Laser seeding attack in quantum key distribution

Anqi Huang,1,2 Alvaro Navarrete,3 Shi-Hai Sun,4 Poompong Chaiwongkhot,5,6 Marcos Curty,3 and Vadim Makarov6,7,8,5

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, ON, N2L 3G1 Canada
3 El Telecomunicació, 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, ON, N2L 3G1 Canada
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

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.

I. INTRODUCTION

The distribution of a secret key between two authorized parties, Alice and Bob, is a fundamental but challenging cryptographic task. Such secret key is the essential resource of the one-time-pad algorithm [1], the only known encryption method that can achieve 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 [4,5].

There is however a big gap between the theory and the practice of QKD because the behaviour of real QKD devices typically deviates from that considered in the security proofs. Such deviation could be exploited by an eavesdropper, Eve, to obtain information about the secret key without being detected in QKD implementations [6,27]. Most of the quantum hacking attacks realized so far exploit imperfections of the single-photon detectors (SPDs) – the “Achilles’ heel” of QKD [7–27]. 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 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 behaviour 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 new 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 analyses 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 desynchronise the source’s phase and even change other parameters [53]. Indeed, the use of non-phase-randomised 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 “laser seeding attack”, that 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 analyses 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. That is, 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 continuous-wave (c.w.) bright light into Alice’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 have noted that slightly different seed wavelengths result in different pulse

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 analyser (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 have noted that slightly different seed wavelengths result in different pulse
Alice’s laser pulses wider with a much longer and higher tail as shown in Fig. 2 (a) and (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 2–4 secondary oscillations under the attack.

We have measured 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 c.w. 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). That is, the pulse energy increases 3.07 (4.57) times for sample 1 (2).

Under the same experimental procedure done with ID300, a similar effect is observed in the laser LP1550-SAD2. The wavelength of the injected c.w. 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 Fig. 2 (a) and (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. That is, 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 3 nmW 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...
In the Z parameter estimation. In the asymptotic limit of an infinite number of pulses, 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 κ > 1. That is, we will assume that µ′ = κµ 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 will consider first the case of the standard decoy-state BB84 protocol with phase-randomized weak coherent pulses (WCPs); afterward, we will 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, µs, ν1 and ν2 that satisfy µs > ν1 > ν2, and they generate secret key only from those events where they employ the signal intensity µs 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]

\[
R_L = p^{\mu_s}_s Y^Z_{1,L} [1 - H_2(e^Y_{1,L})] - f_s G^{\nu_2}_Z H_2(E^{\nu_2}_Z),
\]

where we assume the efficient version of this protocol [63]. In Eq. (1), \(Y^Z_{1,L} (e^Y_{1,L})\) denotes a lower (upper) bound on the single-photon yield \(Y^Z\) (phase error rate \(e^Y\)), the parameter \(f_s\) is the error correction efficiency, \(G^{\nu_2}_Z\) and \(E^{\nu_2}_Z\) represents the overall experimentally observed gain (the overall experimentally observed QBER) when Alice send to Bob a WCP of intensity \(\mu_s\) 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 \(Y^Z_{1,L}\) and \(e^Y_{1,L}\) one can use analytical or numerical tools. Here we use the analytical method proposed in Ref. [61]. In particular, we have that

\[
Y^Z_{1,L} \geq \frac{\mu_s}{\mu_s(\nu_1 - \nu_2) - \nu_2^2 + \nu_2^2} \left[ G^{\nu_2}_Z e^{\nu_2} - \frac{G^{\nu_2}_Z e^{\nu_2} - \nu_2^2}{\mu_s} \right],
\]

\[
e^Y_{1,L} \leq \frac{E^X_Z G^X e^{\nu_1} - E^X_Z G^X e^{\nu_2}}{(\nu_1 - \nu_2)} Y^X_{1,L},
\]

with \(Y^Z_{0,L}\) being a lower bound on \(Y^Z\) given by

\[
Y^Z_{0,L} \geq \frac{\nu_1 G^{\nu_2}_Z e^{\nu_2} - \nu_2 G^{\nu_2}_Z e^{\nu_2}}{\nu_1 - \nu_2},
\]

and where the parameter \(Y^X_{1,L}\) represents a lower bound on \(Y^X\). 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 \(Y^Z_{1,L}\) and \(e^Y_{1,L}\) using Eqs. (2) and (3) but now with the experimentally observed quantities \(G^X_{\mu}\) and \(E^X_{\mu}'\), with α ∈ {X, Z}, \(\mu' = κ\mu\) and \(\mu \in \{\mu_s, \nu_1, \nu_2\}\) for a certain κ that depends on the attack.

In our analysis we shall also evaluate an ultimate upper bound on the secret key rate. That is, this upper bound holds for any possible post-processing 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

\[
R_U \leq \sum_{n \geq 1} r_n (1 - \lambda^n_{BSA}) I^n_{ent}(A; B),
\]

where \(r_n = e^{-\mu_s n}/n!\) is the probability that Alice sends Bob an n-photon state with the signal intensity, \(\lambda^n_{BSA}\) is the maximum weight of separability among all the bipartite quantum states \(\sigma^n_{AB}\) that are compatible with Alice and Bob’s observables, and \(I^n_{ent}(A; B)\) is the Shannon mutual information evaluated on the entanglement part of the state \(\sigma^n_{AB}\) 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 \(\mu_s, \nu_1\) and \(\nu_2\) 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
TABLE I. Experimental parameters used in the simulations.
The background rate and detection efficiency of the SPDs are taken from Ref. [38].

| Parameter                               | Value       |
|-----------------------------------------|-------------|
| Channel loss coefficient (dB/km)        | 0.2         |
| Background rate                         | $Y_0 = 2.6 \times 10^{-5}$ |
| Total misalignment error                | $e_d = 1.5\%$ |
| Detection efficiency of the SPDs         | $\eta_D = 30\%$ |
| Error correction efficiency             | $f_e = 1.12$ |

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.

FIG. 5. Lower ($R_L$) and upper ($R_U$) bounds on the secret key rate as a function of the parameter $\kappa$ 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.

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 $\kappa$ 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 $\kappa$ is large enough (around 1.7 for the experimental parameters used in Fig. 4), 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 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 shall assume that each of Alice and Bob use three different intensities, $\mu_s, \nu_1$ and $\nu_2$ that satisfy $\mu_s > \nu_1 > \nu_2$, and
they generate 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 $\approx 1$), the secret
key rate is lower bounded by

$$R_L = p_{11,LS} Y_{11,LS}^Z[1 - H_2(e_{11,U}^X)] - f_e G_{11,LS}^z H_2(E_{11,LS}^z),$$

(6)

where $p_{11,LS}$ 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 $\mu_s$. $Y_{11,LS}^Z$ 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 ef-
ficiency, $G_{11,LS}^z$ and $E_{11,LS}^z$ are the gain and the QBER
when both Alice and Bob send to the relay Charles WCPs
of intensity $\mu_s$ 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 $Y_{11,LS}^Z$ and $e_{11,U}^X$ based on the experimentally
available data $G_{11,LS}^z$ and $E_{11,LS}^z$, with $\alpha \in \{Z, X\}$ and
$\zeta, \omega \in \{\mu_s, \nu_1, \nu_2\}$, and their knowledge on the probability
distribution $p_{11,LS}^\alpha m$ with $m, n \in \mathbb{N}$, 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
$Y_{11,LS}^Z$ and $e_{11,U}^X$:

$$Y_{11,LS}^Z \geq \frac{1}{(\mu_s - \nu_2)^2(\nu_1 - \nu_2)^2(\mu_s - \nu_1)^2} \times ([\mu_s^2 - \nu_2^2(\mu_s - \nu_2)(G_{11,LS}^z e^{2\nu_1} + G_{11,LS}^z e^{2\nu_2}) - G_{11,LS}^z e^{\nu_1 + \nu_2}) - (\nu_1^2 - \nu_2^2)(\nu_1 - \nu_2)(G_{11,LS}^z e^{2\mu_s} + G_{11,LS}^z e^{2\nu_2} - G_{11,LS}^z e^{\mu_s + \nu_2} - G_{11,LS}^z e^{\mu_s + \nu_1}),$$

(7)

and

$$e_{11,U}^X \leq \frac{1}{(\nu_1 - \nu_2)^2Y_{11,LS}^Z} \times (e^{2\nu_1} G_{11,LS}^z e^{\nu_1 + \nu_2}) e^{2\nu_2} G_{11,LS}^z \times E_{11,LS}^X e^{\nu_2} - e^{\nu_1} G_{11,LS}^z e^{\nu_1 + \nu_2} - e^{\nu_2} G_{11,LS}^z e^{\nu_1} \times E_{11,LS}^X e^{\nu_1}),$$

(8)

where $Y_{11,LS}^Z$ 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 at-
tack 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 secret key from nonposi-
tive 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 E 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 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.

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.

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 analyse this effect in detail. The

| Distance (km) | $R_L$ without attack ($\kappa=1$) | Incorrect $R_L$ with attack ($\kappa=1.5$) | Correct $R_L$ with attack ($\kappa=1.5$) | $R_U$ with attack ($\kappa=1.5$) | Incorrect $R_U$ with attack ($\kappa=2.5$) | $R_U$ with attack ($\kappa=2.5$) |
|-------------|-------------------------------|---------------------------------|-------------------------------|---------------------------------|---------------------------------|-------------------------------|
| 10          | 10−9                          | 10−8                           | 10−7                          | 10−6                           | 10−5                           | 10−4                           |
| 20          |                               |                                |                               |                                |                                |                                |
| 40          |                               |                                |                               |                                |                                |                                |
| 60          |                               |                                |                               |                                |                                |                                |
| 80          |                               |                                |                               |                                |                                |                                |
| 100         |                               |                                |                               |                                |                                |                                |
| 120         |                               |                                |                               |                                |                                |                                |
| 140         |                               |                                |                               |                                |                                |                                |
| 160         |                               |                                |                               |                                |                                |                                |
| 180         |                               |                                |                               |                                |                                |                                |


| Distance (km) | $R_L$ without attack ($\kappa=1.5$) | Incorrect $R_L$ with attack ($\kappa=2.5$) | Correct $R_L$ with attack ($\kappa=2.5$) | $R_U$ with attack ($\kappa=2.5$) |
|-------------|-------------------------------|---------------------------------|-------------------------------|-------------------------------|
| 10          | 10−9                          | 10−8                           | 10−7                          | 10−6                           |
| 20          |                               |                                |                               |                                |
| 40          |                               |                                |                               |                                |
| 60          |                               |                                |                               |                                |
| 80          |                               |                                |                               |                                |
| 100         |                               |                                |                               |                                |
| 120         |                               |                                |                               |                                |
| 140         |                               |                                |                               |                                |
| 160         |                               |                                |                               |                                |
| 180         |                               |                                |                               |                                |
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 c.w. laser with power of several watts. The experimental results reported in [24] show that it is possible to permanently decrease the attenuation by more than 10 dB by the c.w. 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 have 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]. That is, 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’ve 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 \( \kappa \) 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 have seen in Fig. 3 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 behaviour of their laser sources, Alice and Bob could in principle upper bound the maximum value, \( \kappa_{\text{max}} \), that the parameter \( \kappa \) 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 \([\mu, \kappa_{\text{max}} \mu]\), where \( \mu \) 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 \( \kappa_{\text{max}} \) 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 analysed 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 \( \kappa \). 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 have shown theoretically that such increase of the intensity might seriously compromise the security of QKD implementations. For this, we have considered two prominent examples: the standard decoy-state BB84 protocol and MDI-QKD, both implemented with phase-randomized WCPs. In both cases, we have demonstrated 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 Article for publication, we have learned of another laser seeding experiment that changes the wavelength of Alice’s laser rather than its intensity [69].

[1] G. S. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” J. Am. Inst. Electr. Eng. 45, 295–301 (1926)
[2] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM 21, 120–126 (1978)
[3] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM J. Comput. 26, 1484–1509 (1997)
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74, 145–195 (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 Kiyoishi Tamaki, “Secure quantum key distribution,” Nat. Photonics 8, 595–604 (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, 73–82 (2007).
[9] A. Lamas-Linares and C. Kurtsiefer, “Breaking a quantum key distribution system through a timing side channel,” Opt. Express 15, 9388–9393 (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, 686–689 (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, 27938–27954 (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, O. Maroy, 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 M. 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 Legrè, 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 Sajeev, “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, Ruopeng 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, 27369–27384 (2019).

[27] Vladimir Chistiakov, Anqi Huang, Vladimir Egorov, and Vadim Makarov, “Controlling single-photon detector id210 with bright light,” Opt. Express 27, 32253–32262 (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] AR Dixon, JF Dynes, M Lucamarini, B Fröhlich, AW Sharpe, A Plews, W Tam, ZL 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, 2651–2658 (1996).

[33] H. Inamori, “Security of Practical Time-Reversed EPR Quantum Key Distribution,” Algorithmica 34, 340–365 (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. Temporao, 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, Xiongfei 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] Zhiliyan Tang, Zhongfia 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, 312–315 (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, Yingyiqi 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, 090501 (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, 1330–1333 (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, ZL 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, Go Kato, Hoi-Kwong Lo, and Koji Azuma, “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, Masahide 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-
J. F. Dynes, M. Lucamarini, K. A. Patel, A. W. Sharpe, Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-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).

H.-K. Lo and J. Preskill, “Security of quantum key distribution using weak coherent states with nonrandom phases,” Quantum Inf. Comput. 7, 431–458 (2007).

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).

Yan-Lin Tang, Hua-Lei Yin, Xiongfeng Ma, Chi-Hang-Fred 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).

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).

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].

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).

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

D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Inf. Comput. 4, 325–360 (2004).

Hoi-Kwong Lo, Hoi Fung Chau, and Mohammed Ardehali, “Efficient quantum key distribution scheme and a proof of its unconditional security,” J. Cryptology 18, 133–165 (2005).

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).

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).

A. Peres, “Separability criterion for density matrices,” Phys. Rev. Lett. 77, 1413 (1996).

M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed states: necessary and sufficient conditions,” Phys. Lett. A 223, 1 (1996).

Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim, “Secure key from bound entanglement,” Phys. Rev. Lett. 94, 160502 (2005).

David Vojta, Ondřej Sležák, Antonio Lucianetti, and Tomáš Mocik, “ Verdant constant of magneto-active materials developed for high-power faraday devices,” Appl. Sci. 9, 3160 (2019).

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

Shihian 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).

A. Vakhtitov, V. Makarov, and D. R. Hjelme, “Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography,” J. Mod. Opt. 48, 2023–2038 (2001).

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).

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).

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

G. L. Roberts, M. Lucamarini, ZL Yuan, JF Dynes, LC Com- mandar, AW Sharpe, AJ Shields, M. Curty, IV Puthoor, and E Andersson, “Experimental measurement-device-independent quantum digital signatures,” Nat. Commun. 8, 1098 (2017).

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

Qiang Zhao and Qiong Li, “Blind quantum computation with two decoy states,” in Advances in Intelligent Information Hiding and Multimedia Signal Processing (Springer, 2017) pp. 155–162.

Maciej Lewenstein and Anna Sanpera, “Separability and entanglement of composite quantum systems,” Phys. Rev. Lett. 80, 2261 (1998).

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).

We thank Koji Azuma for very useful discussions. This work was funded by the Galician Regional Government (program atlantITic), the Spanish Ministry of Economy and Competitiveness (MINECO), Fondo Europeo de Desarrollo Regional (FEDER; grants TEC2014-54898-R and TEC2017-88243-R), the European Union’s Horizon 2020 program under the Marie Sklodowska-Curie project QCALL (grant 675662), the National Natural Science Foundation of China (grants 11674397, 11601476, 16163201, and 161901483), the National Key Research and Development Program of China (Grant 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. was supported by China Scholarship Council. Á.N. was supported from the Spanish Ministry of Education (FPU scholarship). P.C. was 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 article 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 Alice’s optical pulses. At this wavelength, we observe the increased energy and the longer tail, as shown in Fig. 2 Moreover, we have tested 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 (WCPs) in combination with a variable attenuator to set the intensity of each individual light pulse.

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

\[
G^\mu_\alpha = \sum_n p_n^\mu Y_n^\alpha, \\
E^\mu_\alpha = \frac{1}{G^\mu_\alpha} \sum_n p_n^\mu e_n^\alpha Y_n^\alpha, 
\]

where \( p_n^\mu \) denotes the probability that Alice emits an \( n \)-photon state when she selects the intensity setting \( \mu \). 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 \( \mu \). That is, \( G^\mu_\alpha \) (\( E^\mu_\alpha \)) represents the probability that a WCP of intensity \( \mu \) prepared in the \( \alpha \) basis generates a detection click (a detection click associated to an error in the \( \alpha \) basis) at Bob’s side.

Importantly, Eq. (B1) relates the observed quantities \( G^\mu_\alpha \) and \( E^\mu_\alpha \) with the unknown parameters \( Y_n^\alpha \) and \( e_n^\alpha \) through the known probabilities \( p_n^\mu \). This means, in particular, that by solving the set of linear equations given by Eq. (B1) for different values of \( \mu \) 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 \( \mu \) to say \( \mu' \). In this scenario, Alice and Bob, who are unaware of the attack, would use the experimentally observed quantities \( G^\mu_\alpha \) and \( E^\mu_\alpha \), which depend on the modified mean photon number \( \mu' \), together with the original (but now erroneous) probabilities \( p_n^{\mu'} \) that depend on the original intensity \( \mu \), to estimate the parameters \( Y_1^Z \) and \( e_1^X \). That is, if Eve implements a laser seeding attack, Alice and Bob would use the following set of linear equations to estimate \( Y_1^Z \) and \( e_1^X \):

\[
G^{\mu'}_\alpha = \sum_n p_n^{\mu'} Y_n^\alpha, \\
E^{\mu'}_\alpha = \frac{1}{G^{\mu'}_\alpha} \sum_n p_n^{\mu'} e_n^\alpha Y_n^\alpha. 
\]

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 \( \mu \) with \( \mu' \).

Appendix C: Upper bound \( R_U \) for decoy-state QKD

Here we briefly summarize the technique introduced in Ref. [63] 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) [70] 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, $\sigma^n_{AB}$, 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. That is, this set is defined as

$$S^n = \{ \sigma^n_{AB} | \text{Tr}[A_k \otimes B_j \sigma^n_{AB}] = p^n_{k,j}, \forall k, j \},$$  \hfill (C1)

where $\{A_k\}_k$ and $\{B_j\}_j$ are the measurement operators of Alice and Bob in the virtual entanglement protocol, and $p^n_{k,j}$ represent the realized 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, $\sigma^{n}_{\text{sep}}$, and one entangled state, $\rho^n_{\text{ent}}$, as follows

$$\sigma^n_{AB} = \lambda_n \sigma^{n}_{\text{sep}} + (1 - \lambda_n) \rho^n_{\text{ent}},$$  \hfill (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 $\lambda$, which we shall denote by $\lambda^n_{BSA}$. That is, for every $n$, we want to find the parameter

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

as well as the corresponding entangled state $\rho^n_{\text{ent}}$ 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

$$B_0 = \frac{1}{2} |0\rangle\langle 0|, \quad B_1 = \frac{1}{2} |1\rangle\langle 1|,$$

$$B_\pm = \frac{1}{\sqrt{2}} |\pm\rangle\langle \pm|, \quad B_{\text{vac}} = |\text{vac}\rangle\langle \text{vac}|,$$

where $|\pm\rangle = \frac{1}{\sqrt{2}} (|0\rangle \pm |1\rangle)$, and $|\text{vac}\rangle$ 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&measure QKD scheme the reduced density matrix of Alice, $\rho^n_A = \text{Tr}_B(\sigma^n_{AB})$, is fixed by her state preparation process. In the scenario considered, it turns out that $\rho^n_A$ can be written as $[64]$

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

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

$$\min 1 - \text{Tr}(\sigma^n_{\text{sep}}(\mathbf{x})), \text{ s.t. } \sigma^n_{AB}(\mathbf{x}) \geq 0, \text{ Tr}(\sigma^n_{AB}(\mathbf{x})) = 1, \text{ Tr}[A_k \otimes B_j \sigma^n_{AB}(\mathbf{x})] = p^n_{k,j}, \forall k, j, \text{ Tr}(\sigma^n_{AB}(\mathbf{x})) = \rho^n_A, \sigma^n_{\text{sep}}(\mathbf{x}) \geq 0, \sigma^n_{\text{sep}}(\mathbf{x}) \geq 0, \sigma^n_{\text{sep}}(\mathbf{x}) - \sigma^n_{\text{sep}}(\mathbf{x}) \geq 0,$$

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

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

$$\lambda^n_{BSA} = \text{Tr}(\sigma^n_{\text{sep}}(\mathbf{x}_{\text{sol}})), \rho^n_{\text{ent}} = \frac{\sigma^n_{AB}(\mathbf{x}_{\text{sol}}) - \sigma^n_{\text{sep}}(\mathbf{x}_{\text{sol}})}{1 - \lambda^n_{BSA}}.$$  \hfill (C7)

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

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

where $r_n \approx e^{-n} \mu^n / n!$ is the probability that Alice sends Bob an $n$-photon state, where $\mu$ is the mean photon number of the signal, and $I^n_{\text{ent}}(A; B)$ is the Shannon mutual information evaluated on $q^n_{kj} = \text{Tr}(A_k \otimes B_j \rho^n_{\text{ent}})$. 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. \[^{[63]}\], 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 publicly announce the result. Let \(c \in S_{\text{an}}\) denote Charles’ announcement, where \(S_{\text{an}}\) 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 will 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,

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

where \(\{A_k\}_k\) and \(\{B_j\}_j\) are the measurement operators of Alice and Bob in the virtual entanglement protocol, and \(p_{k,j}^{nm}\) 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 \(p_{k,j}^{nm}\) 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, \(\sigma_{\text{sep},c}^{nm}\), and an entangled state, \(\rho_{\text{ent},c}^{nm}\), as follows

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

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

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 \(\lambda_{AB,c}^{nm}\) (which we shall call \(\lambda_{\text{BSA}}^{nm}\)) and the entangled state \(\rho_{\text{ent},c}^{nm}\) which correspond to the BSA of the states \(\sigma_{AB,c}^{nm} \in S_c^{nm}\). That is,

\[
\lambda_{\text{BSA}}^{nm} = \max \{\lambda_{AB,c}^{nm} | \sigma_{AB,c}^{nm} \in S_c^{nm} \}. \tag{D3}
\]

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

\[
RU \leq \sum_{c \in S_{\text{an}}} \sum_{n,m \geq 1} p_{\text{ent}}^{nm} r_{nm}(1 - \lambda_{\text{BSA}}^{nm}) r_{\text{ent},c}^{nm}(A;B). \tag{D4}
\]

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

To calculate \(\lambda_{\text{BSA}}^{nm}\) and the corresponding entangled state \(\rho_{\text{ent},c}^{nm}\) for the BSA we use again SDP. For this, note that Alice’s (Bob’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 \(k \in \{1, 2, 3, 4\}\) \((j \in \{1, 2, 3, 4\}\). 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, \(\rho_A^{nm} = Tr_B[\sigma_{AB,c}^{nm}]\) and \(\rho_B^{nm} = Tr_A[\sigma_{AB,c}^{nm}]\) are both equal to Eq. (C5), where \(\sigma_{AB,c}^{nm} = \sum_{c \in S_{\text{an}}} p_{\text{ent}}^{nm} \rho_{\text{ent},c}^{nm}\). In fact, in this case, these conditions can even be generalized to \(\sigma_{AB}^{nm} = \rho_A^{nm} \otimes \rho_B^{nm}\).

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

\[
\begin{align*}
\min & - 1 - Tr(\sigma_{\text{sep},c}^{nm}(\mathbf{x})) \\
\text{s.t.} & \sigma_{AB,c}^{nm}(\mathbf{x}) \geq 0 \forall t \in S_{\text{an}} , \\
& Tr[\sigma_{AB,c}^{nm}(\mathbf{x})] = 1 \forall t \in S_{\text{an}} , \\
& Tr[A_k \otimes B_j \sigma_{AB,c}^{nm}(\mathbf{x})] = p_{k,j}^{nm} \forall k,j \forall t \in S_{\text{an}} , \\
& \sum_{t \in S_{\text{an}}} p_{t}^{nm} \sigma_{AB,c}^{nm}(\mathbf{x}) = \rho_A^{nm} \otimes \rho_B^{nm} , \\
& \sigma_{\text{sep},c}^{nm}(\mathbf{x}) \geq 0 , \\
& \sigma_{\text{sep},c}^{nm}(\mathbf{x}) \geq 0 , \\
& \rho_{\text{ent},c}^{nm}(\mathbf{x}) - \sigma_{\text{sep},c}^{nm}(\mathbf{x}) \geq 0 , \tag{D5}
\end{align*}
\]

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 \(\sigma_{\text{sep},c}^{nm}(\mathbf{x})\) that satisfy \(\sigma_{\text{sep},c}^{nm}(\mathbf{x}) \geq 0\). 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 \(\mathbf{x}_{\text{sol}}\) denote the solution given by the SDP in Eq. (D5), then

\[
\begin{align*}
\lambda_{\text{BSA}}^{nm} &= Tr(\sigma_{\text{sep},c}^{nm}(\mathbf{x}_{\text{sol}})) , \\
\rho_{\text{ent},c}^{nm} &= \frac{\sigma_{AB,c}^{nm}(\mathbf{x}_{\text{sol}}) - \sigma_{\text{sep},c}^{nm}(\mathbf{x}_{\text{sol}})}{1 - \lambda_{\text{BSA}}^{nm}} . \tag{D6}
\end{align*}
\]