska-Curie project QCALL (Grant No. 675662), the National Natural Science Foundation of China (Grants No. 11674397, No. 61601476, No. 61632021, and No. 61901483), the National Key Research and Development Program of China (Grant No. 2019QY0702), NSERC of Canada (programs Discovery and CryptoWorks21), CFI, MRIS of Ontario, and the Ministry of Education and Science of Russia (NTI center for quantum communications). A.H. is supported by China Scholarship Council. Á.N. is supported from the Spanish Ministry of Education (FPU scholarship). P.C. is supported by the Thai DPST scholarship.

AUTHOR CONTRIBUTIONS

A.H. performed the experimental testing with the assistance of S.-H.S. and P.C. Á.N. and M.C. performed the key rate analysis. V.M. and M.C. supervised the study. A.H., Á.N., and M.C. wrote the Paper with input from all authors.

APPENDIX A. LASER SEEDING BY DIFFERENT WAVELENGTHS

In the laser-seeding attack, we pick the wavelength of the injected light to obtain the maximum energy of

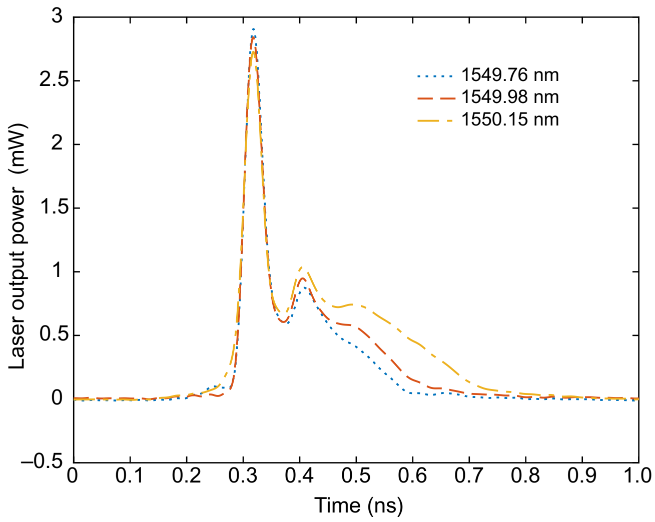

FIG. 7. Averaged waveforms of the laser pulses measured from ID300 sample 1 with 2-mW tampering power for different wavelengths. Each oscillogram is an average over 2000 pulses.

Alice's optical pulses. At this wavelength, we observe the increased energy and the longer tail, as shown in Fig. 2. Moreover, we test the injected light with slightly different wavelengths that are still in the wavelength range of the laser diode from the high-speed oscilloscope, see Fig. 7. Sample 1 of ID300 with 1-nm linewidth is shown as an example. When 2-mW power is injected into the laser, different wavelengths result in different waveforms. At 1550.15 nm, Alice's pulse has the highest energy but relatively lower peak power. When the wavelength is slightly off the center wavelength, at 1549.98 nm, the peak power becomes higher, however the tail is lower. This trend continues when the wavelength is shifted further to 1549.76 nm.

APPENDIX B. DECOY-STATE QKD PROTOCOL

In decoy-state QKD, the transmitter emits quantum states that are diagonal in the Fock basis, and whose mean photon number is selected at random, within a predefined set of possible values, for each output signal. These states are typically generated with an attenuated laser diode emitting phase-randomized weak coherent pulses in combination with a variable attenuator to set the intensity of each individual light pulse.

In particular, let Y_n^α (e_n^α) denote the n-photon yield (error rate) in the polarization basis $\alpha \in \{Z, X\}$. That is, Y_n^α (e_n^α) represents the probability that an n-photon state prepared in the α basis generates a detection click (a detection click associated to an error in the α basis) at Bob's side. For each intensity setting μ, these quantities are related to the overall experimentally observed gain, G_α^μ, and to the overall experimentally observed error rate, E_α^μ, in the α basis as follows:

$$
\begin{aligned}
G_\alpha^\mu &= \sum_n p_n^\mu Y_n^\alpha, \\
E_\alpha^\mu &= \frac{1}{G_\alpha^\mu} \sum_n p_n^\mu e_n^\alpha Y_n^\alpha,
\end{aligned}
\tag{B1}
$$

where p_n^μ denotes the probability that Alice emits an n-photon state when she selects the intensity setting μ. In the case of WCPs, these probabilities follow a Poissonian distribution, $p_n^\mu = e^{-\mu}\mu^n/n!$, that only depends on the mean photon number μ. More precisely, G_α^μ (E_α^μ) represents the probability that a WCP of intensity μ prepared in the α basis generates a detection click (a detection click associated to an error in the α basis) at Bob's side.

Importantly, Eq. (B1) relates the observed quantities G_α^μ and E_α^μ with the unknown parameters Y_n^α and e_n^α through the *known* probabilities p_n^μ. This means, in particular, that by solving the set of linear equations given by Eq. (B1) for different values of μ one can obtain tight bounds on the relevant parameters Y_1^Z and e_1^X, which are required to determine the resulting secret key rate.

Now suppose that Eve performs a laser-seeding attack that increases the output intensity of the emitted pulses from μ to say μ'. In this scenario, Alice and Bob, who are unaware of the attack, would use the experimentally observed quantities $G_\alpha^{\mu'}$ and $E_\alpha^{\mu'}$, which depend on the modified mean photon number μ', together with the original (but now *erroneous*) probabilities p_n^μ that depend on the original intensity μ, to estimate the parameters Y_1^Z and e_1^X. In other words, if Eve implements a laser-seeding attack, Alice and Bob would use the following set of linear equations to estimate Y_1^Z and e_1^X:

$$
\begin{aligned}
G_\alpha^{\mu'} &= \sum_n p_n^\mu Y_n^\alpha, \\
E_\alpha^{\mu'} &= \frac{1}{G_\alpha^{\mu'}} \sum_n p_n^\mu e_n^\alpha Y_n^\alpha.
\end{aligned}
\tag{B2}
$$

In so doing, the bounds obtained for Y_1^Z and e_1^X by solving Eq. (B2) are not guaranteed to be correct bounds for the single-photon yield in the Z basis nor for the phase error rate. Indeed, the correct bounds for these two quantities satisfy Eq. (B1) after substituting μ with μ'.

APPENDIX C. UPPER BOUND R_U FOR DECOY-STATE QKD

Here we briefly summarize the technique introduced in Ref. [64] to derive an upper bound on the secret key rate for a decoy-state QKD protocol. It basically consists in finding the best separable approximation (BSA) [79] among all bipartite quantum states that are compatible with the measurement results observed by Alice and Bob in an execution of the protocol. That is, these are the states that Alice and Bob could have shared in a virtual entanglement protocol that is equivalent to the actual protocol. For simplicity, Ref. [64] considers a decoy-state protocol where Alice and Bob use an infinite number of decoy settings. Note, however, that in the asymptotic limit where Alice sends Bob an infinite number of signals, an upper bound on the secret key rate for this protocol applies as well to a protocol using a finite number of decoy settings. We follow the same procedure here.

In particular, let S^n denote the set of all bipartite quantum states, σ^n_{AB}, which are compatible with Alice and Bob's measurement results in a virtual entanglement protocol that is equivalent to the actual protocol when Alice sends Bob an n-photon signal. More precisely, this set is defined as

$$S^n = \{\sigma^n_{AB} | \mathrm{Tr}[A_k \otimes B_j \sigma^n_{AB}] = p^n_{kj} \; \forall k,j\}, \tag{C1}$$

where $\{A_k\}_k$ and $\{B_j\}_j$ are the measurement operators of Alice and Bob in the virtual entanglement protocol, and p^n_{kj} represent the measured statistics associated to the n-photon signals emitted by Alice. Since we assume that Alice uses an infinite number of decoy intensities, we consider that she can estimate these probabilities precisely.

The states $\sigma^n_{AB} \in S^n$ can always be expressed as a convex sum of one separable state, σ^n_{sep}, and one entangled state, ρ^n_{ent}, as follows:

$$\sigma^n_{AB} = \lambda_n \sigma^n_{\mathrm{sep}} + (1-\lambda_n)\rho^n_{\mathrm{ent}}, \tag{C2}$$

for some real parameter $\lambda_n \in [0,1]$. Then, the BSA of the states in S^n corresponds to that state with the maximum value of the parameter λ_n, which we shall denote by λ^n_{BSA}. In other words, for every n, we want to find the parameter

$$\lambda^n_{\mathrm{BSA}} = \max[\lambda_n | \sigma^n_{AB} \in S^n], \tag{C3}$$

as well as the corresponding entangled state ρ^n_{ent} for the BSA.

In standard decoy-state QKD with four sending states, Alice's measurement operators $\{A_k\}_k$ can be described by a projective measurement in a four-dimensional Hilbert space, i.e., $A_k = |k\rangle\langle k|$ with $k \in \{1,2,3,4\}$. Each operator A_k is associated with Alice sending one of the four possible polarization states of the BB84 protocol. On Bob's side, his measurement operators $\{B_j\}_j$ correspond to a positive-operator valued measurement (POVM) with the following elements:

$$\begin{aligned} B_0 &= \frac{1}{2}|0\rangle\langle 0|, \quad B_1 = \frac{1}{2}|1\rangle\langle 1|, \\ B_\pm &= \frac{1}{2}|\pm\rangle\langle \pm|, \quad B_{\mathrm{vac}} = |\mathrm{vac}\rangle\langle \mathrm{vac}|, \end{aligned} \tag{C4}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, and $|\mathrm{vac}\rangle$ is the vacuum state. As already mentioned in the main text, here we implicitly assume that double-click events are randomly assigned by Bob to single-click events.

In addition, we have that in a prepare-and-measure QKD scheme the reduced density matrix of Alice, $\rho^n_A = \mathrm{Tr}_B(\sigma^n_{AB})$, is fixed by her state preparation process. In the scenario considered, it turns out that ρ^n_A can be written as [64]

$$\rho^n_A = \frac{1}{4}\begin{bmatrix} 1 & 0 & 2^{-n/2} & 2^{-n/2} \\ 0 & 1 & 2^{-n/2} & (-1)^n 2^{-n/2} \\ 2^{-n/2} & 2^{-n/2} & 1 & 0 \\ 2^{-n/2} & (-1)^n 2^{-n/2} & 0 & 1 \end{bmatrix}. \tag{C5}$$

Putting all the conditions together, one can obtain the parameter λ^n_{BSA} and the corresponding entangled state ρ^n_{ent}, for each n, by solving the following semidefinite program (SDP) [64]:

$$\begin{aligned} &\min\ 1 - \mathrm{Tr}[\sigma^n_{\mathrm{sep}}(\boldsymbol{x})], \\ &\text{s.t. } \sigma^n_{AB}(\boldsymbol{x}) \geq 0, \\ &\quad \mathrm{Tr}[\sigma^n_{AB}(\boldsymbol{x})] = 1, \\ &\quad \mathrm{Tr}[A_k \otimes B_j \sigma^n_{AB}(\boldsymbol{x})] = p^n_{kj}, \quad \forall k,j, \\ &\quad \mathrm{Tr}_B[\sigma^n_{AB}(\boldsymbol{x})] = \rho^n_A, \\ &\quad \sigma^n_{\mathrm{sep}}(\boldsymbol{x}) \geq 0, \\ &\quad \sigma^{n,\Gamma}_{\mathrm{sep}}(\boldsymbol{x}) \geq 0, \\ &\quad \sigma^n_{AB}(\boldsymbol{x}) - \sigma^n_{\mathrm{sep}}(\boldsymbol{x}) \geq 0, \end{aligned} \tag{C6}$$

where the vector $\boldsymbol{x}$ is used to parametrize the density operators and Γ denotes partial transposition of one of the subsystems. Note that in Eq. (C6) the state $\sigma^n_{\mathrm{sep}}(\boldsymbol{x})$ represents an unnormalized state, i.e., if we compare this state with that given in Eq. (C2) we have that $\sigma^n_{\mathrm{sep}}(\boldsymbol{x}) = \lambda_n \sigma^n_{\mathrm{sep}}$.

From the optimal solution, $\boldsymbol{x}_{\mathrm{sol}}$, of the SDP above we have that

$$\begin{aligned} \lambda^n_{\mathrm{BSA}} &= \mathrm{Tr}[\sigma^n_{\mathrm{sep}}(\boldsymbol{x}_{\mathrm{sol}})], \\ \rho^n_{\mathrm{ent}} &= \frac{\sigma^n_{AB}(\boldsymbol{x}_{\mathrm{sol}}) - \sigma^n_{\mathrm{sep}}(\boldsymbol{x}_{\mathrm{sol}})}{1 - \lambda^n_{\mathrm{BSA}}}. \end{aligned} \tag{C7}$$

The upper bound on the secret key rate can then be written as [64,80]

$$R_U \leq \sum_{n \geq 1} r_n (1 - \lambda^n_{\mathrm{BSA}}) I^{\mathrm{ent}}_n(A;B), \tag{C8}$$

where $r_n \approx e^{-\mu}\mu^n/n!$ is the probability that Alice sends Bob an n-photon state, where μ is the mean photon number of the signal, and $I^{\mathrm{ent}}_n(A;B)$ is the Shannon mutual information evaluated on $q^n_{kj} = \mathrm{Tr}(A_k \otimes B_j \rho^n_{\mathrm{ent}})$. Note that to calculate Eq. (C8) it is typically sufficient to consider only a finite number of terms in the summation, because of the limit imposed by the unambiguous state discrimination attack. See Ref. [64] for further details.

APPENDIX D. UPPER BOUND R_U FOR MDI QKD

Here we extend the results in Ref. [64] to the MDI QKD framework to calculate an upper bound on the secure key rate coming, for simplicity, from nonpositive partial transposed entangled states [66,67]. Like in Ref. [64], we consider for simplicity that Alice and Bob use an infinite number of decoy settings (see also Appendix C).

In MDI QKD, both Alice and Bob are transmitters while, in the middle, an untrusted third party, Charles, is supposed to perform a Bell state measurement on the incoming signals and publicity announce the result. Let $c \in S_{\rm an}$ denote Charles' announcement, where $S_{\rm an}$ is the set of all possible announcements. This set includes the possible Bell states that Charles can obtain with his measurement as well as the inconclusive event. For each announcement c, we denote the set of bipartite quantum states, $\sigma_{AB,c}^{nm}$, that Alice and Bob could have shared in an equivalent virtual entanglement protocol (given that in the actual protocol they sent n and m photons to Charles, respectively) as S_c^{nm}. That is, S_c^{nm} contains all the bipartite quantum states $\sigma_{AB,c}^{nm}$ that are compatible with Alice and Bob's measurement outcomes in the equivalent virtual entanglement protocol,

$$S_c^{nm} = \{\sigma_{AB,c}^{nm} | \mathrm{Tr}[A_k \otimes B_j \sigma_{AB,c}^{nm}] = p_{kj}^{nmc} \ \forall k,j\}, \tag{D1}$$

where $\{A_k\}_k$ and $\{B_j\}_j$ are the measurement operators of Alice and Bob in the virtual entanglement protocol, and p_{kj}^{nmc} represent the measured statistics associated to Charles" announcement c when Alice (Bob) sends him an n-photon (m-photon) signal. In the same way as in Appendix C, here it is assumed that Alice and Bob can estimate the probabilities p_{kj}^{nmc} precisely because they use an infinite number of decoy intensities.

Similar to the case of the standard decoy-state BB84 protocol considered previously, we have that the states $\sigma_{AB,c}^{nm} \in S_c^{nm}$ can always be decomposed as the convex sum of a separable state, $\sigma_{{\rm sep},c}^{nm}$, and an entangled state, $\rho_{{\rm ent},c}^{nm}$, as follows:

$$\sigma_{AB,c}^{nm} = \lambda_{nm}^c \sigma_{{\rm sep},c}^{nm} + (1-\lambda_{nm}^c)\rho_{{\rm ent},c}^{nm}, \tag{D2}$$

for some real parameter $\lambda_{nm}^c \in [0,1]$.

Now we follow the technique introduced in Ref. [64] (see also Appendix C). In particular, for each pair of values n and m, we search for the parameter λ_{nm}^c (which we call $\lambda_{\rm BSA}^{nmc}$) and the entangled state $\rho_{{\rm ent},c}^{nm}$, which corresponds to the BSA of the states $\sigma_{AB,c}^{nm} \in S_c^{nm}$. More precisely,

$$\lambda_{\rm BSA}^{nmc} = \max\{\lambda_{nm}^c | \sigma_{AB,c}^{nm} \in S_c^{nm}\}. \tag{D3}$$

Then we have that the secret key rate is upper bounded by

$$R_U \leq \sum_{c\in S_{\rm an}} \sum_{n,m\geq 1} p_{c|nm} r_{nm} (1-\lambda_{\rm BSA}^{nmc}) I_{nm,c}^{\rm ent}(A;B), \tag{D4}$$

where $p_{c|nm}$ is the conditional probability that Charles announces c given that Alice (Bob) sends him an n-photon (m-photon) state, $r_{nm} \approx e^{-2\mu}\mu^{n+m}/(n!m!)$ is the probability that Alice and Bob send Charles an n-photon state and an m-photon state, respectively, where μ is the mean photon number of their WCPs, and $I_{nm,c}^{\rm ent}(A;B)$ is the Shannon mutual information calculated on the statistics $q_{kj}^{nmc} = \mathrm{Tr}(A_k \otimes B_j \rho_{{\rm ent},c}^{nm})$, with $\rho_{{\rm ent},c}^{nm}$ being the entanglement part of the BSA of the states $\sigma_{AB,c}^{nm} \in S_c^{nm}$.

To calculate $\lambda_{\rm BSA}^{nmc}$ and the corresponding entangled state $\rho_{{\rm ent},c}^{nm}$ for the BSA we use again SDP. For this, note that Alice's (Bob's) measurement operators $\{A_k\}_k$ ($\{B_j\}_j$) can be described by a projective measurement in a four-dimensional Hilbert space, i.e., $A_k = |k\rangle\langle k|$ ($B_j = |j\rangle\langle j|$) with $k \in \{1,2,3,4\}$ ($j \in \{1,2,3,4\}$). Each operator A_k (B_j) is associated with Alice (Bob) sending one of the four possible polarization states of the BB84 protocol to Charles.

In addition, and similar to the case of Appendix C, we have that both the reduced density matrices of Alice and Bob are fixed by their state preparation processes. More precisely, $\rho_A^{nm} = \mathrm{Tr}_B(\sigma_{AB}^{nm})$ and $\rho_B^{nm} = \mathrm{Tr}_A(\sigma_{AB}^{nm})$ are both equal to Eq. (C5), where $\sigma_{AB}^{nm} = \sum_{c\in S_{\rm an}} p_{c|nm}\sigma_{AB,c}^{nm}$. In fact, in this case, these conditions can even be generalized to $\sigma_{AB}^{nm} = \rho_A^n \otimes \rho_B^m$.

Putting all the conditions together, one can obtain the parameter $\lambda_{\rm BSA}^{nmc}$ and the corresponding entangled state $\rho_{{\rm ent},c}^{nm}$, for each n, m, and c, by solving the following SDP,

$$\begin{aligned}
&\min\ 1 - \mathrm{Tr}[\sigma_{{\rm sep},c}^{nm}(\boldsymbol{x})],\\
&\text{s.t. } \sigma_{AB,t}^{nm}(\boldsymbol{x}) \geq 0 \quad \forall t \in S_{\rm an},\\
&\qquad \mathrm{Tr}[\sigma_{AB,t}^{nm}(\boldsymbol{x})] = 1 \quad \forall t \in S_{\rm an},\\
&\qquad \mathrm{Tr}[A_k \otimes B_j \sigma_{AB,t}^{nm}(\boldsymbol{x})] = p_{kj}^{nmt}, \quad \forall k,j, \forall t \in S_{\rm an}\\
&\qquad \sum_{t\in S_{\rm an}} p_{t|nm}\sigma_{AB,t}^{nm}(\boldsymbol{x}) = \rho_A^n \otimes \rho_B^m,\\
&\qquad \sigma_{{\rm sep},c}^{nm}(\boldsymbol{x}) \geq 0,\\
&\qquad \sigma_{{\rm sep},c}^{nm,\Gamma}(\boldsymbol{x}) \geq 0,\\
&\qquad \sigma_{AB,c}^{nm}(\boldsymbol{x}) - \sigma_{{\rm sep},c}^{nm}(\boldsymbol{x}) \geq 0,
\end{aligned} \tag{D5}$$

where, as mentioned previously, we disregard for simplicity the secret key coming from positive partial transposed entangled states [68] by neglecting in Eq. (D5) the key material provided by those states $\sigma_{{\rm sep},c}^{nm}(\boldsymbol{x})$ that satisfy $\sigma_{{\rm sep},c}^{nm,\Gamma}(\boldsymbol{x}) \geq 0$. A general but computationally more demanding method that considers also the key provided by positive partial transposed entangled states has been proposed, for instance, in Ref. [80]. Let $\boldsymbol{x}_{\text{sol}}$ denote the solution given by the SDP in Eq. (D5), then

$$\begin{aligned}\lambda^{nmc}_{\text{BSA}} &= \text{Tr}[\sigma^{nm}_{\text{sep},c}(\boldsymbol{x}_{\text{sol}})],\\ \rho^{nm}_{\text{ent},c} &= \frac{\sigma^{nm}_{AB,c}(\boldsymbol{x}_{\text{sol}}) - \sigma^{nm}_{\text{sep},c}(\boldsymbol{x}_{\text{sol}})}{1-\lambda^{nmc}_{\text{BSA}}}.\end{aligned} \tag{D6}$$

[1] G. S. Vernam, Cipher printing telegraph systems for secret wire and radio telegraphic communications, J. Am. Inst. Electr. Eng. **45**, 295 (1926).

[2] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120 (1978).

[3] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Comput. **26**, 1484 (1997).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[5] 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).

[6] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki, Secure quantum key distribution, Nat. Photonics **8**, 595 (2014).

[7] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Phys. Rev. A **74**, 022313 (2006), erratum ibid. **78**, 019905 (2008).

[8] 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).

[9] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Opt. Express **15**, 9388 (2007).

[10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photonics **4**, 686 (2010).

[11] 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).

[12] 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).

[13] 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).

[14] 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).

[15] 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).

[16] S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Passive Faraday-mirror attack in a practical two-way quantum-key-distribution system, Phys. Rev. A **83**, 062331 (2011).

[17] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device Calibration Impacts Security of Quantum Key Distribution, Phys. Rev. Lett. **107**, 110501 (2011).

[18] Audun Nystad Bugge, Sebastien Sauge, Aina Mardhiyah Ghazali, Johannes Skaar, Lars Lydersen, and Vadim Makarov, Laser Damage Helps the Eavesdropper in Quantum Cryptography, Phys. Rev. Lett. **112**, 070503 (2014).

[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] Anqi Huang, Shihan Sajeed, Poompong Chaiwongkhot, Mathilde Soucarros, Matthieu Legré, and Vadim Makarov, Testing random-detector-efficiency countermeasure in a commercial system reveals a breakable unrealistic assumption, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[21] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Insecurity of Detector-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **117**, 250505 (2016).

[22] Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagné, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legré, Carter Minshull, and Shihan Sajeed, Creation of backdoors in quantum communications via laser damage, Phys. Rev. A **94**, 030302(R) (2016).

[23] Anqi Huang, Shi-Hai Sun, Zhihong Liu, and Vadim Makarov, Quantum key distribution with distinguishable decoy states, Phys. Rev. A **98**, 012330 (2018).

[24] Anqi Huang, Ruoping Li, Serguei Tchouragoulov, Vladimir Egorov, and Vadim Makarov, Laser damage attack against optical attenuators in quantum key distribution, arXiv:1905.10795 [quant-ph].

[25] Yi Zheng, Peng Huang, Anqi Huang, Jinye Peng, and Guihua Zeng, Practical security of continuous-variable quantum key distribution with reduced optical attenuation, Phys. Rev. A **100**, 012313 (2019).

[26] Yi Zheng, Peng Huang, Anqi Huang, Jinye Peng, and Guihua Zeng, Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack, Opt. Express **27**, 27369 (2019).

[27] Vladimir Chistiakov, Anqi Huang, Vladimir Egorov, and Vadim Makarov, Controlling single-photon detector id210 with bright light, Opt. Express **27**, 32253 (2019).

[28] Charles Ci Wen Lim, Nino Walenta, Matthieu Legré, Nicolas Gisin, and Hugo Zbinden, Random variation of detector efficiency: A countermeasure against detector blinding attacks for quantum key distribution, IEEE J. Sel. Top. Quantum Electron. **21**, 6601305 (2015).

[29] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, W. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato et al., Quantum key distribution with hacking countermeasures and long term field trial, Sci. Rep. **7**, 1978 (2017).

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

[31] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[32] Eli Biham, Bruno Huttner, and Tal Mor, Quantum cryptographic network based on quantum memories, Phys. Rev. A **54**, 2651 (1996).

[33] H. Inamori, Security of practical time-reversed EPR quantum key distribution, Algorithmica **34**, 340 (2002).

[34] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-world Two-photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[35] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Tempor ao, and J. P. von der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).

[36] Yang Liu, Teng-Yun Chen, Liu-Jun Wang, Hao Liang, Guo-Liang Shentu, Jian Wang, Ke Cui, Hua-Lei Yin, Nai-Le Liu, Li Li, Xiongfeng Ma, Jason S. Pelc, M. M. Fejer, Cheng-Zhi Peng, Qiang Zhang, and Jian-Wei Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[37] Zhiyuan Tang, Zhongfa Liao, Feihu Xu, Bing Qi, Li Qian, and Hoi-Kwong Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[38] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W-B Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum key distribution without detector vulnerabilities using optically seeded lasers, Nat. Photonics **10**, 312 (2016).

[39] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan, Measurement-Device-Independent Quantum Key Distribution Over Untrustful Metropolitan Network, Phys. Rev. X **6**, 011024 (2016).

[40] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan, Measurement Device Independent Quantum Key Distribution Over 404 km Optical Fibre, Phys. Rev. Lett. **117**, 190501 (2016).

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

[42] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

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

[44] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, Phys. Rev. A **51**, 1863 (1995).

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

[46] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[47] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, Finite-key security analysis of quantum key distribution with imperfect light sources, New J. Phys. **17**, 093011 (2015).

[48] Marco Lucamarini, Iris Choi, Martin B. Ward, James F. Dynes, Z. L. Yuan, and Andrew J. Shields, Practical Security Bounds Against the Trojan-horse Attack in Quantum Key Distribution, Phys. Rev. X **5**, 031030 (2015).

[49] Kiyoshi Tamaki, Marcos Curty, and Marco Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[50] W. Wang, K. Tamaki, and M. Curty, Finite-key security analysis for quantum key distribution with leaky sources, New J. Phys. **20**, 083027 (2018).

[51] K. Yoshino, Mikio Fujiwara, Kensuke Nakata, Tatsuya Sumiya, Toshihiko Sasaki, Masahiro Takeoka, Masahide Sasaki, Akio Tajima, Masato Koashia, and Akihisa Tomita, Quantum key distribution with an efficient countermeasure against correlated intensity fluctuations in optical pulses, npj Quantum Inf. **4**, 8 (2018).

[52] Akihiro Mizutani, Go Kato, Koji Azuma, Marcos Curty, Rikizo Ikuta, Takashi Yamamoto, Nobuyuki Imoto, Hoi-Kwong Lo, and Kiyoshi Tamaki, Quantum key distribution with setting-choice-independently correlated light sources, npj Quantum Inf. **5**, 8 (2019).

[53] Margarida Pereira, Marcos Curty, and Kiyoshi Tamaki, Quantum key distribution with flawed and leaky sources, arXiv:1902.02126 [quant-ph].

[54] Shi-Hai Sun, Feihu Xu, Mu-Sheng Jiang, Xiang-Chun Ma, Hoi-Kwong Lo, and Lin-Mei Liang, Effect of source tampering in the security of quantum cryptography, Phys. Rev. A **92**, 022304 (2015).

[55] H.-K. Lo and J. Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Inf. Comput. **7**, 431 (2007).

[56] S.-H. Sun, M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, Partially random phase attack to the practical two-way quantum-key-distribution system, Phys. Rev. A **85**, 032304 (2012).

[57] Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-HangFred Fung, Yang Liu, Hai-Lin Yong, Teng-Yun Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan, Source attack of decoy-state quantum key distribution using phase information, Phys. Rev. A **88**, 022308 (2013).

[58] Shi-Hai Sun, Mu-Sheng Jiang, Xiang-Chun Ma, Chun-Yan Li, and Lin-Mei Liang, Hacking on decoy-state quantum key distribution system with partial phase randomization, Sci. Rep. **4**, 4759 (2014).

[59] Xiao-Ling Pang, Ai-Lin Yang, Chao-Ni Zhang, Jian-Peng Dou, Hang Li, Jun Gao, and Xian-Min Jin, Hacking quantum key distribution via injection locking, arXiv:1902.10423 [quant-ph].

[60] J. F. Dynes, M. Lucamarini, K. A. Patel, A. W. Sharpe, M. B. Ward, Z. L. Yuan, and A. J. Shields, Testing the photon-number statistics of a quantum key distribution light source, Opt. Express **26**, 22733 (2018).

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

[62] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[63] Hoi-Kwong Lo, Hoi Fung Chau, and Mohammed Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, J. Cryptology **18**, 133 (2005).

[64] Marcos Curty, Tobias Moroder, Xiongfeng Ma, Hoi-Kwong Lo, and Norbert Lütkenhaus, Upper bounds for the secure key rate of the decoy-state quantum key distribution, Phys. Rev. A **79**, 032335 (2009).

[65] Feihu Xu, He Xu, and Hoi-Kwong Lo, Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution, Phys. Rev. A **89**, 052333 (2014).

[66] A. Peres, Separability Criterion for Density Matrices, Phys. Rev. Lett. **77**, 1413 (1996).

[67] M. Horodecki, P. Horodecki, and R. Horodecki, Separability of mixed states: Necessary and sufficient conditions phys, Phys. Lett. A **223**, 1 (1996).

[68] Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, Secure Key from Bound Entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[69] David Vojna, Ondřej Slezák, Antonio Lucianetti, and Tomáš Mocek, Verdet constant of magneto-active materials developed for high-power faraday devices, Appl. Sci. **9**, 3160 (2019).

[70] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, Reducing the isolation of quantum cryptography systems by high-power laser, Manuscript under preparation.

[71] Shihan Sajeed, Igor Radchenko, Sarah Kaiser, Jean-Philippe Bourgoin, Anna Pappa, Laurent Monat, Matthieu Legré, and Vadim Makarov, Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing, Phys. Rev. A **91**, 032326 (2015).

[72] 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).

[73] 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).

[74] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo, Implementation of two-party protocols in the noisy-storage model, Phys. Rev. A **81**, 052336 (2010).

[75] Hua-Lei Yin, Yao Fu, and Zeng-Bing Chen, Practical quantum digital signature, Phys. Rev. A **93**, 032316 (2016).

[76] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, Experimental measurement-device-independent quantum digital signatures, Nat. Commun. **8**, 1098 (2017).

[77] Ke Xu and Hoi-Kwong Lo, Blind quantum computing with decoy states, arXiv:1508.07910 [quant-ph].

[78] Qiang Zhao and Qiong Li, in *Advances in Intelligent Information Hiding and Multimedia Signal Processing* (Springer, 2017), pp. 155–162.

[79] Maciej Lewenstein and Anna Sanpera, Separability and Entanglement of Composite Quantum Systems, Phys. Rev. Lett. **80**, 2261 (1998).

[80] Tobias Moroder, Marcos Curty, and Norbert Lütkenhaus, Upper bound on the secret key rate distillable from effective quantum correlations with imperfect detectors, Phys. Rev. A **73**, 012311 (2006).

Correction: The order of the affiliation numbers for the sixth author has been reset, and minor fixes to wording in Secs. I and III have been made.