APL Photonics

RESEARCH ARTICLE | JUNE 12 2025

Evaluation of quantum key distribution systems against injection-locking attacks

Jerome Wiesemann ; Fadri Grünenfelder ; Ana Blázquez Coído ; Nino Walenta ; Davide Rusca

APL Photonics 10, 066112 (2025)
https://doi.org/10.1063/5.0260685

AIP Publishing

Evaluation of quantum key distribution systems against injection-locking attacks

Cite as: APL Photon. 10, 066112 (2025); doi: 10.1063/5.0260685
Submitted: 26 January 2025 • Accepted: 28 May 2025 •
Published Online: 12 June 2025

Jerome Wiesemann,[1,a] Fadri Grünenfelder,[2,3,4] Ana Blázquez Coído,[2,3,4] Nino Walenta,[1] and Davide Rusca[2,3,4]

AFFILIATIONS

[1] Fraunhofer Institute for Telecommunications, Heinrich Hertz Institute, HHI, 10587 Berlin, Germany
[2] Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[3] Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[4] AtlanTTic Research Center, University of Vigo, Vigo E-36310, Spain

[a] **Author to whom correspondence should be addressed:** jwiesemann@uwaterloo.ca

ABSTRACT

While ideal quantum key distribution (QKD) systems are well-understood, practical implementations face various vulnerabilities, such as side-channel attacks resulting from device imperfections. Current security proofs for decoy-state BB84 protocols either assume uniform phase randomization of Alice's signals, which is compromised by practical limitations and attacks like injection locking, or rely on a (partially) characterized phase distribution. This work presents an experimental method to characterize the phase de-randomization from injection locking using a heterodyne detection setup, providing a lower bound on the degree of isolation required to protect QKD transmitters against injection-locking attacks. The methods presented are source-agnostic and can be used to evaluate general QKD systems against injection-locking attacks.

I. INTRODUCTION

Quantum key distribution (QKD) is a method of establishing information-theoretically secure keys between two parties, commonly known as Alice and Bob.[1–3] Unlike classical methods that rely on computational assumptions about a potential adversary, Eve, QKD provides a solution where Eve is limited only by the laws of quantum physics. While the security of ideal QKD systems is rather well-understood,[4–8] security proofs make various model assumptions about the physical implementation.[9,10] Any discrepancy between the model and the implementation, for example due to device imperfections, may lead to *side-channel attacks*, where Eve gathers additional information about the key that is not modeled in the proof.[11–13] Usually, the model must then be adjusted to account for given device imperfections, and security proven for this new model. In the last two decades, much effort has been devoted to closing the gap between the implementation and the model, e.g., by increasing the complexity of the theoretical models[10,14,15] or by proposing new protocols with fewer assumptions on the behavior of both the transmitter[16,17] and the receiver.[18,19]

As a well-known example, earlier analyses assumed that Alice generates single photons.[5,20] Owing to their greater practicality, weakly coherent states have become a favored means to generate Alice's signals as part of the *decoy-state BB84 protocol*,[21–23] which is arguably the most widespread protocol at present due to its high practicality and key rates. A common assumption of security proofs for decoy-state QKD is that the phases of Alice's signals are uniformly random.[6,8,14] Security can still be proven without uniformly distributed phases, but performance is drastically affected with current security proofs[10,24,25] and requiring a (partial) characterization of the degree of phase randomization.

The *injection-locking attack* specifically aims at attacking the phase randomization process by injecting light into Alice's setup in order to lock the phase of her light source. We note that even without this attack, perfect uniform distribution is experimentally not feasible, and the degree of phase randomization must be

experimentally characterized. Laser-seeding attacks have been experimentally demonstrated using phase information[26] and frequency information.[27] The effect of laser-seeding attacks on the intensity has been studied experimentally and theoretically in Ref. 28. Injection locking has also been used for a photon-number splitting attack.[29] A recent work describes the effect of injection locking on phase de-randomization,[30] but their analysis focuses on modeling laser behavior and is thus not generally applicable without specific assumptions about that behavior. Until now, analyses of injection locking have focused on experimental demonstrations but do not provide a rigorous method to evaluate QKD systems against such an attack.

Our work specifically aims at proposing an approach to experimentally characterize the degree of phase randomization of QKD systems under injection locking using a metric similar to recent theoretical analyses of imperfect phase randomization.[25,31] We present a robust method to evaluate QKD transmitters against phase de-randomization from injection locking. The main result is a characterization yielding a minimum degree of isolation required to protect QKD transmitters against injection-locking attacks. The experimental methods presented are source-agnostic and can be used to evaluate QKD systems against injection-locking attacks, e.g., in evaluation laboratories through black-box testing as part of a certification process. While we demonstrate the methods using a DFB laser in this work, the device under test (DUT) can be substituted, for instance, with a QKD transmitter.

In Sec. II, we begin by discussing the role of phase randomization in QKD and introduce the q_{rel}-parameter as a metric to quantify the degree of phase de-randomization under an injection-locking attack. We also describe the injection-locking attack and discuss how it affects the security of QKD systems. We then present the methods used to determine the relative phase distribution of the DUT using a heterodyne detection setup in Sec. III and discuss the effect of polarization on the degree of injection locking. Finally, the main result is a characterization of the q_{rel}-parameter as a function of the injected optical power, which yields a lower bound on the degree of optical isolation required to protect QKD systems against injection-locking attacks.

II. BACKGROUND

A. Phase randomization in QKD

In most of the current security proofs for the decoy-state BB84 protocol, Alice is assumed to send phase-randomized weak coherent states.[6,8,14,32,33] Uniform phase randomization is a core assumption of these proofs. Indeed, a state with intensity μ sent by a phase-randomized coherent source can be represented by the density matrix,

$$\rho_\mu = \int_0^{2\pi} d\theta f(\theta) |\sqrt{\mu} e^{i\theta}\rangle\langle\sqrt{\mu} e^{i\theta}|, \tag{1}$$

where $|\sqrt{\mu} e^{i\theta}\rangle$ are coherent states with mean photon number μ and phase θ,[34] and f is the probability density function (PDF) representing the probability of sending a coherent state with a given phase. In the case of uniformly distributed phases, $f(\theta) = 1/(2\pi)$, and the equation mentioned earlier can be rewritten as a coherent superposition of Fock states $|n\rangle$ (see Appendix A)

$$\rho_\mu = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} |n\rangle\langle n|, \tag{2}$$

i.e., it is diagonal in the Fock basis. This is used in security proofs to reduce the problem to a discussion of the statistics of vacuum, single-photon, and multi-photon events.[6,8,14,33] In the case of imperfect phase randomization, e.g., due to device imperfections or active attacks such as injection locking, Eq. (2) does not hold, and the standard decoy-state BB84 method cannot be applied. It is still possible to prove security without uniform phase randomization, but current security proofs[24,25,31] require a characterization of either the full PDF $f(\theta)$ or a metric q describing the degree of phase randomization, which we introduce in Sec. II C. We will use a metric closely related to the q-parameter to quantify the degree of phase de-randomization induced by Eve from an injection-locking attack. This metric provides a practical means for evaluating the security of QKD systems against these attacks.

B. Injection-locking attack

There exist two commonly used methods to practically implement phase randomization in QKD: incorporating a phase modulator or using a gain-switched laser. The drawback of the former approach is that it requires an additional active component, a phase modulator, combined with a high-quality entropy source for selecting the random phase, and that the phase choices are discrete, which negatively affects the performance compared to uniform phase randomization.[24,35] A popular alternative is gain-switched lasers, which inherently produce phase-randomized pulses. Indeed, in each gain-switching cycle, the pulse is generated from spontaneous emission and amplification of photons with a random phase. This, however, requires that spontaneous emission initiates the buildup, which implies that no residual photons remain in the cavity between pulses. If, however, residual photons remain in the cavity, they can initiate the process through stimulated emission, leading to phase correlations between these residual photons and the newly generated pulse.

The injection-locking attack precisely aims at making use of this property. In fact, Eve injects light with a known phase into Alice's laser cavity such that, following the earlier discussion, the phase of the generated pulses is correlated with that of the injected light. This alters the PDF describing Alice's phase randomization such that, generally, Eq. (1) does not simplify to Eq. (2) any longer. The injection-locking attack does not apply to implementations with active phase randomization, which, however, exhibit the previously mentioned drawbacks.

To the best of our knowledge, an experimental method to rigorously characterize the influence of Eve on the phase randomization process by means of injection locking has not yet been developed and is, therefore, the aim of this work. The methods presented can be used to evaluate QKD systems against injection-locking attacks, e.g., through means of black-box testing. In the following, we use a gain-switched laser as it is vulnerable to these attacks, but note that our methods can also be used to characterize other light sources.

C. Quantifying phase randomization

We quantify the influence of Eve on the phase randomization by choosing a metric closely related to the one introduced in two

recent theoretical analyses of imperfect phase randomization.[25,31] To simplify the discussion, we assume that no phase correlations are present in the laser cavity without an injection-locking attack, such that Alice's signals are independently and identically prepared. We note that this assumption is reasonable, as phase correlations at a 5 GHz repetition rate are already small,[36] and we are operating at a repetition rate that is two orders of magnitude lower in this work. The degree of phase randomization of a sequence of N phases is described by the q-parameter defined as[31]

$$f\left(\theta^{(n)}|\theta^{(n-1)}\dots\theta^{(1)}\right) \geq \frac{q}{2\pi}, \tag{3}$$

for all $\theta^{(n)} \in [0, 2\pi)$, where $n \in \{1, \dots, N\}$ and $0 < q \leq 1$. In other words, the q-parameter is a lower bound on the probability of generating a pulse with any given phase. For uniformly distributed phases, $q = 1$, while for imperfect phase randomization, $q < 1$, and q approaches zero if, for example, the phase distribution is strongly localized.

Hence, the q-parameter describes the degree of phase randomization of Alice's pulses. However, the methods we present do not allow for a direct measurement of the phase $\theta^{(n)}$ but rather the phase $\Delta\theta^{(n)}$ relative to a reference phase, cf. Sec. III B. Hence, we quantify the degree of phase randomization, relative to a reference phase, by defining a metric similar to the q-parameter, which we call the *relative q-parameter* and denote q_{rel}, defined as the lower bound

$$f\left(\Delta\theta^{(n)}|\Delta\theta^{(n-1)}\dots\Delta\theta^{(1)}\right) \geq \frac{q_{\text{rel}}}{2\pi}, \tag{4}$$

for all $\Delta\theta^{(n)} \in [0, 2\pi)$, where $n \in \{1, \dots, N\}$ and $0 < q_{\text{rel}} \leq 1$, analogously to Eq. (3). We use this metric to quantify the influence of Eve on the phase randomization when performing an injection-locking attack. While it does not directly correspond to the q-parameter, it is closely related as it quantifies the degree of phase randomization relative to Eve's reference phase. In fact, $q = q_{\text{rel}}$ in the case of an ideal attack. We discuss this more thoroughly in Sec. III B.

As discussed in Sec. II B, if Eve injects light into the laser cavity, she can modify the PDF describing the phase randomization of Alice's signals. In theory, Eve can introduce correlations between any two pulses by changing the degree of injection locking based on previous measurement outcomes (e.g., by adjusting the optical power or polarization state of her laser). Nevertheless, if the smallest q_{rel} she can induce from an injection-locking attack is known, then Eq. (4) holds even if Eve arbitrarily varies the degree of injection locking from pulse to pulse. Consequently, we can ignore correlations in our analysis and focus on determining the smallest q_{rel} Eve can induce with an injection-locking attack. To simplify the notation, we define

$$f\left(\Delta\theta^{(n)}\right) := f\left(\Delta\theta^{(n)}|\Delta\theta^{(n-1)}\dots\Delta\theta^{(1)}\right), \tag{5}$$

in the following. In Sec. III, we show how to determine the phase distribution of Alice's pulses under an injection-locking attack, relative to a reference phase, and then compute the q_{rel}-parameter.

III. PHASE RANDOMIZATION CHARACTERIZATION

A. Setup

The goal is to quantify the degree of phase de-randomization Eve can induce with an injection-locking attack. In order to achieve this, a heterodyne detection setup with a continuous DFB master laser (ML), corresponding to Eve, and a gain-switched DFB slave laser (SL), corresponding to Alice, is used. The setup is illustrated in Fig. 1 and the equipment listed in Appendix B. The ML injects light into the SL, and the phase correlations are measured using an interferometer and two homodyne detectors. By increasing the isolation between the ML and SL, using a variable optical attenuator (VOA), we can simulate Alice's components and determine the degree of phase de-randomization Eve can induce with her ML as a function of the optical power reaching Alice's laser, cf. Sec. III E. We note that in this work, the DUT is a gain-switched DFB laser, but it can be replaced by a QKD transmitter to perform black-box testing (cf. Sec. III E).

We use master and slave lasers with similar spectra, as depicted in Fig. 2. Matching of the spectra may significantly affect the degree of injection locking. We thus note an important property of this method, namely that the characterization may only be as good as the ML simulates Eve's best possible attack. In fact, the methods presented in this work provide a lower bound on the degree of injection locking Eve can induce. We remark that the dependency of the experimental characterization on the ML is due to injection locking strongly depending on the specific properties of the devices involved and that there may not exist a single light source that replicates an ideal attack for all DUTs. An alternative approach would involve adopting a different characterization method altogether; however, this requires further experimental and theoretical investigations. Nevertheless, we note that this dependency on the specific equipment used is an inherent limitation of an evaluation process conducted as black-box testing.

The SL spectrum under light injection is depicted in Fig. 2 for matching ML and SL spectra with a slight offset. The central wavelength of the ML can be controlled by adjusting the temperature of the laser. The spectra are acquired using an optical spectrum analyzer (OSA) placed at the SL input and at the monitoring port (see Fig. 1) to determine the ML and SL spectra, respectively. The acquisition was performed with a resolution of 0.05 nm. We observe a spectral shift when the SL is injection-locked, which can be exploited as demonstrated in Ref. 27. We note that intensity changes due to light injection were observed in Ref. 28 and are likely to be observable in our case as well, although we did not measure these effects since they were already studied in previous studies.

The ML injects continuous light, with a linewidth of 1 MHz according to the manufacturer, into the SL. The ML coherence time must be much longer than the propagation delay of one arm with respect to the other in the interferometer. If this is not the case, the light interfering at the 90° optical hybrid does not have a fixed phase relation, even if the SL is perfectly locked. In addition, the ML coherence time must be longer than the pulse duration of the SL. In our case, both conditions are satisfied since the coherence time of the ML is about 1 μs, while the pulse duration of the SL is 12.5 ns, and the difference in arm length is on the order of a meter, which corresponds to a propagation delay of 5 ns.

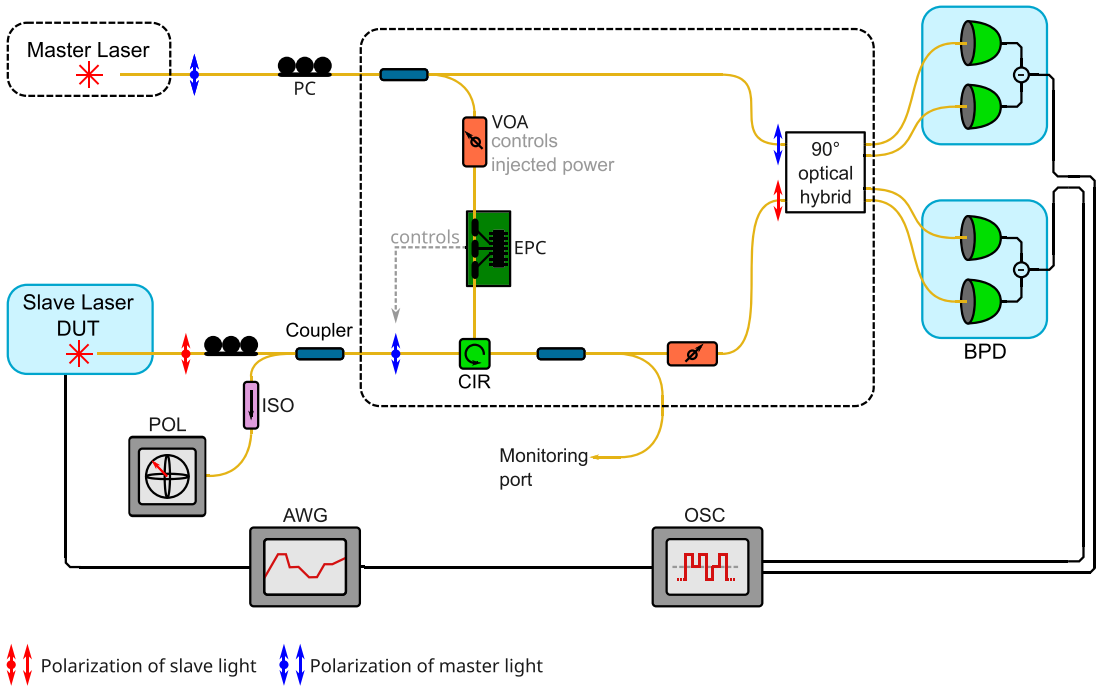

FIG. 1. Setup used to characterize the phase distribution under an injection-locking attack. The dashed boxes indicate temperature-stabilized environments. The double-headed arrow with a dot in the center symbolizes an arbitrary polarization. PC: polarization controller, VOA: variable optical attenuator, EPC: electronic polarization controller, CIR: circulator, BPD: balanced photodiodes, OSC: oscilloscope, AWG: arbitrary waveform generator, POL: polarizer, ISO: isolator, DUT: device under test.

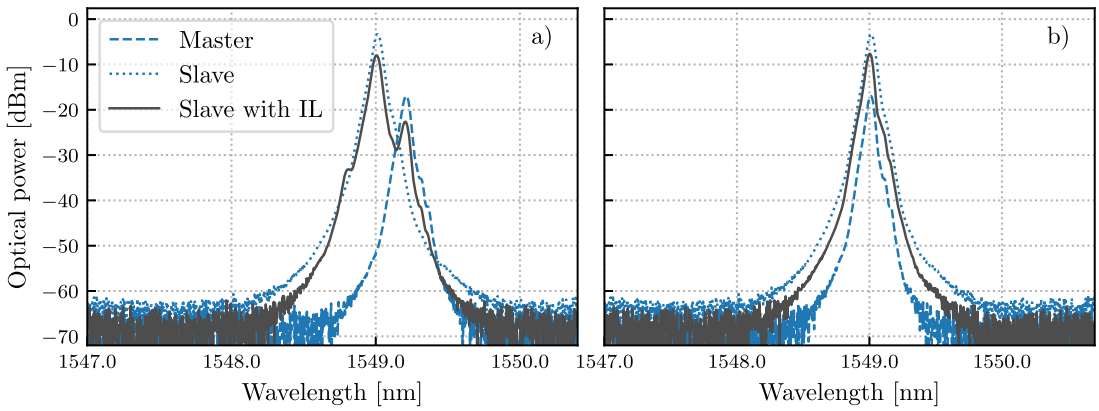

FIG. 2. Spectra of the master laser (ML) and slave laser (SL), as well as the SL spectrum under light injection for (a) slight spectrum offset (ϑ_{ML} = 20 °C) and (b) matching spectra (ϑ_{ML} = 17.9 °C). The ML central wavelength can be controlled by adjusting the temperature of the laser ϑ_{ML}. Note that a 5 dB attenuator is placed in front of the OSA when acquiring the SL spectrum with light injection.

The SL is gain-switched using an arbitrary waveform generator (AWG). The SL is modulated with a 40 MHz rectangular signal with a 50% duty cycle. As discussed in Sec. II A, under normal conditions, gain-switching results in a random phase between each pulse, following the PDF $f\left(\theta^{(n)}\right)$. Now, due to light injection from the ML, the phase of the SL is correlated with that of the ML, resulting in a different PDF. We cannot directly determine the phase distribution, as the phase measurement is inherently relative to a reference phase. However, we can use the q_{rel}-parameter, introduced in Sec. II C, as a metric to quantify the phase distribution of the SL relative to the ML. This motivates why the characterization depends on the ability for the ML to simulate Eve's best possible attack.

The SL phase distribution, relative to the ML phase, is determined by interfering the ML signal with the SL signal using an interferometer. In the following, the ML will be referred to as the local oscillator and the SL as the signal. The interferometer is

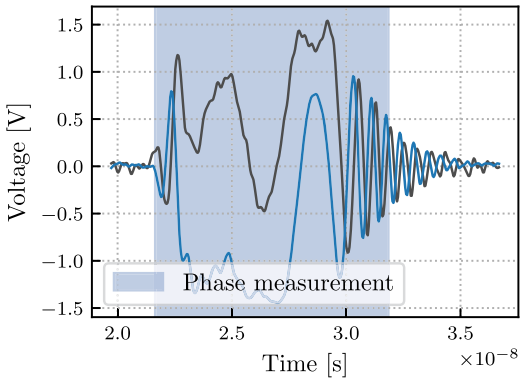

FIG. 3. Example oscilloscope homodyne detection signal with 0° (blue) and 90° (black) phase shifts with −42.3 dBm injection locking measured at the input of the slave laser. The blue region represents the window used to determine the phase of the pulse.

maintained in a thermally controlled environment to minimize thermal fluctuations and the resulting phase fluctuations due to the long interferometer path lengths. We require that the phase fluctuations introduced by the interferometer happen on timescales longer than the acquisition time. In other words, phase fluctuations must be negligible during the time period over which the signal is recorded to produce the histogram discussed below, i.e., Fig. 5. Otherwise the resulting phase distribution may be more uniformly distributed than expected.[37] We found that the change in phase induced by the interferometer during the time of one measurement (200 μs) is less than 5×10^{-4} rad and, therefore, negligible. This was found by replacing the SL with a Faraday mirror and, therefore, interfering with the ML with itself.

An example homodyne detection signal, measured on the oscilloscope, is depicted in Fig. 3 with injection locking. In Sec. III B, we determine the relative phase of the SL pulses from the homodyne detection signal.

B. Determining the relative phase of the pulses

In the following, we denote T_S as the SL period and introduce n to denote the nth pulse. Let $\tau_n = t - nT_S$ describe the time coordinate relative to the nth pulse. In the following, for any function with subscript n, the time dependency is relative to the nth pulse. We write the electric field of the nth pulse of the SL at a fixed point in space as

$$\mathbf{E}_S^{(n)}(\tau_n) = e^{i\theta^{(n)}(\tau_n)}\mathbf{A}_S^{(n)}(\tau_n), \tag{6}$$

where $\theta^{(n)}(\tau_n)$ describes the phase of the optical pulse, which is generally random and,

$$\mathbf{A}_S^{(n)}(\tau_n) = \left(\mathbf{A}_S^{(n)}(\tau_n)\right)^*. \tag{7}$$

Notice that this expression is general, and we do not make any assumption about the shape of the pulse nor its spectrum. We also write the LO signal as a generic field

$$\mathbf{E}_{LO}^{(n)}(\tau_n) = e^{i\theta_{LO}^{(n)}(\tau_n)}\mathbf{A}_{LO}^{(n)}(\tau_n), \tag{8}$$

where $\mathbf{A}_{LO}^{(n)}(\tau_n) = \left(\mathbf{A}_{LO}^{(n)}(\tau_n)\right)^*$. Assuming perfectly balanced photodetectors, the homodyne detection signal of the nth pulse is then given by (see Appendix C)

$$I_0^{(n)}(\tau_n) = A(\tau_n)\cos\left(\theta^{(n)}(\tau_n) - \theta_{LO}^{(n)}(\tau_n)\right), \tag{9}$$

where $A(\tau_n) := 2\mathbf{A}_S^{(n)}(\tau_n)\cdot\mathbf{A}_{LO}^{(n)}(\tau_n)$. Similarly, the 90° phase shifted homodyne detection signal is

$$I_{\pi/2}^{(n)}(\tau_n) = A(\tau_n)\sin\left(\theta^{(n)}(\tau_n) - \theta_{LO}^{(n)}(\tau_n)\right). \tag{10}$$

Therefore, the phase difference between the SL and ML for the nth pulse at time τ_n is given by

$$\Delta\theta^{(n)}(\tau_n) = \arctan 2\left(I_0^{(n)}(\tau_n), I_{\pi/2}^{(n)}(\tau_n)\right), \tag{11}$$

where arctan 2 denotes the 2-argument arctangent and we define $\Delta\theta^{(n)}(\tau_n) := \theta^{(n)}(\tau_n) - \theta_{LO}^{(n)}(\tau_n)$ to simplify the notation. Intuitively, this phase difference describes the phase of Alice's pulses relative to Eve's reference phase. We see that a heterodyne detection setup yields the relative phase; hence, why we introduced the q_{rel}-parameter in Sec. II C. We also observe that the q-parameter and q_{rel}-parameter are closely related, as in the case of an ideal attack, $\theta_{LO}^{(n)}(\tau_n) = \theta_{LO}^{(m)}(\tau_m)$ for all m, n, such that $q_{rel} = q$ as $f\left(\Delta\theta^{(n)}\right) \equiv f\left(\theta^{(n)}\right)$ up to a constant offset. By definition, we have $q_{rel} \geq q$.

We note that the earlier description allows for general time-dependent phase distributions. Hence, in the following, we add a time-dependency to the PDF $f(\Delta\theta^{(n)}, \tau_n)$ to describe the relative phase distribution for each point τ_n on the pulse. Similarly, we denote $q_{rel}(\tau_n)$ as the relative q-parameter corresponding to $f(\Delta\theta^{(n)}, \tau_n)$, following Eq. (4). This dependency on τ_n of the relative phase randomization stems from the fact that the ML is not ideal and that the phase randomization process (and phase shift) of the SL may vary over the duration of the pulse. The latter observation is an effect that, to the best of our knowledge, is not currently incorporated in security proofs that assume a modulation of a constant phase shift over the pulse duration.[24,25,31]

In the following, for each measurement, we choose an acquisition time of 200 μs on the oscilloscope, which corresponds to $N = 8000$ pulses. As discussed before, any phase fluctuation, e.g., resulting from temperature fluctuations, must be negligible during the acquisition time. On the other hand, a longer acquisition time implies more samples and, therefore, a better confidence interval on the q_{rel}-parameter. The oscilloscope has a finite sampling rate (of 50 Gsps in our case), and we determine the relative phase $\Delta\theta^{(n)}(\tau_n)$ at each measurement point τ_n, following Eq. (11). We assume that fluctuations of the relative phase are negligible within one sampling period. The minimum sampling rate required for the characterization thus depends on the pulse width and the desired granularity. Under realistic attack conditions that can last for hours, the polarization of the injected light can fluctuate due to polarization drifts in the optical fibers. In addition, the SL temperature may drift over time. Therefore, to ensure long-term stability, both the temperature and polarization of the

ML can be stabilized actively, e.g., by implementing a feedback loop.

We choose a time window that is centered in the pulse to determine the phase, cf. Fig. 3, as the intensity of the homodyne detection signal is too low on the edges of the pulse (and outside of the pulse) for a reliable characterization of the q_{rel}-parameter. This is an experimental limitation, and using, for example, a faster oscilloscope may allow for a characterization over a broader time window. See Appendix D for a more thorough discussion on how the window is chosen. For each sample at time τ_n in this window, we determine the corresponding relative phase $\Delta\theta^{(n)}(\tau_n)$ following Eq. (11). This can be visualized as follows. For each pulse, the homodyne detection signal acquired by the oscilloscope at a given time τ_n is plotted in phase space where the x-coordinate is given by $I_0^{(n)}(\tau_n)$ and the y-coordinate is given by $I_{\pi/2}^{(n)}(\tau_n)$, as depicted in Fig. 4, for −42.3 dBm light injection (measured at the input of the slave laser) and without injection locking. We acquire the measurements without injection locking by disconnecting the fiber between the ML and SL. Following Eq. (11), the instantaneous relative phase $\Delta\theta^{(n)}(\tau_n)$ between the nth pulse of the SL and the ML is then given by the angle between the vectors $(x,y)^{\mathrm{T}}$ and $(1,0)^{\mathrm{T}}$.

For all τ_n in the window described earlier, we plot the histogram of the phases for a given injected optical power, as depicted in Fig. 5 for $\tau_n = 6.56$ ns with and without light injection. We clearly observe that the relative phase of the generated optical pulses is localized under an injection-locking attack while being almost uniformly distributed without injection locking.

In this section, we have seen how to determine the relative phase of the SL pulses from the heterodyne detection signal. In Sec. III C, we quantify the degree of phase de-randomization from injection locking by determining the q_{rel}-parameter introduced in Sec. II C from the histogram depicted in Fig. 5.

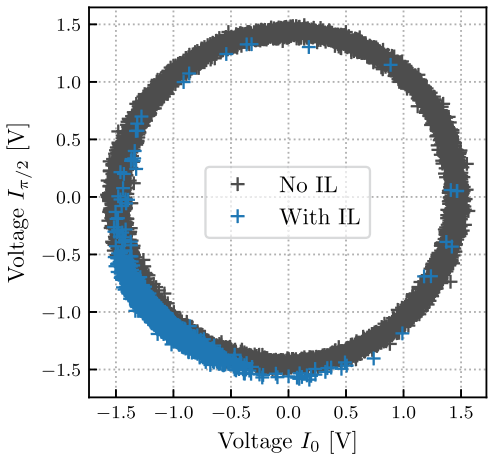

FIG. 4. Homodyne detection signals $I_0^{(n)}(\tau_n)$ and $I_{\pi/2}^{(n)}(\tau_n)$ of the $N = 8000$ acquired slave laser pulses, plotted in phase space for $\tau_n = 6.56$ ns with −42.3 dBm injected power measured at the input of the slave laser and without injection locking.

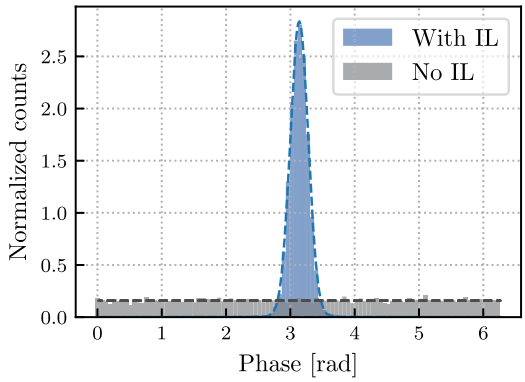

FIG. 5. Histogram of the phases for the $N = 8000$ slave laser pulses, determined from Fig. 4, for $\tau_n = 6.56$ ns with −42.3 dBm injected power measured at the input of the slave laser and without injection locking.

C. Determining the degree of phase de-randomization from injection locking

The q_{rel}-parameter introduced in Sec. II C describes the phase randomization of the SL relative to the ML. The next step is to determine the q_{rel}-parameter from the histogram depicted in Fig. 5 for each τ_n. The histogram yields information about the probability of finding a phase in a certain interval, which is given by the bin width. However, the q_{rel}-parameter is defined in terms of the PDF $f\left(\Delta\theta^{(n)}, \tau_n\right)$. As such, we choose a suitable model to fit the histogram with. The model used is a wrapped Voigt profile

$$f_w(\phi,\mu,\sigma,\gamma) = \sum_{k=-\infty}^{\infty} V(\phi + 2\pi k, \mu, \sigma, \gamma), \tag{12}$$

where $V(\phi, \mu, \sigma, \gamma)$ is the uncentered Voigt profile, μ is the median of the uncentered profile, σ is the variance of the normal distribution, and γ is the scaling parameter of the Cauchy distribution. We fit the data using nonlinear regression and truncate the sum at $k = \pm 10$. We emphasize that the chosen model is part of the assumptions underlying the characterization. Another suitable model can be chosen to fit the histogram.

We recall that this method does not assume the phase shift to be constant over the pulse duration. We define the minimum q_{rel}-parameter as

$$q_{\mathrm{rel}}^{\min} = \min_{\tau_n} q_{\mathrm{rel}}(\tau_n), \tag{13}$$

where we recall that $q_{\mathrm{rel}}(\tau_n)$ is defined as the lower bound

$$f(\Delta\theta^{(n)}, \tau_n) \geq \frac{q_{\mathrm{rel}}(\tau_n)}{2\pi}. \tag{14}$$

We note that with enough samples, it may be possible to apply suitable concentration inequalities to directly determine the minimum of the PDF corresponding to the phase histogram, cf. Fig. 5, without making any model assumptions. By choosing a small enough bin width, one can assume that the phase distribution remains approximately constant within each bin. The drawback of this approach is that it requires substantially more samples to produce tight bounds.

This implies longer acquisition times, which may be experimentally challenging due to inevitable temperature fluctuations.

We will use the methods described in this section to determine the minimum q_{rel}-parameter $q_{\mathrm{rel}}^{\mathrm{min}}$ as a function of the optical power injected by Eve in Sec. III E. However, we first discuss a technical aspect related to the influence of the ML polarization on the degree of injection locking in Sec. III D.

D. Polarization-dependency of injection locking

In general, the amount of optical power coupling into the DUT laser cavity depends on the polarization of the injected light. Therefore, for optimal injection locking, the best polarization state of the injected light has to be found. With the light sources used in this work, we expect that the ML and SL light should match in polarization for the best coupling. However, our method does not rely on this assumption. To find the best polarization state (and, therefore, replicate Eve's best attack strategy), we measure the polarization of the ML light at the input of the SL (see Fig. 1) and simultaneously acquire the heterodyne detection signal.

This procedure is repeated for a series of polarization states to obtain a scan of the Poincaré sphere. For each point on the sphere, we determine the corresponding $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter following Sec. III C. The outcome is shown in Fig. 6(a). The polarization state associated with the smallest $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter can then be used for subsequent measurements of the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter, e.g., when modifying the attenuation between ML and SL using the VOA.[38] While this measurement provides the best polarization state for the injected light with minimal assumptions on the DUT, the process may take a considerable amount of time. As an example, the scan, whose results are depicted in Fig. 6(a), took around 5 h to complete. If possible, it is preferable to use a faster method to find the best polarization state.

Another method for finding the optimal polarization is to measure the power of the ML light reflected at the cavity of the SL while it is neither biased nor modulated. The intuition behind this method is that the active material is absorptive when the DFB laser is off. This way, we can determine how well the ML couples into the SL laser cavity. To confirm this, we measure the reflected light at the monitoring port while determining the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter as a function of the polarization state. Since reflections at the cavity are low, we used a single-photon detector (SPD) for this task (see Fig. 1). The result of this measurement is depicted in Fig. 6(b) and indicates that for the DFB lasers used in this work, the power of the reflected light is indeed lowest when the polarization state of the ML yields the smallest $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter, up to experimental uncertainty. Based on this result, we may now minimize the power of the reflected light to find the best polarization state of the injected light. This method is preferable if the DUT is a DFB laser, since it only takes in the order of minutes to find the optimal polarization, compared to hours for the first approach.

For the DFB lasers used in this work, both methods are equivalent and yield comparable results (cf. Fig. 6). However, if the DUT is a more complex optical system, it has to be verified that the above-mentioned methods can be used interchangeably. For example, if the DUT exhibits polarization dependent losses outside the laser cavity, the second method is not applicable in a straightforward manner, but the first method still is. To summarize, the first polarization optimization method is general and applicable for a broad range of DUTs but takes considerably longer to complete than the second method, i.e., analyzing the backreflections, which is, however, only limited to DUTs where the correlation between

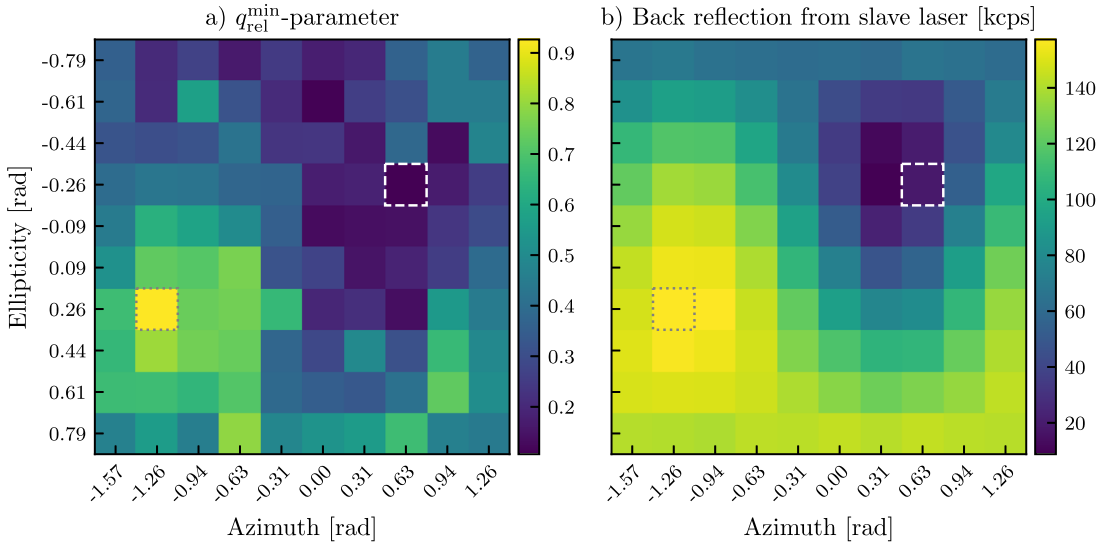

FIG. 6. $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter vs polarization state of the light injected into the slave laser. The dashed (dotted) lines mark the polarization states with minimum (maximum) $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter. The injected optical power was −55.3 dBm, measured at the input of the slave laser. (a) Heatmap of the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter vs polarization state of the injected light. (b) Heatmap of the single-photon detector count rate while measuring the reflected light at the slave laser cavity while the slave laser was turned off vs the polarization state of the injected light.

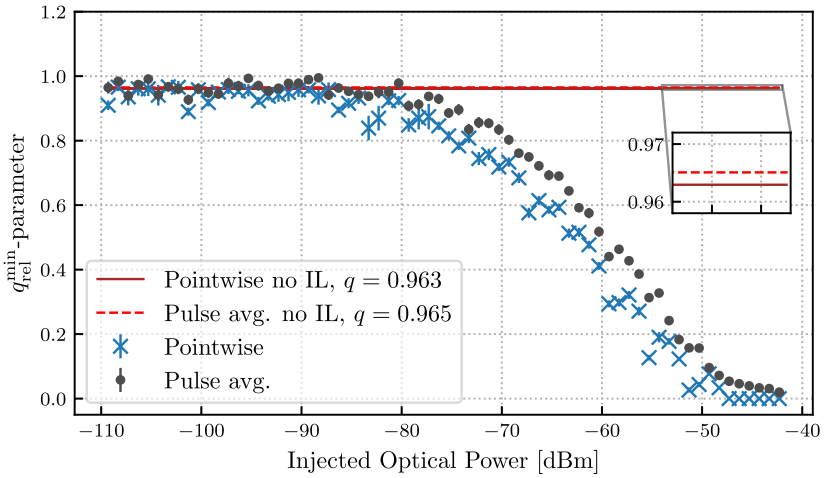

FIG. 7. Degree of phase de-randomization, quantified by the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter defined in Eq. (13), as a function of the optical power injected into the slave laser. "Pointwise" and "Pulse avg." refer to the two different methods for determining the phase (see Sec. III B). IL: injection locking.

backreflections and the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter is known. For all measurements discussed in the remainder of this work, we use the second method.

E. Maximum degree of injection locking

After determining the optimal polarization state of the ML following Sec. III E, we determine the minimum q_{rel}-parameter $q_{\mathrm{rel}}^{\mathrm{min}}$, cf. Sec. III C, as a function of the injected optical power for the optimal polarization. In order to achieve this, we incrementally increase the attenuation at the VOA, cf. Fig. 1, to simulate Alice's components (e.g., fixed attenuators, bandpass filters, isolators, etc.). The result is depicted in Fig. 7. For completeness, we also plot the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter resulting from integrating the homodyne detection signal, cf. Eqs. (9) and (10), over the pulse duration. We can see that, for the DFB lasers used in this work, the ML does not significantly influence the phase randomization of the SL if the injected optical power is below ∼−90 dBm.

The error bars for the $q_{\mathrm{rel}}^{\mathrm{min}}$-parameters depicted in Fig. 7 result from applying the bootstrapping method to the phase values obtained in the experiment.[39] We resampled the data 50 times. An additional source of error that is not accounted for in Fig. 7 is a drift in the difference in central frequencies of the ML and SL on a scale that cannot be resolved by the OSA used, which has a resolution of 0.05 nm.

When considering attacks based on light injection, the maximum optical power Eve can inject is commonly defined by the laser-induced damage threshold (LIDT) of the optical fiber.[12] Taking into account the total attenuation of Alice's components, this upper-bounds the optical power reaching Alice's laser. As an example, considering a standard telecommunication optical fiber with a laser-induced damage threshold of 100 W,[12] Alice requires at least about 140 dB of attenuation (in the direction opposite to the propagation of her pulses) in order to ensure Eve's injection-locking attack does not significantly affect the phase randomization of her laser, following Fig. 7. Note that the LIDT can be reduced by using a power-limiting device.[40] Other countermeasures to injection-locking attacks involve implementing watchdog detectors or polarization scramblers. However, these may open more loopholes than they close, as Eve can attack active countermeasures in a less predictable manner than passive countermeasures.

The injection-locking attack is closely related to the Trojan-horse attack, where Eve injects light into the transmitter and analyzes the backreflections carrying information about Alice's internal setting choices. Increasing the attenuation is a robust and commonly used countermeasure to both attacks. For comparison, following Ref. 10, about 200 dB of attenuation (back and forth, as opposed to one-way for injection-locking) is required to yield almost ideal key rates accounting for Trojan-horse attacks with a QKD system operating at 500 MHz and at 1550 nm. Following the results presented in this work, security against one attack does not necessarily imply security against the other. For example, systems implementing more optical isolators may be safe against injection-locking attacks but not against Trojan-horse attacks, while for systems implementing more fixed attenuators, the opposite may be true. Therefore, we recommend performing system-specific tests for both attacks.

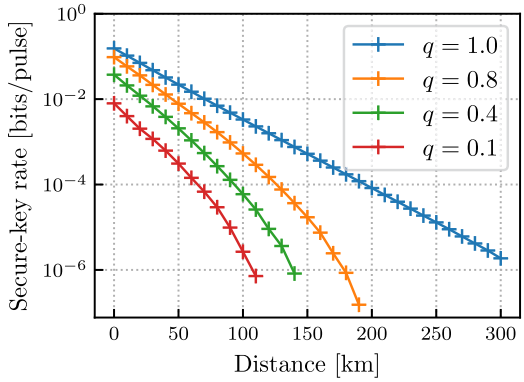

FIG. 8. Asymptotic secure-key rate vs distance for the three-state protocol with imperfect phase randomization for various q-parameters. The channel attenuation is assumed to be 0.16 dB km^{-1}.

We also note that Eve may reduce Alice's isolation in a laser-damage attack targeting the optical isolators and attenuators.[41] Following the results in Ref. 41, adding a sacrificial isolator as the last component before the quantum channel is sufficient to protect the components behind it from a laser-damage attack. Given that the attenuation of the sacrificial isolator is under Eve's control, it should not be taken into account as a countermeasure to other attacks, such as injection-locking and the Trojan-horse attack.

The impact of imperfect phase randomization on the achievable secure-key rate is depicted in Fig. 8 for the three-state protocol in the asymptotic limit and with ideal detectors using the freely available code from Ref. 25. While the secure-key rate significantly drops at long distances with decreasing q-parameter, a secure key can still be established at short distances with $q = 0.1$.

As discussed in Sec. III A, we recall that an important aspect of the proposed method is its reliance on the ML's ability to simulate Eve's optimal attack, which fundamentally limits the characterization. Without further assumptions and with current security proofs necessitating at least a partial characterization of the phase distribution, developing a method to characterize the maximum degree of injection locking without dependency on the ML used is both challenging and requires further experimental and theoretical investigation.

We note that the methods described in this work can be used to evaluate QKD systems against injection-locking attacks by means of black-box testing. In this case, we replace the slave laser in Fig. 1 by the QKD system under test and inject light with the optimal polarization state, which is determined following the discussion in Sec. III D. The QKD system should be operated so as to facilitate the evaluation and simulate the best possible scenario for Eve. For example, we turn off any modulation of components other than the laser, e.g., intensity modulators and VOAs, to ensure that only the gain-switching of the laser shows a time-dependency, and set any component affecting the attenuation of Alice's setup to the highest transmission that can arise during operation. We then verify that for the maximum chosen optical power injected, the resulting $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter is greater than the q-parameter and/or $q_{\mathrm{rel}}^{\mathrm{min}}$-parameter provided by the implementer. Indeed, by definition, $q_{\mathrm{rel}}^{\mathrm{min}} \geq q$ and $q_{\mathrm{rel}}^{\mathrm{min}} \to q$ in the limit of an ideal attack, cf. Sec. III B.

IV. CONCLUSION

We have presented a general method to determine the maximum degree of phase de-randomization Eve can induce from an injection-locking attack, quantified by the q_{rel}-parameter. This approach is source-agnostic, making it applicable to any QKD system that uses optical pulses, e.g., those implementing the decoy-state BB84 protocol.[6,8] An important feature of our method is that its effectiveness in characterizing the maximum degree of injection locking is directly given by how well the master laser can emulate Eve's optimal attack strategy.

Using the DFB lasers in this work, we observed that a minimum attenuation of ~140 dB is required to largely protect Alice from an injection-locking attack. However, it is crucial to perform system-specific characterizations for each QKD implementation, as the vulnerability to such attacks can vary drastically depending on the light source employed. Compared to other related side-channel attacks, such as the Trojan-horse attack, our results show that security against one attack does not necessarily imply security against the other, further underlying the importance of performing system-specific tests. We believe our methods remain valid for a broad range of master lasers and DUTs. The methods presented in this work can be used for black-box testing, serving as a valuable tool for evaluating QKD systems against injection-locking attacks.

Finally, we emphasize that while evaluating QKD systems against side-channel attacks is certainly an important step toward certifiable (and certified) QKD systems, device imperfections (e.g., injection locking) must be thoroughly characterized and/or rigorously taken into account in the security proof. Following the discussions in this work, the next step is to determine the maximum degree of injection locking that Eve can induce *independently* of the devices used to perform the characterization.

ACKNOWLEDGMENTS

We acknowledge Hugo Zbinden and Margarida Pereira for fruitful discussions. We acknowledge Shlok Nahar, Twesh Upadhyaya, and Norbert Lütkenhaus for making their simulation code publicly available. The authors are subcontractors in the EC funded project, Nostradamus, Topic ID: CNECT/2023/OP/0032. It is the goal of Nostradamus to describe the blueprint for a testing and validation infrastructure to enable the evaluation and certification of QKD devices and related technologies, as well as to implement and operate a prototypical testbed facility to offer initial evaluation services, which are mandatory for the accreditation from a European security authority. The authors would like to acknowledge the whole project team for the support and valuable exchange. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them. This work was supported by the Galician Regional Government (consolidation of Research Units: AtlantTIC), MICIN with funding from the European Union NextGenerationEU (Grant No. PRTR-C17.I1), and the Galician Regional Government with its own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication, the European Union's Horizon Europe Framework Program under the project "Quantum Security Networks Partnership" (QSNP, Grant Agreement No. 101114043), and the "Hub Nacional de Excelencia en Comunicaciones Cuánticas" funded by the Ministerio para la Transformación Digital y de la Función Pública and the European Union NextGenerationEU.

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

Jerome Wiesemann and Fadri Grünenfelder contributed equally to this paper.

D.R. and N.W. supervised the research. J.W. and F.G. performed the research. D.R. assisted and supported the research. A.B.C.

provided part of the setup and assisted in building the setup. F.G. and J.W. analyzed the data. J.W. and F.G. wrote the paper. All authors participated in discussions and reviewed the paper.

Jerome Wiesemann: Conceptualization (equal); Data curation (equal); Formal analysis (equal); Investigation (lead); Methodology (equal); Software (equal); Validation (equal); Visualization (equal); Writing – original draft (lead); Writing – review & editing (lead). **Fadri Grünenfelder**: Conceptualization (equal); Data curation (equal); Formal analysis (lead); Investigation (equal); Methodology (equal); Resources (equal); Software (equal); Supervision (supporting); Validation (lead); Visualization (equal); Writing – original draft (lead); Writing – review & editing (lead). **Ana Blázquez Coído**: Conceptualization (supporting); Investigation (supporting); Methodology (supporting); Resources (supporting). **Nino Walenta**: Conceptualization (equal); Formal analysis (supporting); Funding acquisition (lead); Project administration (lead); Supervision (equal); Writing – review & editing (equal). **Davide Rusca**: Conceptualization (equal); Formal analysis (supporting); Funding acquisition (lead); Methodology (supporting); Project administration (lead); Resources (equal); Supervision (lead); Validation (lead); Writing – review & editing (supporting).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author upon reasonable request.

APPENDIX A: DIAGONAL FORM OF THE SIGNAL DENSITY MATRIX

The density matrix representation from Eq. (2) follows from Eq. (1) if the phases are uniformly distributed, i.e., $f(\theta) = 1/(2\pi)$. To see this, we recall that a coherent state of one mode of the electromagnetic field can be written as a superposition of Fock states[34]

$$|\alpha\rangle = \sum_{n=0}^{\infty} e^{-|\alpha|^2/2} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{A1}$$

We can now write $|\alpha\rangle = |\sqrt{\mu} e^{i\theta}\rangle$, where μ is the mean photon number and θ denotes the phase of the state. Plugging this expression into Eq. (1), where $f(\theta)$ describes a uniform distribution, yields

$$\rho_\mu = \int_0^{2\pi} \frac{d\theta}{2\pi} \sum_{n=0}^{\infty} \sum_{m=0}^{\infty} e^{-\mu} e^{i(n\theta - m\theta)} \frac{\sqrt{\mu}^n \sqrt{\mu}^m}{\sqrt{n!m!}} |n\rangle\langle m|. \tag{A2}$$

Identifying the representation of the Kronecker delta $\delta_{nm} = (2\pi)^{-1} \int_0^{2\pi} d\theta e^{i(n\theta - m\theta)}$ results in

$$\rho_\mu = \sum_n e^{-\mu} \frac{\mu^n}{n!} |n\rangle\langle n|, \tag{A3}$$

which corresponds to a coherent superposition of Fock states, i.e., Eq. (2), and shows that the density matrix is diagonal in the Fock basis.

APPENDIX B: LIST OF COMPONENTS

We list all the components used to perform the characterization, i.e., the components depicted in Fig. 1, as follows:

- Master laser: Gooch and Housego AA0701-193414-010-SM900-FCA-50 1550 nm.
- Slave laser: LP-PD LP-ML1001A-55-FA.
- Optical spectrum analyzer: Yokogawa Spectrum Analyzer AQ6375E-10-L1-F/FC/RFC.
- Polarimeter: Thorlabs PAX1000IR2/M.
- Balanced detectors: Thorlabs PDB480C-AC.
- Manual polarization controller: Thorlabs FPC560.
- Motorized polarization controller: Thorlabs MPC320.
- Programmable temperature controller: Stanford research systems PTC10.
- Single-photon avalanche diode: IDQube-NIR-FR-MMF-LN.
- Arbitrary waveform generator: Tektronix AFG31102.
- Variable optical attenuator: EXFO FVA-600.
- Mixed signal oscilloscope: Tektronix MSO64B 6-BW-4000 Installed Option, 4 GHz Bandwidth.
- 90° optical hybrid: iXblue COH24.
- Laser diode controller: Newport LDX-3412-240V.
- Circulator: Thorlabs 6015-3-APC.

APPENDIX C: HOMODYNE DETECTION SIGNAL

Assume generic electric fields $\boldsymbol{E}_S(t)$ and $\boldsymbol{E}_{LO}(t)$ at a point in space for the signal and local oscillator. Following their interference, the measured intensities at both arms of the interferometer are

$$I_1(t) = \frac{1}{2} |\boldsymbol{E}_S(t) + \boldsymbol{E}_{LO}(t)|^2, \tag{C1}$$

$$I_2(t) = \frac{1}{2} \left|\boldsymbol{E}_S(t) + e^{i\pi} \boldsymbol{E}_{LO}(t)\right|^2, \tag{C2}$$

and the resulting homodyne detection signal is $I_0(t) = I_1(t) - I_2(t)$. Here, we assume perfectly balanced detectors. Now, if a 90° optical hybrid is used as in Fig. 1, then the electric fields in the arms are

$$I_3(t) = \frac{1}{2} \left|e^{-i\frac{\pi}{2}} \boldsymbol{E}_S(t) + \boldsymbol{E}_{LO}(t)\right|^2, \tag{C3}$$

$$I_4(t) = \frac{1}{2} \left|\boldsymbol{E}_S(t) + e^{-i\frac{\pi}{2}} e^{i\pi} \boldsymbol{E}_{LO}(t)\right|^2, \tag{C4}$$

which leads to a homodyne detection signal $I_{\pi/2}(t) = I_3(t) - I_4(t)$.

APPENDIX D: TIME WINDOW FOR q_{rel}-PARAMETER DETERMINATION

The sum of the squared residuals is defined as

$$S^2 = \sum_{n=1}^{N} \left(f_w(\Delta\theta_n, \mu_{opt}, \sigma_{opt}, \gamma_{opt}) - c_n\right)^2, \tag{D1}$$

where $\Delta\theta_n$ is $\Delta\theta^{(n)}$ (τ_n) evaluated at the time that minimizes q_{rel}^{min}, c_n is the amount of counts in the nth histogram bin (an example is shown in Fig. 5), and μ_{opt}, σ_{opt}, and γ_{opt} are the optimal parameters found by the non-linear regression fit when determining q_{rel}^{min}.

To determine the minimum q_{rel}-parameter q_{rel}^{min}, cf. Eq. (13), we selected the time window highlighted in light blue in Fig. 3. This

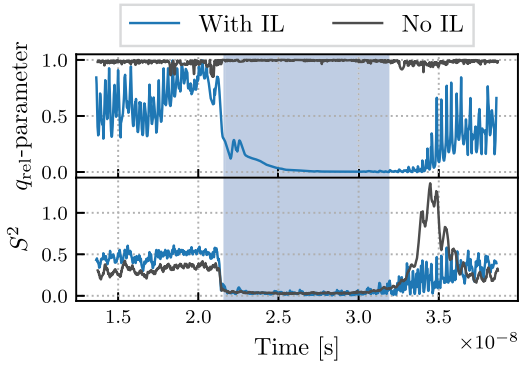

FIG. 9. q_{rel}-parameter and sum of squared residuals S^2. The time window for the determination of the q_{rel}-parameter is shaded in light blue.

selection ensures that our model, described in Eq. (12), agrees with the observed data and produces reliable results. The goodness of the fit is quantified by the sum of the squared residuals S^2, and its behavior with respect to the time τ_n is shown in Fig. 9, together with the q_{rel}-parameter.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of International Conference on Computers, Systems & Signal Processing Bangalore, India, Dec. 9–12, 1984 (IEEE Computer Society Press, 1984), pp. 175–179; reprinted in Theor. Comput. Sci. **560**, 7–11 (2014).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).

[3] 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**, 1301–1350 (2009).

[4] R. Renner, "Security of quantum key distribution," arXiv:quant-ph/0512258 (2005).

[5] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nat. Commun. **3**, 634 (2012).

[6] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, "Concise security bounds for practical decoy-state quantum key distribution," Phys. Rev. A **89**, 022307 (2014).

[7] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum **1**, 14 (2017).

[8] D. Rusca, A. Boaron, F. Grünenfelder, A. Martin, and H. Zbinden, "Finite-key analysis for the 1-decoy state QKD protocol," Appl. Phys. Lett. **112**, 171104 (2018).

[9] V. Zapatero, Á. Navarrete, and M. Curty, "Implementation security in quantum key distribution," arXiv:2310.20377 [quant-ph] (2023).

[10] G. Currás-Lorenzo, M. Pereira, G. Kato, M. Curty, and K. Tamaki, "Security of high-speed quantum key distribution with imperfect sources," arXiv:2305.05930 [quant-ph] (2025).

[11] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, "An approach for security evaluation and certification of a complete quantum communication system," Sci. Rep. **11**, 5110 (2021).

[12] V. Makarov, A. Abrikosov, P. Chaiwongkhot, A. K. Fedorov, A. Huang, E. Kiktenko, M. Petrov, A. Ponosova, D. Ruzhitskaya, A. Tayduganov, D. Trefilov, and K. Zaitsev, "Preparing a commercial quantum key distribution system for certification against implementation loopholes," arXiv:2310.20107 (2023).

[13] BSI, "A study on implementation attacks against QKD systems," Technical Report, German Federal Office for Information Security, 2024.

[14] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus, "Phase error rate estimation in QKD with imperfect detectors," arXiv:2408.17349 [quant-ph] (2025).

[15] X. Sixto, Á. Navarrete, M. Pereira, G. Currás-Lorenzo, K. Tamaki, and M. Curty, "Quantum key distribution with imperfectly isolated devices," arXiv:2411.13948 [quant-ph] (2024).

[16] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, and Z.-F. Han, "Experimental demonstration of fully passive quantum key distribution," Phys. Rev. Lett. **131**, 110802 (2023).

[17] M. Curty, X. Ma, H.-K. Lo, and N. Lütkenhaus, "Passive sources for the Bennett-brassard 1984 quantum-key-distribution protocol with practical signals," Phys. Rev. A **82**, 052325 (2010).

[18] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).

[19] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).

[20] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," arXiv:quant-ph/0212066 [quant-ph] (2004).

[21] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).

[22] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).

[23] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).

[24] X. Sixto, G. Currás-Lorenzo, K. Tamaki, and M. Curty, "Secret key rate bounds for quantum key distribution with faulty active phase randomization," EPJ Quantum Technol. **10**, 53 (2023).

[25] S. Nahar, T. Upadhyaya, and N. Lütkenhaus, "Imperfect phase-randomisation and generalised decoy-state quantum key distribution," Phys. Rev. Appl. **20**, 064031 (2023); arXiv:2304.09401 [quant-ph].

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

[27] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, "Hacking quantum key distribution via injection locking," Phys. Rev. Appl. **13**, 034008 (2020).

[28] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **12**, 064043 (2019).

[29] X.-X. Zhang, M.-S. Jiang, Y. Wang, Y.-F. Lu, H.-W. Li, C. Zhou, Y. Zhou, and W.-S. Bao, "Analysis of an injection-locking-loophole attack from an external source for quantum key distribution," Phys. Rev. A **106**, 062412 (2022).

[30] V. Lovic, D. G. Marangon, P. R. Smith, R. I. Woodward, and A. J. Shields, "Quantified effects of the laser-seeding attack in quantum key distribution," Phys. Rev. Appl. **20**, 044005 (2023).

[31] G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, K. Tamaki, and M. Curty, "Security of quantum key distribution with imperfect phase randomisation," Quantum Sci. Technol. **9**, 015025 (2024); arXiv:2210.08183 [quant-ph].

[32] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," arXiv:quant-ph/0610203 [quant-ph] (2007).

[33] J. Wiesemann, J. Krause, D. Tupkary, N. Lütkenhaus, D. Rusca, and N. Walenta, "A consolidated and accessible security proof for finite-size decoy-state quantum key distribution," arXiv:2405.16578 [quant-ph] (2024).

[34] R. J. Glauber, "Coherent and incoherent states of the radiation field," Phys. Rev. **131**, 2766–2788 (1963).

[35] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, "Discrete-phase-randomized coherent state source and its application in quantum key distribution," New J. Phys. **17**, 053014 (2015).

[36]F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, "Performance and security of 5 GHz repetition rate polarization-based quantum key distribution," Appl. Phys. Lett. **117**, 144003 (2020).
[37]Alternatively, the phase fluctuations may be characterized, and the resulting phase distribution adjusted accordingly.
[38]Importantly, it has to be ensured that modifying the VOA attenuation does not affect the polarization state of the ML. Otherwise, the best polarization state must be determined for each attenuation individually, following the methods described in this section.
[39]S. Huet, A. Bouvier, M.-A. Poursat, and E. Jolivet, *Statistical Tools for Nonlinear Regression: A Practical Guide with S-PLUS and R Examples* (Springer-Verlag, 2004).
[40]G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, and C. C. W. Lim, "Securing practical quantum communication systems with optical power limiters," PRX Quantum **2**, 030304 (2021).
[41]A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, and A. Huang, "Protecting fiber-optic quantum key distribution sources against light-injection attacks," PRX Quantum **3**, 040307 (2022).