Characterization of State-Preparation Uncertainty in Quantum Key Distribution

Anqi Huang[1,*] Akihiro Mizutani,[2] Hoi-Kwong Lo,[3,4,5] Vadim Makarov,[6,7,8] and Kiyoshi Tamaki[9]

[1]*Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer Science and Technology, National University of Defense Technology, Changsha 410073, People's Republic of China*

[2]*Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan*

[3]*Department of Electrical & Computer Engineering and Department of Physics, Centre for Quantum Information and Quantum Control (CQIQC), University of Toronto, Toronto, Ontario M5S 3G4, Canada*

[4]*Department of Physics, University of Hong Kong, Pokfulam, Hong Kong*

[5]*Quantum Bridge Technologies, Inc., 100 College Street, Toronto, Ontario M5G 1L5, 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*

[9]*Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*

To achieve secure quantum key distribution, all imperfections in the source unit must be incorporated in a security proof and measured in the lab. Here we perform a proof-of-principle demonstration of the experimental techniques for characterizing the source phase and intensity fluctuation in commercial quantum key distribution systems. When we apply the measured phase-fluctuation intervals to the security proof that takes into account fluctuations in the state preparation, it predicts a key distribution distance of over 100 km of fiber. The measured intensity fluctuation intervals are, however, so large that the proof predicts zero key, indicating a source improvement may be needed. Our characterization methods pave the way for a future certification standard.

I. INTRODUCTION

Quantum key distribution (QKD), which guarantees information-theoretically secure communication in theory, has become one of the most widely applied techniques of quantum information processing [1,2]. However, practical imperfections in devices challenge the theoretically guaranteed security during QKD global-scale deployment [3–12]. Fortunately, a measurement-device-independent (MDI) QKD protocol [13] is immune to all measurement-side secure loopholes, because this protocol does not make assumption on the measurement devices. Thus, the loopholes in the source unit are the last obstacle to achieve security of QKD in reality [8,9,14–16]. The most effective solution to eliminate such a security threat is to consider the practical imperfections of the source in the security model.

The most widely used ideal source model is the one that emits only a single photon without encoding errors, and based on this model, numerous security proofs have

been made [17–19]. Unfortunately, however, this model does not properly reflect the actual properties of practical sources. One imperfection is that a practical source sometimes emits multiple photons. Another is that an encoding operation inevitably entails modulation inaccuracies owing to limited precision of experimental devices. These imperfections must be incorporated in the security proofs. Thanks to the invention of the decoy-state method [20–22], where Alice probabilistically varies the mean photon number of phase-randomized coherent light and it only matters that the source has a sufficiently large portion of single-photon emission, we can remove the requirement of the single-photon source [23]. To tackle the encoding inaccuracies, two approaches have been proposed. The first one is to take this into account by considering the fidelity between the Z- and X-basis states [24–26]. The second one is to employ a loss-tolerant protocol where basis-mismatched events are exploited besides the basis-matched ones for a better estimation of leaked information [27–29]. The loss-tolerant protocol has a remarkable property that the secret key is tolerant to the channel loss even if the source emits a state deviated from the expected one.

---

*angelhuang.hn@gmail.com

Owing to this advantage, this protocol has attracted intensive attention in theory [30–33] and experiment [30,34]. The original loss-tolerant protocol [27] has been made more practical by generalizing it to the case where Alice knows only the intervals of the phase and intensity fluctuations of the coherent source [32,33]. Long-distance QKD using the loss-tolerant protocol has been realized under realistic intervals of phase and intensity fluctuations [30,31,33,35,36].

To apply these security proofs to calculate the key rate of a running QKD system, one obtains some parameters from the QKD system during raw key exchange as the inputs of the calculation. For instance, the detection gain and qubit error rate (QBER) should be observed in order to calculate the secure key rate in the decoy-state protocol [21]. Similarly, the trace distance should be known before quantifying the amount of leaked information from the source [15,37]. For the imperfect state encoding, the fluctuation or deviation of state modulation should be characterized as a crucial value for key-rate calculation. Reference [30] experimentally measures the averaged phase deviation of modulation and applies it to the loss-tolerant protocol [27] with finite-size analysis. However, there is no methodology so far to characterize the fluctuation interval of the imperfect modulation in a practical QKD system [33].

Here we propose two methods of experimentally characterizing fluctuation, one for phase and another for intensity. We apply each of them to a QKD system to obtain the intervals of phase and intensity fluctuation. By following the loss-tolerant protocol in Ref. [33], we treat the optical pulses that lie in this interval as untagged signals and the others as tagged signals. Note that the secret key is extracted from the untagged signals, and the information of the tagged signals is completely leaked to an eavesdropper. The simulation shows that secret key can be produced between Alice and Bob over more than 100 km of fiber with 10^{13} pulses sent, when the phase fluctuation is only considered. However the measured intensity fluctuation is too large for the secret key to be produced, owing to the relatively unstable type of source used in the QKD system we test (a gain-switched semiconductor laser). We therefore simulate performance of a system that has the actual measured phase fluctuation and a fraction of the measured intensity fluctuation, to demonstrate how much the source has to be improved.

The rest of this article is organized as follows. In Sec. II we state all the assumptions on the QKD system in our method. Section III presents the methodology of characterizing the phase fluctuation on an experimental example of a modified Clavis2 QKD system from ID Quantique. Section IV presents the methodology of characterizing the intensity fluctuation on a different prototype QKD system. The experimentally obtained values of phase and intensity fluctuation are applied to the security proof in Sec. V. We conclude in Sec. VI.

II. ASSUMPTIONS IN EXPERIMENTS

To characterize the uncertainty of state preparation, the intervals of phase fluctuation are measured on a commercial plug-and-play phase-encoding QKD system Clavis2 from ID Quantique [38]. Since no decoy states are employed in the Clavis2 system, the intervals of intensity fluctuation are measured on another prototype QKD system running a decoy-state BB84 protocol with polarization encoding. The phase and intensity intervals are measured on two separate QKD systems because we have had no access to a QKD system that employs a phase-encoding loss-tolerant protocol with decoy-state method. However, the methodology of characterization proposed in this work is general and applicable to the loss-tolerant QKD systems.

The phase and intensity fluctuations are considered in the security proof proposed in Ref. [33]. For those not familiar with the security model in Ref. [33], the framework is recapped in Appendix A. In this security proof, the source's phase and intensity fluctuation falls within a phase interval R_{ph}^{c} and intensity interval R_{int}^{k} with probability at least $(1 - p_{\mathrm{fail}})$. A value outside either R_{ph}^{c} or R_{int}^{k} is regarded as an error, which happens with probability at most p_{fail}. Given a mean value m of the phase or intensity for a certain state the source prepares, the interval may be defined as $(1 \pm x\%/100\%) m$, or briefly $\pm x\%$, where x is an arbitrary factor. If a statistical distribution of the emitted states is measured and found to be Gaussian, as is the case in our experiments, the interval may alternatively be defined as $m \pm y\sigma$, or briefly $\pm y\sigma$, where σ is the standard deviation and y an arbitrary factor. The error probability p_{fail} has to be a small value, usually on the order of 10^{-9}. These are the only two parameters required by the proof.

In order to ensure our characterization is valid, below we summarize all the assumptions we make in the experiments.

(1) The phase and intensity values obtained by measuring bright pulses with classical photodetectors are identical to these of pulses attenuated to a single-photon level.

(2) The laser generates single-mode pulses with the randomized common phase of signal and reference pulses, which corresponds to Assumption (A1) in Appendix A.

(3) The phase distribution for each choice of $c^{i} \in \mathcal{C} := \{0_{Z}, 1_{Z}, 0_{X}\}$ and the intensity distribution for each choice of $k^{i} \in \mathcal{K} := \{k_{1}, k_{2}, k_{3}\}$ are identically and independently distributed, although our security model can handle the setting-choice-independent correlation (SCIC) that is explained in (A2) in Appendix A.

(4) The classical photodetectors are well characterized to linearly convert optical power to electrical voltage, and the oscilloscopes measure the input electrical voltage linearly.

(5) In our experiment, we first measure the phase value in each of about 10^{5} samples (or intensity value in $1.5 \times$

10^5 signal and 2.5×10^4 decoy and vacuum states each). Then we plot the resulting phase (or intensity) distributions. For simplicity, we assume that these sample sizes are large enough to ignore statistic noise.

(6) The phase $\theta_A = 0$ is assumed to be a reference state, relative to which the other states are encoded. We then characterize the noise at $\theta_A = 0$ and remove it from the other states. This removes both fluctuation introduced by the remaining parts of the experiment and any possible fluctuation of the reference state itself. Regarding intensity modulator (IM), it is assumed to be free of fluctuation when the QKD system is powered on but does not run a raw-key exchange. The measured results for the case of no key exchange then characterize the fluctuation from the remaining parts of the experiment. Also, we assume that these fluctuations are the same during our measurements of the other values of θ_A or intensity. Therefore, we can use a signal-processing technique to remove the noise.

(7) The filtering technique of singular-value-decomposition (SVD; see Appendix B) is assumed to work sufficiently well to remove most of the noise and output distributions of phase and intensity that are close to the real ones.

(8) The fluctuation measured from the nonrandom phase modulation is assumed to be identical to that of random phase modulation during the stage of raw-key exchange in QKD protocol.

III. EXPERIMENT OF PHASE CHARACTERIZATION

In this work, we first focus on the experimental characterization of phase fluctuation. The characterized phase interval R_{ph}^c is applied to estimate the upper bound on the number of phase errors per Eq. (24) in Ref. [33]. In order to study the methodology of fluctuation measurement and have a rough idea about the values of phase-fluctuation

interval R_{ph}^c in practical QKD systems, we conduct a proof-of-principle measurement to characterize this parameter. The phase interval R_{ph}^c is measured in the commercial QKD system Clavis2 from ID Quantique [38], which is a plug-and-play scheme [39,40]. Of note, this scheme is quite suitable to measure the phase value, because it is inherently stable without active calibration—the phase drift, polarization birefringence, and laser-intensity fluctuations are automatically compensated.

The Clavis2 system works as follows (see Fig. 1). To avoid confusion, we call Bob in this system as Charlie hereafter, who performs the characterization of phase fluctuation instead of acting as the receiver of a running QKD system like Bob. The laser emits linear-polarization pulses in a single mode with randomized phases at the repetition rate of 5 MHz. Each pulse then splits to be two pulses (signal pulse in the long arm and reference pulse in the short arm with 50 ns timing difference), combined and sent to Alice via an optical fiber. At this point, the signal and reference pulses are in the vertical and the horizontal polarizations, respectively. Alice modulates only the phase of the signal pulse, reflects both pulses with a Faraday mirror (FM), and sends them back to Charlie after attenuating the pulses to single-photon level. Charlie modulates the phase of the reference pulse (that is now routed into the long arm), and then the interfered signals are detected by two single-photon detectors (SPDs). The delay line in Alice is used to store a packet of 1700 incoming pulse pairs (called a frame), thus avoiding an intersection between the incoming and reflected pulses in the quantum channel.

In the experiment, we would like to characterize the phase fluctuation R_{ph}^c of the built-in PM in Alice in the Clavis2 system. Note that the previous work in Ref. [30] measured only the mean value of the modulated phase, but not its distribution. In order to measure the latter, we modify Bob in Clavis2 to be a Charlie module as shown in Fig. 2, which acts as a characterization apparatus. We design this measurement apparatus accordingly to apply
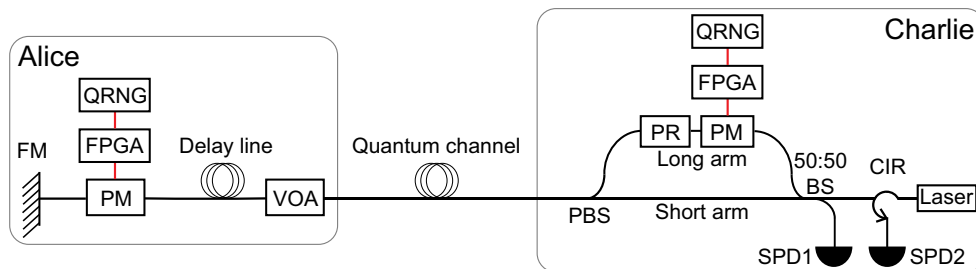

FIG. 1. Scheme of Clavis2 plug-and-play QKD system. Alice's PM controlled by a field-programmable gate array (FPGA) randomly applies a phase $\theta_A \in \{0, \pi/2, \pi, 3\pi/2\}$, and Charlie's PM controlled by another FPGA randomly applies a phase $\theta_B \in \{0, \pi/2\}$. The quantum random-number generators (QRNGs) provide random numbers to the FPGAs, in order to randomly select the phases. The 90° polarization rotator (PR) in Charlie is not a discrete component but is implemented by effectively "twisting" the fiber in the plane of the drawing, such that the light polarizations in the two arms become orthogonal at the PBS. In practice, this is achieved by aligning the axes of the polarization-maintaining fiber pigtails appropriately between the PBS and PM. SPD, single-photon detector; BS, beam splitter; PBS, polarization beam splitter; FM, Faraday mirror; CIR, circulator; VOA, variable optical attenuator.
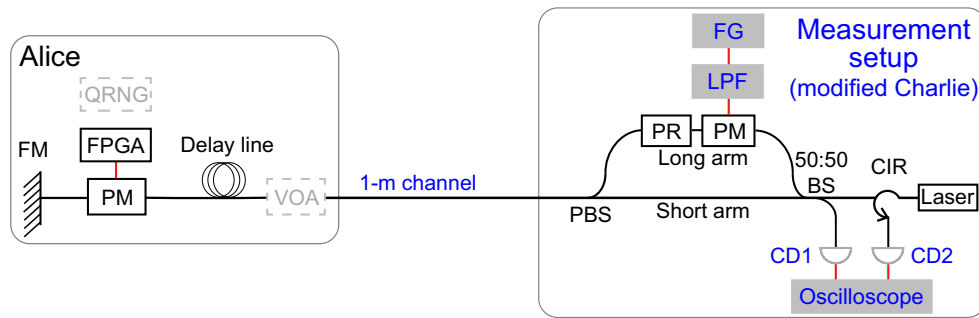
FIG. 2.   Setup for phase-distribution measurement. Alice and Charlie are connected by a 1-m fiber. The device under test, Alice's phase modulator (PM), is still controlled by the FPGA in the system, and Charlie's PM is controlled by an external function generator (FG). The replacements required for this measurement are highlighted in gray; the VOA and the QRNG in Alice are inactivated. See text for details. CD, classical photodetector (optical-to-electrical converter); LPF, low-pass filter.

a stable, calibrated, passively low-pass-filtered phase shift to the entire frame of the incoming light pulses to do a correct measurement. In this figure, replacements are highlighted in gray, and inactivated components are in gray dashed boxes. In order to obtain pulses with high intensities, we set Alice's VOA to its lowest possible setting (about 2 dB). The SPDs at the outputs of Charlie's interferometer are replaced with two classical optical-to-electrical (O/E) converters (LeCroy OE455 with 3.5-GHz electrical bandwidth) connected to an oscilloscope (LeCroy 760Zi with 6-GHz analog bandwidth and 20-GHz sampling rate). In order to separately measure the distribution of each phase value, we inactivate the QRNG in Alice and apply the same phase value to every pulse. Charlie's PM is controlled by an external function generator (FG; Highland Technology P400) to provide a stable, fluctuation-free phase $\theta_B \in \{0, \pi/2\}$. We explain this point in more detail later. A passive low-pass filter (LPF) with 20-kHz cutoff is inserted between the output of the function generator and Charlie's PM, ensuring a low-noise electrical signal at the latter. Note that in the plug-and-play system used here, one cannot simply apply a static phase shift in the modified Charlie, as it would have canceled out when the frame of light pulses goes out of Charlie then returns. However, a single long phase-shifting electrical pulse externally applied at the modified Charlie's PM well in advance of the returning frame is sufficient to perform an accurate measurement in this system configuration.

The procedure of the experiment is as follows.

Stage 0. Preset.

This stage mainly focuses on preparing the electronic signal applied to Charlie's PM to serve a stable modulation, which ensures the fluctuation we later measure in the experiment is only from Alice's PM, but not from that of Charlie. When a frame of pulses comes back to Charlie, the function generator applies a 500-μs-long voltage pulse that covers the entire 350-μs frame, avoiding frequent rising and falling edges and thus avoiding oscillations in the voltage. Also, this voltage pulse is applied slightly before

the frame and ends after the frame. Thus, no optical pulse is modulated during the rising and falling edges of the voltage pulse, and an identical phase is applied to all the optical pulses in the frame. Furthermore, the 20-kHz-bandwidth LPF mitigates small fluctuation due to any electronic noise, resulting in a steady voltage level. This strategy of providing a stable modulation to Charlie's PM is applied to both the following calibration and measurement. However, we cannot adopt this technique to Alice's PM because the phase is not randomly modulated pulse by pulse, which does not satisfy the fundamental assumption of QKD.

Stage 1. Calibration.

Calibration is necessary to perform precise measurement and determine the voltage value applied to Charlie's PM for $\theta_B = \pi/2$. First, we set both $\theta_A = 0$ and $\theta_B = 0$. Ideally, this would result in a full interference: CD2 receives all the energy, but zero energy measured by CD1. However, in practice, the energy detected by CD1 is not zero, due to imperfect alignment between Alice and Charlie. Thus, we denote the output energy at CD1 under this misalignment by $D_{1,\min}$, meanwhile the output energy measured by CD2 is maximum, denoted by $D_{2,\max}$. Then we keep $\theta_A = 0$ and scan the voltage applied to Charlie's PM. During the scanning, the maximum output energy measured by CD1 is denoted by $D_{1,\max}$, and at this moment the output energy measured by CD2 is minimum, denoted by $D_{2,\min}$. It is notable that $D_{2,\max}$ is slightly smaller than $D_{1,\max}$ because the circulator between the interferometer's output and CD2 introduces loss. A ratio $R = D_{1,\max}/D_{2,\max}$ quantifies this extra loss, which we compensate in the phase calculation in Stage 3.

To obtain a precise voltage for $\theta_B = \pi/2$, we gradually increase the voltage applied to Charlie's PM from zero (while keeping $\theta_A = 0$), until we detect the energy of $(D_{1,\max} - D_{1,\min})/2$ at CD1 and the energy of $(D_{2,\max} - D_{2,\min})/2$ at CD2. These happen simultaneously. This moment implies the relative phase between Alice and Charlie is $\pi/2$. Since we have set $\theta_A = 0$, we can deduce that $\theta_B = \pi/2$.

After this calibration, we perform the following stages for each phase value $\theta_A \in \{0, \pi/2, \pi\}$.

Stage 2. Measurement.

In order to measure the fluctuation of each θ_A, Alice's PM modulates every pulse individually but applies the same phase. Charlie's PM applies either $\theta_B = 0$ (for Alice's phase $\theta_A = \pi/2$) or $\theta_B = \pi/2$ (for $\theta_A = 0$ or π) to ensure that phase difference between Alice and Charlie is always $\pi/2$ no matter which θ_A Alice selects. The $\pi/2$ working point is necessary for the measurement, because at the 0 and π points of full interference, the derivative of the output energy would tend to zero and not allow phase extraction. On the other hand, the point at $\pi/2$ can provide the maximal derivative of the output energy as a function

of the phase, allowing us to perform an accurate measurement. Typical waveforms measured by CD1 and CD2 are shown in Fig. 3. The measured energy of each pulse is calculated by integrating the power between the gray lines. The whole system keeps running until we collect 10^5 pulses for each phase value.

Stage 3. Phase calculation.

Let us denote the energy measured by the two detectors as D_{1,θ_A} and D_{2,θ_A}. The value of the actual phase, θ'_A, can be calculated after we compensate the extra loss for CD2 by multiplying its energy by the ratio R obtained at Stage 1 and subtract the global misalignment between Alice and Charlie. Thus, the phase deviation δ between the real phase θ'_A and the ideal phase θ_A can be calculated as [41]

$$\delta = \theta'_A - \theta_A = \begin{cases} 2 \arctan\left(-\sqrt{\dfrac{D_{1,\theta_A} - D_{1,\min}}{R\left(D_{2,\theta_A} - D_{2,\min}\right)}}\right) - \Delta, & \text{if } \theta'_A - \theta_B < 0 \\ 2 \arctan\sqrt{\dfrac{D_{1,\theta_A} - D_{1,\min}}{R\left(D_{2,\theta_A} - D_{2,\min}\right)}} - \Delta, & \text{if } \theta'_A - \theta_B > 0 \end{cases}, \tag{1}$$

where $\Delta = \theta_A - \theta_B$ is the nominal phase difference between Alice and Charlie. According to the measured D_{1,θ_A} and D_{2,θ_A} over 10^5 pulses for each θ_A, the empirical distribution of δ is shown in Fig. 4(a).

Stage 4. Noise removal.

As mentioned in Assumption (6), we assume that $\theta_A = 0$ is ideal, and the measurement result in this case characterizes the fluctuation from the remaining parts of the
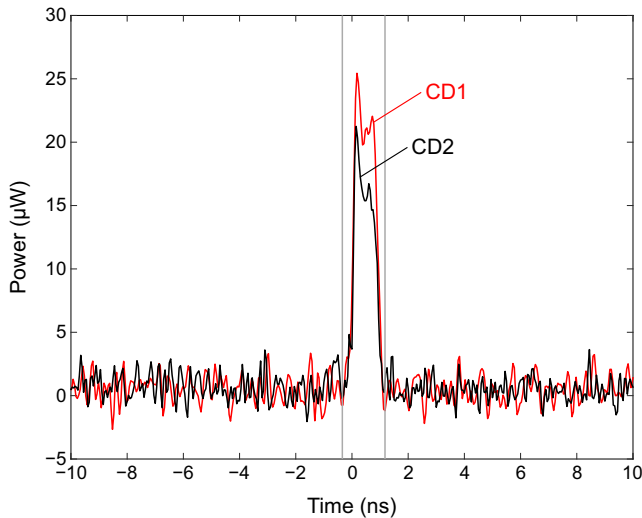

FIG. 3. Typical waveforms measured by CD1 and CD2 for $\theta_A = \pi/2$. The energy of each pulse is calculated by integrating the power between the gray lines.

experiment, which we treat as noise. To obtain the real phase distributions for $\theta_A = \pi/2$ and π, we have to filter out this noise from the measured results. This is done by using a SVD filter [42,43] (see Appendix B), with help from the characterized distribution of noise. In this processing, the SVD algorithm is first applied to the signal of the measured Gaussian noise to factorize out the singular values (the positive square root of eigenvalues) of the noise, which contributes to small singular values [44]. Then a filtering threshold is set. Consequently, the SVD algorithm is employed to the signal measured by CD1 and CD2 in the cases $\theta_A = \pi/2$ and π. The obtained singular values that are smaller than the threshold are discarded to remove the effect of the noise. The remaining singular values are reconstructed by the reverse SVD to form the filtered signal.

Then the phase distribution is calculated again, as is shown in Fig. 4(b). We note that thanks to Assumption (6), we can assume that the distributions in Fig. 4(b) represent the real distributions of phases that are modulated by Alice. Since the distributions are assumed to be Gaussian, which looks indeed to be the case in Fig. 4, we describe the real phase $\theta'_A = \theta_A + \delta$ by a mean value $\overline{\theta'_A}$ and a standard deviation $\sigma_{\theta'_A}$, listed in Table I. Here $\overline{\theta'_A}$ represents the amount of systematic error remaining after a careful calibration process and $\sigma_{\theta'_A}$ quantifies the actual random fluctuation of the optical pulses' phase.

While Clavis2 does not self-calibrate the voltages applied at the phase modulators after leaving the factory,
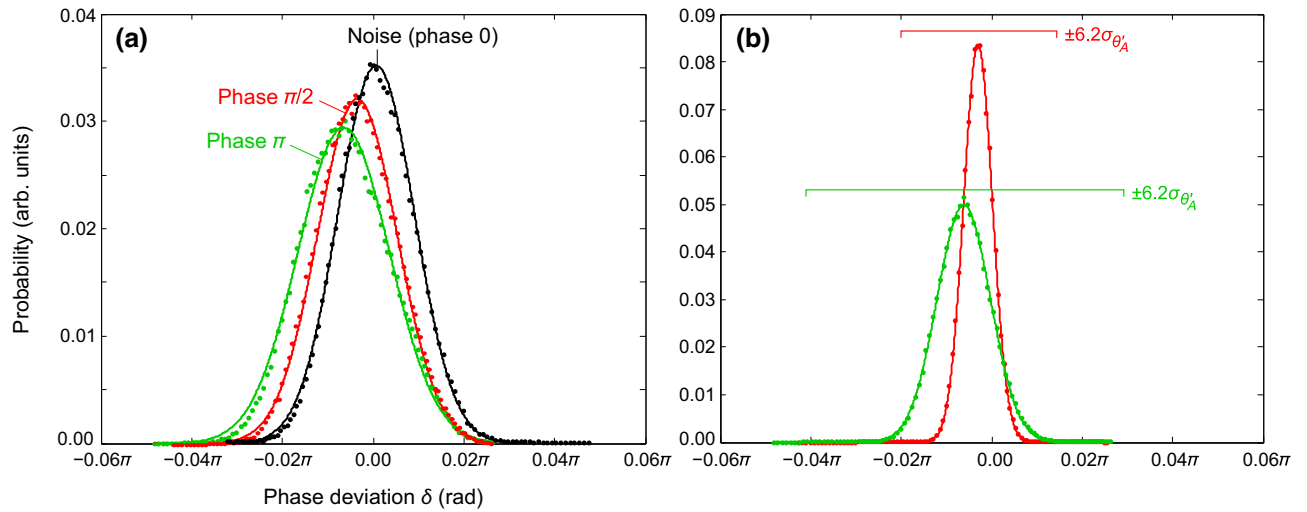
FIG. 4. Empirical distribution of phase deviation δ for different phases Alice applies, (a) before and (b) after noise filtering at Stage 4. The dots are measured data, and the curves are Gaussian approximations. Intervals R_{ph}^c are shown as bars.

other QKD systems may periodically recalibrate them, making $\overline{\theta'_A}$ vary during the operation. They may also drift with changing environmental conditions (such as the temperature) and the age of the hardware. However, a minor deviation of the mean from the ideal value has virtually no effect on the key rate in this security proof [33].

IV. EXPERIMENT OF INTENSITY CHARACTERIZATION

In this section, we present the methodology and experimental results of measuring the intensity fluctuation. Similar to the phase interval, the characterized intensity interval R_{int}^k is applied to estimate the lower bound on the single-photon detection rate among the signal states according to Eq. (21) in Ref. [33], which is then employed in the framework of security proof proposed in Ref. [33]. To demonstrate the method of characterizing the intensity interval, we conduct a proof-of-principle experiment on another industrial-prototype BB84 QKD system that employs weak + vacuum decoy-state protocol [21] and polarization encoding. (Since Clavis2 lacks intensity modulation and this BB84 system uses polarization encoding, we could not measure both phase and intensity fluctuation in the same system. However using two different systems

should not impair the demonstration of either characterization methodology.) Here we measure R_{int}^k for the signal, decoy, and vacuum state.

In our test, we employ only the source unit Alice of this QKD system, whose scheme is shown in Fig. 5. In Alice, a laser diode generates identical optical pulses at 40-MHz repetition rate, which are randomly modulated to different intensities by an intensity modulator (IM). These optical pulses are then encoded into different polarization states by a polarization modulator (pol-M) and attenuated by a VOA. The randomization of the polarization modulation and intensity modulation is provided by the FPGA with random numbers generated by QRNG. We assume any of the above parts except the VOA may contribute to the intensity fluctuation of the source. The VOA, being a slow electromechanical device, should be unable to introduce fast fluctuations. In order to be able to characterize the intensity fluctuations, we set the VOA at its minimum
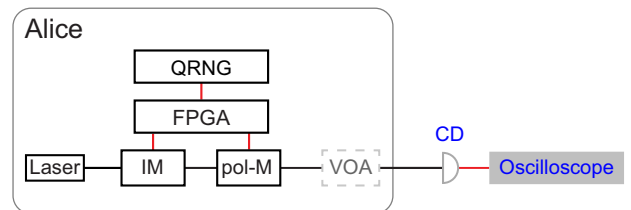

FIG. 5. Setup for intensity distribution measurement. In the device under test, Alice's laser diode generates optical pulses. They pass through an intensity modulator (IM) and polarization modulator (pol-M), which are both controlled by the FPGA with random numbers provided by QRNG. The VOA in Alice is inactivated by bypassing it. The measurement devices are classical photodetector (CD; optical-to-electrical converter) and oscilloscope.

TABLE I. Parameters of Gaussian approximation of phase distributions.

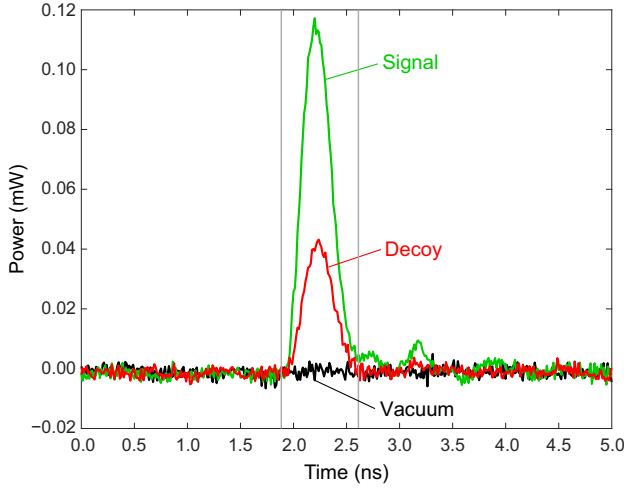| Nominal phase θ_A	$\overline{\theta'_A}$	$\sigma_{\theta'_A}$
0	0	0
$\pi/2$	0.4970π	0.0028π
π	0.9939π	0.0057π

FIG. 6. Typical waveforms of the three intensity states measured in the experiment. The energy of each pulse is calculated by integrating the power between the gray lines.

TABLE II. Parameters of Gaussian approximation of intensity distributions.

State	$\bar{\mu}$	σ_μ
Vacuum	-0.78×10^{-3}	0.0083
Decoy	0.236	0.0149
Signal	0.602	0.0258

attenuation, obtaining brighter pulses. The output of Alice is sent to an O/E converter (Picometrix PT-40A with 38-GHz electrical bandwidth) that connects to an oscilloscope (Agilent DSOX93304Q with 33-GHz analog bandwidth and 80-GHz sampling rate). The system is set to run the raw-key exchange during our test.

The procedure of the experiment is as follows.

Stage 1. Noise calibration.

Before conducting the intensity interval characterization, the distribution of instrument noise shall be calibrated first. Thus, after configuring the testing setup, all the equipment, including Alice, is powered on, but no raw-key exchange is started. The oscilloscope collects the distribution of instrument noise as a reference, which is shown in the inset in Fig. 7(a).

Stage 2. Measurement.

In order to measure the intensity fluctuations of the signal, decoy, and vacuum state, Alice continuously runs the raw-key exchange to generate optical pulses with random intensities (with signal:decoy:vacuum probability ratio of 6:1:1), until 2×10^5 pulses in total are collected by the oscilloscope. In this way, the three intensity levels are recorded in one run. The typical waveforms measured in the experiment are shown in Fig. 6.

Stage 3. Intensity calculation.

After the measurement, we process the recorded oscillograms to calculate the single-photon-level intensities. The photon number of each optical pulse is calculated as

$$\mu = \frac{(S_e/G_{o-e})\,A}{hc/\lambda}, \qquad (2)$$

where the measured area under the voltage oscillogram of each pulse S_e is obtained by integrating the signal between the gray lines in Fig. 6, the conversion gain of the O/E

converter $G_{o-e} = 703$ V/W as calibrated by its manufacturer, and normal transmission of the VOA including its insertion loss in the QKD system during the raw-key exchange $A = 1.876 \times 10^{-6}$ (-57.3 dB). The denominator is the energy of a single photon at the laser wavelength $\lambda = 1550.12$ nm, with h being the Planck constant and c the speed of light. The calculated pulse intensities are then binned in histograms to produce distributions shown in Fig. 7(a).

Stage 4. Noise removal.

To remove instrument noise from the measured results, we use a SVD filter (see Appendix B) with an input of the instrument noise distribution collected at *Stage 1*. The SVD processing is identical to that described in *Stage 4* of the phase interval measurement. The processing is applied to the measured electrical signals of all three intensity levels. The filtered electrical signals are then used to calculate the photon numbers again according to Eq. (2), which are binned into histograms again. The result is shown in Fig. 7(b). Similarly to the phase distributions, the distributions of intensities are also nearly Gaussian, with their parameters listed in Table II. It is notable that, in theory, the vacuum state is zero. However, in practice, measurement is always affected by noise, so we cannot get the perfect zero for the vacuum state but obtain, in this particular instance, a small negative value.

The extracted intensity distributions are much wider relative to their mean values than the phase distributions. We attribute this to stochastic dynamic processes in the gain-switched laser that generate energy noise (and timing jitter) of short pulses produced by it. As will be shown shortly, this leads to zero secure key rate with the available proof. This indicates that this simple gain-switched laser source may be unsuitable for secure QKD. Improvements to the source that reduce the laser's timing jitter [45] might also reduce its energy noise and should be tested in future work. Moreover, the random modulation of intensity, compared to the fixed modulation of phase, may also introduce extra fluctuation, which also shall be investigated in future work.

V. SIMULATION OF SECRET KEY RATE

We employ the security proof and simulation technique proposed in Ref. [33] to calculate the secret key rate. In order to thoroughly show the effect of the phase and intensity fluctuation on the secret key rate, we consider three
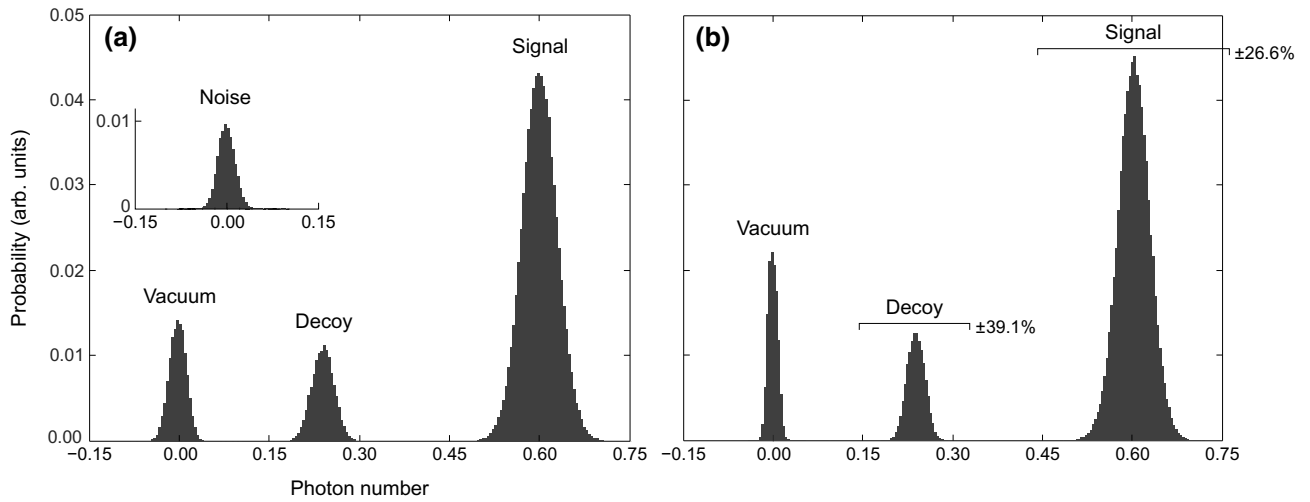
FIG. 7.   Distribution of intensities for different states Alice prepares (a) before and (b) after noise filtering. Inset: noise distribution. Intervals R_{int}^k are shown as bars.

cases. We first calculate the key rate with phase fluctuation only (assuming there is no intensity fluctuation), then with intensity fluctuation only, then with both phase and intensity fluctuation. For all the following simulations we assume that Bob uses single-photon detectors with 80% photon detection efficiency and dark count probability of 10^{-9} per optical pulse, such as superconducting-nanowire detectors from Scontel [46]. The security parameter ε_s is set to be 10^{-10}, and the efficiency of the error-correcting codes f_e is assumed to be 1.05. We assume fiber loss of 0.20 dB/km.

A. Phase fluctuation only

We first simulate the scenario when the intensity modulation is perfect and only the phase fluctuation exists. We apply the experimental values of phase fluctuation from Table I. The phase falling outside the fluctuation interval $\overline{\theta'_A} \pm 6.2\sigma_{\theta'_A}$ either for $\theta_A = 0$ or $\pi/2$ is regarded as an error, and the probability of having such error $p_{\text{fail}} = 1.13 \times 10^{-9}$. Signal and decoy intensities are optimized at each fiber length. The simulation results are shown in Fig. 8. The dashed (solid) lines show the secret key rates without (with) phase fluctuation, for three different total numbers of pulses sent by Alice N_{sent}.

The presence of the phase fluctuation reduces the secure key rate at a short distance by about a factor of 4 and the maximum transmission distance by about 35 km. Notably, the distance can still be longer than 100 km for 10^{13} pulses sent. Although in Clavis2 a key distribution session of the latter size would take about 2 months, a higher-speed 1-GHz system could complete it under 3 h.

To see how much phase noise the system can tolerate, we have also run the simulation with an artificially increased fluctuation, multiplying the experimentally

obtained $\sigma_{\theta'_A}$ by a factor. The system keeps producing secret key until approximately $2\sigma_{\theta'_A}$.

B. Intensity fluctuation only

Next, we calculate the key rates with intensity fluctuation but no phase fluctuation. Unfortunately, the simulation cannot directly take the measured mean photon numbers and standard deviations shown in Table II to obtain a positive key rate. This is because the measured mean photon numbers of the decoy and signal are not optimized for the simulation at each fiber length. Moreover, the measured intensity fluctuation of the gain-switched laser diode source is too large to generate a key under this proof.
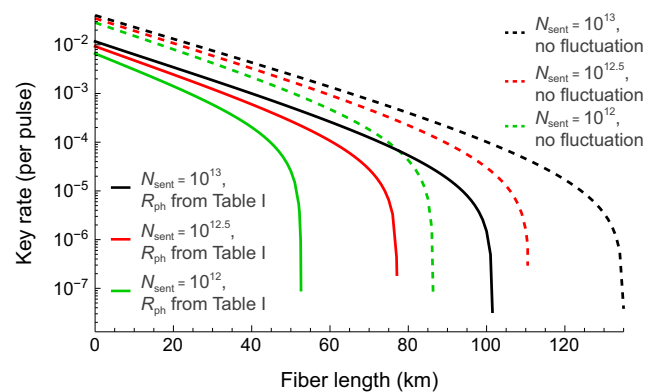

FIG. 8.   Simulated key rate when only phase fluctuation is considered. The dashed lines are key rates with the measured mean value of phase but without any fluctuation. The solid lines show key rates with the phase fluctuation obtained from experiment in Table I. The number of pulses sent by Alice is 10^{13} for black lines, $10^{12.5}$ for red (dark gray) lines, and 10^{12} for green (light gray) lines.
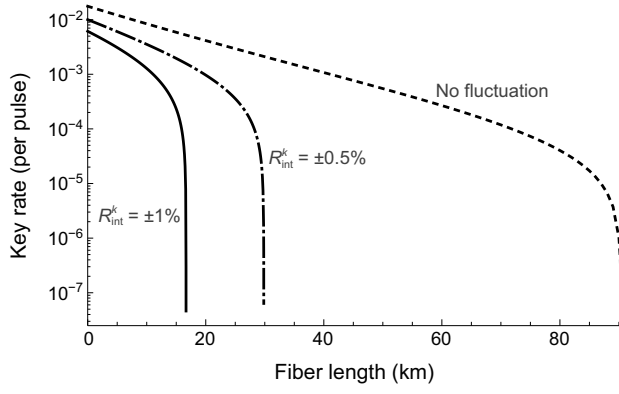
FIG. 9. Simulated key rates with only intensity fluctuation and fixed mean photon numbers obtained from the experiment. The dashed line is the key rate with no fluctuation at all. Then dash-dotted (solid) line is the key rate with $\pm0.5\%$ ($\pm1\%$) fluctuation of intensity modulation. The number of pulses sent by Alice is 10^{13}.
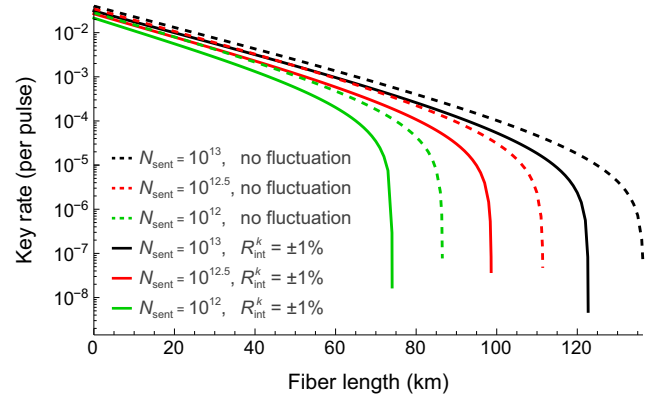

FIG. 10. Simulated key rates with only intensity fluctuation with optimized mean photon numbers at each distance. The dashed lines are the secret key rates without any fluctuation, while the solid lines are those with $\pm1\%$ fluctuation of intensity modulation. The number of pulses sent by Alice is 10^{13} for black lines, $10^{12.5}$ for red (dark gray) lines, and 10^{12} for green (light gray) lines.

Therefore, in order to provide a reference for an acceptable level of intensity fluctuation, we analyze the key rates under two scenarios: (a) the mean photon numbers are fixed and taken from the experimental results but the fluctuation interval is set to be $\pm0.5\%$ or $\pm1\%$, and (b) the mean photon numbers are optimized for each fiber length and fluctuation is also set to be $\pm1\%$. In both scenarios, we set the probability that the actual intensity value is outside the fluctuation interval at 1.41×10^{-9}. The vacuum state is assumed to have $\bar{\mu} = 10^{-3}$ and zero fluctuation. The phase is set to have zero fluctuation but the measured mean values $\overline{\theta'_A}$ (Table I); the latter values have virtually no effect on the key rate in this security proof [33].

Scenario (a): Fixed mean photon numbers with fixed fluctuation. The mean photon numbers for the decoy and signal are taken from Table II, and $N_{\text{sent}} = 10^{13}$. The resulting key rates with different amounts of intensity fluctuation are shown in Fig. 9. The fluctuation is set to be $\pm0.5\%$ or $\pm1\%$ for both the signal and decoy state. While without the imperfection the distance reaches 90 km, a moderate amount of fluctuation of just $\pm0.5\%$ ($\pm1\%$) reduces it to 30 km (17 km). This high sensitivity to the fluctuation is attributed to our using the fixed mean photon numbers of the states. Note that the fluctuation ranges simulated are approximately 25–80 times smaller than those obtained from the experiment in Sec. IV: the $\pm6.2\sigma_\mu$ range is $\pm39.1\%$ for the decoy state and $\pm26.6\%$ for the signal state. The source intensity noise should thus be drastically reduced to accommodate the available security proof.

Scenario (b): Optimized mean photon numbers with fixed fluctuation. In this simulation, the mean photon number of the decoy state is optimized between 0.001 and 0.15, and that of the signal state is optimized between 0.1 and 0.8. The results are shown in Fig. 10. Key rates for three

different N_{sent} are plotted, with all the other parameters being identical.

This simulation shows that optimising the mean photon numbers of the decoy and signal allows to tolerate the intensity fluctuation much better. The key rate at a short distance is not significantly reduced and the maximum transmission distance only decreases by about 13 km. For the same fluctuation of $\pm1\%$, the maximum distance with optimized photon numbers reaches 123 km versus 17 km with the fixed photon numbers. This is a significant advantage. However this means the experimental characterization should in the future be extended to measure fluctuation in a range of mean photon numbers, which makes it more complex.

C. Phase and intensity fluctuation

Finally, we consider fluctuations in both the intensity and phase. The overall error probability is set to be 2.54×10^{-9}, which is the probability that the phase is outside the fluctuation interval of $\pm6.2\sigma_{\theta'_A}$ or the actual intensity value is outside the fluctuation interval of $\pm1\%$ or $\pm3\%$. Other relevant assumptions are taken from the phase-only and intensity-only fluctuation simulations. The results are shown in Fig. 11.

Combining the phase and intensity fluctuation introduces some drop in the key rate and maximum distance. For example, with only intensity fluctuation of $\pm1\%$ interval, the maximum distance is 123 km for $N_{\text{sent}} = 10^{13}$ (Fig. 10), however when the phase fluctuation is added it drops to 78 km (Fig. 11). When the intensity interval is widened to $\pm3\%$, the key rate and maximum distance decay rapidly, and no key is produced for the lowest
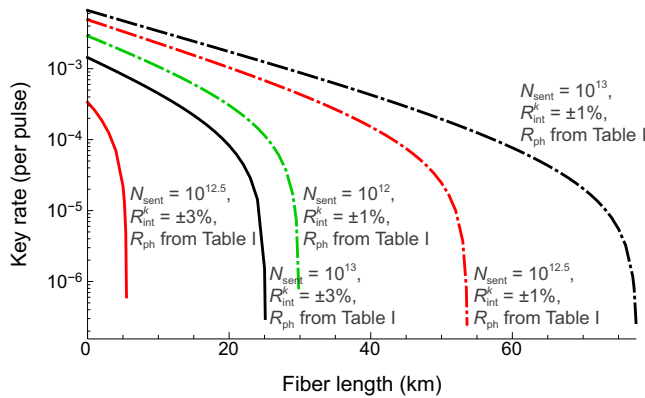
FIG. 11.　Simulated key rates when both phase and intensity fluctuations are considered. The phase fluctuations are obtained from the experiment (Table I) and the mean photon numbers of the decoy and signal state are optimised at each fiber length. The dash-dotted (solid) lines are the key rate with $\pm 1\%$ ($\pm 3\%$) intensity fluctuation. The number of pulses sent by Alice is 10^{13} for black lines, $10^{12.5}$ for red (dark gray) lines, and 10^{12} for green (light gray) lines.

$N_{\text{sent}} = 10^{12}$. This shows that controlling the intensity fluctuation in the QKD hardware is crucial, at least with the security proof currently available [33].

We stress that our security proof [33] assumes that when an individual state is outside the set fluctuation range, Eve can get perfect information about the raw key, which is the worst scenario in theory but is not a specific known attack. We admit this for the simplicity of analysis, and this assumption may be one of the major causes of the severe performance degradation. In the future, we plan to consider how to remove this assumption for better performance.

VI. CONCLUSION

We propose and experimentally demonstrate methodology for characterizing source fluctuation in phase and intensity in QKD. We then apply our characterization results to the security proof of the three-state, loss-tolerant protocol [33]. The fluctuations lead to a significant reduction in the secure key rate and maximum transmission distance in fiber. In fact, the intensity fluctuation we measure on the gain-switched semiconductor laser source is so large that the proof predicts no key. There is room for improvement in the source hardware, especially to reduce its intensity fluctuation. An alternative might be using a seeded pulsed laser source [45] or using a continuous-wave laser and produce phase-randomized pulses with intensity and phase modulators. Likewise the security proof and details of the QKD protocol might be improved to give a higher key rate at the same fluctuation. This may be helped by knowing the distribution of fluctuation (such as the Gaussian distribution we measure) [47] or by combining with the idea of twisting [48]. Finally, the development

of security proofs for other QKD protocols that incorporate source fluctuation is desirable [49,50]. Although the security proof we use [33] cannot handle intersymbol interference [51–55], our experimental characterization techniques can be adapted to also measure the latter. This characterization methodology is a necessary element in the upcoming formal security standards and certification of QKD.

Author contributions

A.H. performed the experiments. A.M. and K.T. performed the simulations. H.-K.L., V.M., and K.T. supervised the study. A.H. wrote the paper with help from all authors.

APPENDIX A: PROTOCOL FRAMEWORK

We briefly describe the protocol [33] that the security proof with modulation fluctuation is based on. Here we consider the loss-tolerant protocol [27] with decoy-state method, which uses three encoding states, $\{0_Z, 1_Z, 0_X\}$, with asymmetric choice between two bases. Additionally, we follow the framework of security proof in Ref. [33], and the secret key is extracted from the events where Alice and Bob both select Z basis. The detection events where Alice and Bob have chosen different bases are used for estimating the phase error rate, i.e., the amount of information leaked to the eavesdropper.

Before describing the protocol [33], we summarize the assumptions on the light source. How our experiment allows us to satisfy these assumptions and extract the values for the relevant parameters is explained in main text. The following labels (A1)–(A7) correspond to the ones in

Ref. [33]. Note that the main contribution of our experiment is to measure the phase intervals R_{ph}^c and intensity intervals R_{int}^k in (A6).

(A1) Assumption on the emitted state: we assume that each emitted state is a perfectly phase-randomized and single-mode coherent state. We just assume that our experiments with both QKD systems satisfy this assumption.

(A2) Correlation assumption: we assume that each emitted signal is allowed to be correlated in a setting-choice-independent correlation (SCIC) manner [56]. Note that SCIC means that there exists a parameter g^i in the source device that determines the ith emitted state, and these $\{g^i\}$ are allowed to be correlated with each other. For example, g^i is a temperature of the source device of the ith pulse emission.

(A3) Random choice assumption: we assume that each intensity choice $k \in \mathcal{K} := \{k_1, k_2, k_3\}$ and each phase choice $c \in \mathcal{C} := \{0_Z, 1_Z, 0_X\}$ are independent random variables with fixed chosen probabilities.

(A4) Independence assumption of the phase and the intensity: we assume that the ith phase and intensity are independent from one another, which we just suppose in our experiment.

(A5) Unique determination assumption of the phase and the intensity: given the intensity and phase choices and the parameter g^i, the ith phase and intensity are uniquely determined, which we also just assume in our experiment.

(A6) Assumption on the intervals for the phase and intensity: for each phase choice c, Alice knows the phase interval R_{ph}^c and for each intensity choice k, she knows the intensity interval R_{int}^k. The contribution of this paper is to characterize R_{ph}^c and R_{int}^k in practical QKD systems.

(A7) Assumption on the number of tagged signals: among all the emitted pulses, the number of tagged signals n_{tag} are assumed to be upper bounded by the probability p_{fail}. Again, the tagged signals are the emitted pulses whose intensity or phase is outside the intervals. This is just a theoretical assumption. We can thus freely choose the number of tagged signals n_{tag} and the probability p_{fail} of their falling outside the intervals R_{ph}^c and R_{int}^k, such that we obtain the maximum key rate.

Then, the loss-tolerant protocol in Ref. [33] operates as follows.

Step 0: device characterization and parameter determination. Alice first characterizes her phase-fluctuation interval, R_{ph}^c, and intensity-fluctuation interval, R_{int}^k, where $c \in \mathcal{C} = \{0_Z, 1_Z, 0_X\}$ for different encoding states and $k \in \mathcal{K} = \{k_1, k_2, k_3\}$ for different intensities. Furthermore, Alice and Bob shall decide the security parameter ε_s, and the number of pulses sent N_{sent}.

Step 1: state preparation and transmission. Alice randomly chooses an intensity setting $k \in \mathcal{K}$ and a basis with probability $P \in \{P_Z, P_X\}$. If Z basis is selected, she prepares bit 0_Z or bit 1_Z with equal probability. Otherwise, she chooses bit 0_X. The prepared state is sent to Bob via a quantum channel.

Step 2: detection. Bob measures the received states by randomly choosing a basis from Z, X with probability $P \in \{P_Z, P_X\}$. The detection outcome is $b \in \{0, 1, \perp, \emptyset\}$, where $\perp$ and $\emptyset$ represent a double-click event and no-click event respectively. In the double-click event, a bit value is randomly assigned.

Alice and Bob repeat Step 1 and Step 2 until N_{sent} pulses are sent to Bob.

Step 3: sifting. Bob declares the detection events and his basis choices for these events over an authenticated public channel. Alice checks her basis choices during these events and announces to Bob. They keep the events where both of them have selected Z basis as a sifted key.

Step 4: parameter estimation. Alice uses a subset of the sifted key and the intensity interval R_{int}^k to calculate a lower bound on the number of single-photon events $S_{Z,1}^L$, by Eq. (21) in Ref. [33]. Moreover, she calculates an upper bound on the number of phase errors $N_{ph,Z,1}^U$ with help of phase interval R_{ph}^c, according to Eq. (24) in Ref. [33]. Thus, an upper bound on the phase error rate is given by $e_{ph,Z,1}^U = N_{ph,Z,1}^U / S_{Z,1}^L$.

Step 5: error correction. Through the public channel, Bob corrects his sifted key to be identical to that of Alice.

Step 6: privacy amplification. Alice and Bob conduct privacy amplification to shorten the key length by using the results from Step 4 and Step 5 to obtain the final secret key with length l, which satisfies [33]

$$l \le S_{Z,1}^L \left[1 - h(e_{ph,Z,1}^U) \right] - \log_2 \frac{2}{\varepsilon_{PA}} - \lambda_{EC}, \qquad (A1)$$

where $h(x)$ is the binary entropy function, $\varepsilon_{PA} > 0$ is the parameter related to the success probability of privacy amplification, and λ_{EC} is the cost of error correction.

APPENDIX B: DENOISING BY SINGULAR VALUE DECOMPOSITION

The instrument noise produced by our characterization setups is assumed to be additive and independently and identically distributed (IID) Gaussian, or the white noise. We would like to filter out this uncorrelated instrument noise from the measured phase and intensity fluctuations produced by the QKD systems under test. If these phase and intensity fluctuations also had Gaussian distribution, their denoising would be very simple. The denoised distribution would be Gaussian with the same mean as the measured distribution and the standard deviation $\sigma = \sqrt{\sigma_{measured}^2 - \sigma_{noise}^2}$, where $\sigma_{measured}$ is the standard deviation of the measured fluctuation-with-instrument-noise

distribution and σ_{noise} is the standard deviation of the measured instrument-noise-only distribution.

However, if the phase and intensity fluctuations might not follow the Gaussian distribution, we need to adopt a more general denoising technique. In this case, filtering has to be applied to individual measured waveforms (shown in Figs. 3 and 6). In our study, we apply a filtering process based on singular value decomposition (SVD) [42,43,57]. The measured waveforms are put into rows in an $m \times n$ matrix M, which is then factorized as

$$M = USV^{\top}, \tag{B1}$$

where U is an $m \times m$ unitary matrix of orthonormal eigenvectors of $MM^{\top}$, S is an $m \times n$ diagonal matrix of singular values that are the square roots of the eigenvalues of $M^{\top}M$ and are arranged in descending order, and $V^{\top}$ is an $n \times n$ unitary matrix containing the orthonormal eigenvectors of $M^{\top}M$. After this SVD processing, the data contained in the matrix M is represented by the singular values in matrix S.

The singular values and corresponding singular vectors contain complete information about matrix M. The characteristics of the waveforms are mainly described by the first few singular values in matrix S. Meanwhile, the small singular values of the additive instrument noise are assumed to be spread over its m dimension [44]. Therefore, theoretically the SVD method could divide the data space of the measured waveforms into true signal and noise subspaces by distinguishing and separating the singular values. Specifically, for the instrument noise that is IID Gaussian, a threshold could be applied to distinguish between small singular values of the noise and large ones of the signal. This threshold is determined taking into account the prior knowledge about the strength of the instrument noise [58]. We then truncate (i.e., zero) the small singular values that fall below the threshold. Practice shows that the SVD method can be effective at filtering out the noise. The specific algorithm we use is the following.

Step 0. Construct the matrix of waveforms. After obtaining the measured waveforms of optical pulses detected by the O/E converter as oscillograms (shown in Figs. 3 and 6), each waveform period constitutes a row of the matrix M. Let us consider the intensity fluctuation as an example. Since the repetition frequency of the measured QKD system is 40 MHz and the sampling rate of the oscilloscope is 80 GHz, each period contains 2000 sampling points, which populate a row of the matrix M. To limit the computing time of SVD, our data is split into multiple matrices containing each 100 periods of oscillogram's data, so that the size of each matrix M is 100×2000. In principle, the waveforms could be processed in fewer matrices of a larger size, however this would take more computing time.

Step 1. Obtain singular values. The singular value decomposition is applied to each matrix M, obtaining the matrix S with singular values on the diagonal. For
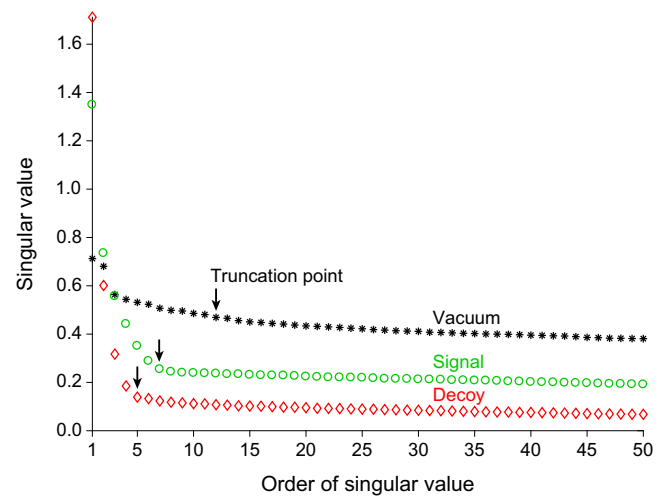

FIG. 12. The first 50 singular values obtained by SVD for the measured waveforms of optical pulses.

example, in the case of intensity fluctuation, the SVD is first applied to the waveforms of instrument noise, which allows us to know all the singular values of the noise. The instrument noise waveforms are processed in blocks of 100, then their singular values are averaged over all the blocks to obtain a reference set. Then the waveforms of optical pulses for the vacuum, decoy, and signal state are processed by SVD to obtain their singular values as well (individually for each block, without averaging). Figure 12 shows the first 50 singular values for the measured waveforms of the three latter states in one of the blocks. It can be seen that only a few singular values are dominating elements with information about the intensity, and the remaining singular values are relatively smaller due to the IID instrument noise.

Step 2. Determine the truncation threshold. A truncation threshold ϵ is manually determined either to be the singular value that suddenly becomes smaller than the previous one or the singular value that is close to the maximum one of the instrument noise. The former approach is used when a SNR is high, such as for the waveforms of optical pulses for the decoy and signal state. The latter approach is used when the SNR is relatively low, such as for the vacuum state. In our measurement of intensity fluctuation, the maximum singular value of the instrument noise in the reference set is 0.4691, which we regard as the truncation threshold of the vacuum state. Thus, for the signal (decoy, vacuum) state, ϵ is set to be the value of the seventh (fifth, twelfth) element, as illustrated in Fig. 12.

Step 3. Truncate and reconstruct the filtered waveform. The singular values that are equal to or smaller than ϵ are zeroed, obtaining matrix S'. The filtered waveform is then reconstructed as $M' = US'V^{\top}$. After that, the energy of each optical pulse is calculated by integrating the filtered waveform, whose data is each row of matrix M'. The

fluctuation distributions after filtering are then calculated according to *Stage 3* presented in main text for the cases of both phase fluctuation and intensity fluctuation.

We remark that for the measurements presented in this study in Figs. 4 and 7, the distributions filtered by SVD happen to be close to Gaussian. The simple Gaussian denoising technique described in the beginning of this Appendix gives a result that is close to that of SVD. However the SVD can also handle non-Gaussian experimentally measured distributions (which we observe in some of our experiments), thus it remains our chosen denoising method.

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

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

[3] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12,** 113026 (2010).

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

[5] 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).

[6] 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).

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

[8] Anqi Huang, Álvaro Navarrete, Shi-Hai Sun, Poompong Chaiwongkhot, Marcos Curty, and Vadim Makarov, Laser-Seeding Attack in Quantum Key Distribution, Phys. Rev. Appl. **12,** 064043 (2019).

[9] Anqi Huang, Ruoping Li, Vladimir Egorov, Serguei Tchouragoulov, Krtin Kumar, and Vadim Makarov, Laser-Damage Attack Against Optical Attenuators in Quantum Key Distribution, Phys. Rev. Appl. **13,** 034017 (2020).

[10] Zhihao Wu, Anqi Huang, Huan Chen, Shi-Hai Sun, Jiang-fang Ding, Xiaogang Qiang, Xiang Fu, Ping Xu, and Junjie Wu, Hacking single-photon avalanche detectors in quantum key distribution via pulse illumination, Opt. Express **28,** 25574 (2020).

[11] Shihai Sun and Anqi Huang, A review of security evaluation of practical quantum key distribution system, Entropy **24,** 260 (2022).

[12] Binwu Gao, Zhihai Wu, Weixu Shi, Yingwen Liu, Dongyang Wang, Chunlin Yu, Anqi Huang, and Junjie Wu, Ability of strong-pulse illumination to hack self-differencing avalanche photodiode detectors in a high-speed quantum-key-distribution system, Phys. Rev. A **106,** 033713 (2022).

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

[14] Nitin Jain, Elena Anisimova, Imran Khan, Vadim Makarov, Christoph Marquardt, and Gerd Leuchs, Trojan-horse attacks threaten the security of practical quantum cryptography, New J. Phys. **16,** 123030 (2014).

[15] A. Huang, S.-H. Sun, Z. Liu, and V. Makarov, Quantum key distribution with distinguishable decoy states, Phys. Rev. A **98,** 012330 (2018).

[16] Anastasiya Ponosova, Daria Ruzhitskaya, Poompong Chaiwongkhot, Vladimir Egorov, Vadim Makarov, and Anqi Huang, Protecting Fiber-Optic Quantum Key Distribution Sources Against Light-Injection Attacks, PRX Quantum **3,** 040307 (2022).

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

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

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

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

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

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

[23] Note that a basic assumption in the decoy-state method is that signal and decoy pulses are indistinguishable, but this assumption has been waived in Refs. [9,33].

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

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

[26] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11,** 045018 (2009).

[27] 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).

[28] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden, Secure Quantum Key Distribution over 421 km of Optical Fiber, Phys. Rev. Lett. **121,** 190502 (2018).

[29] Fadri Grünenfelder, Alberto Boaron, Davide Rusca, Anthony Martin, and Hugo Zbinden, Simple and high-speed polarization-based QKD, Appl. Phys. Lett. **112,** 051108 (2018).

[30] Feihu Xu, Kejin Wei, Shihan Sajeed, Sarah Kaiser, Shihai Sun, Zhiyuan Tang, Li Qian, Vadim Makarov, and Hoi-Kwong Lo, Experimental quantum key distribution with source flaws, Phys. Rev. A **92,** 032305 (2015).

[31] Akihiro Mizutani, Marcos Curty, Charles Ci, Wen Lim, Nobuyuki Imoto, and Kiyoshi Tamaki, Finite-key security analysis of quantum key distribution with imperfect light sources, New J. Phys **17**, 093011 (2015).

[32] Yuichi Nagamatsu, Akihiro Mizutani, Rikizo Ikuta, Takashi Yamamoto, Nobuyuki Imoto, and Kiyoshi Tamaki, Security of quantum key distribution with light sources that are not independently and identically distributed, Phys. Rev. A **93**, 042325 (2016).

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

[34] Zhiyuan Tang, Kejin Wei, Olinka Bedroya, Li Qian, and Hoi-Kwong Lo, Experimental measurement-device-independent quantum key distribution with imperfect sources, Phys. Rev. A **93**, 042308 (2016).

[35] Feng-Yu Lu, Zhen-Qiang Yin, Rong Wang, Guan-Jie Fan-Yuan, Shuang Wang, De-Yong He, Wei Chen, Wei Huang, Bing-Jie Xu, Guang-Can Guo, and Zheng-Fu Han, Practical issues of twin-field quantum key distribution, New J. Phys. **21**, 123030 (2019).

[36] Feng-Yu Lu, Xing Lin, Shuang Wang, Guan-Jie Fan-Yuan, Peng Ye, Rong Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Guang-Can Guo, and Zheng-Fu Han, Intensity modulator for secure, stable, and high-performance decoy-state quantum key distribution, npj Quantum Inf. **7**, 75 (2021).

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

[38] Clavis2 specification sheet, http://marketing.idquantique.com/acton/attachment/11868/f-00a0/1/-/-/-/-/Clavis%20QKD%20Datasheet.pdf, visited 16 January 2018.

[39] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "Plug and play" systems for quantum cryptography, Appl. Phys. Lett. **70**, 793 (1997).

[40] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug&play system, New J. Phys. **4**, 41 (2002).

[41] The outputs of the Mach-Zehnder interferometer are $I_1 = I \sin^2\left((\theta'_A - \theta_B)/2\right)$, $I_2 = I \cos^2\left((\theta'_A - \theta_B)/2\right)$, where I is the initial intensity of the source. Therefore, the ratio $I_1/I_2 = \tan^2\left((\theta'_A - \theta_B)/2\right)$. Since we compensate the extra loss and subtract the misalignment in our experiment, $I_1 = D_{1,\theta_A} - D_{1,\min}$ and $I_2 = R\left(D_{2,\theta_A} - D_{2,\min}\right)$. Therefore, we can obtain the phase deviation as shown in Eq. (1).

[42] Peter Grassberger, Rainer Hegger, Holger Kantz, Carsten Schaffrath, and Thomas Schreiber, On noise reduction methods for chaotic data, Chaos **3**, 127 (1993).

[43] Konstantinos Konstantinides, Balas Natarajan, and Gregory S. Yovanof, Noise estimation and filtering using block-based singular value decomposition, IEEE Trans. Image Process. **6**, 479 (1997).

[44] Wen-Xian Yang and Peter W. Tse, Development of an advanced noise reduction method for vibration analysis based on singular value decomposition, NDT E Int. **36**, 419 (2003).

[45] Taofiq K. Paraïso, Robert I. Woodward, Davide G. Marangon, Victor Lovic, Zhiliang Yuan, and Andrew J. Shields, Advanced laser technology for quantum communications (tutorial review), Adv. Quantum Technol. **4**, 2100062 (2021).

[46] Scontel SSPD product line, http://www.scontel.ru/products/sspd/, visited 24 February 2021.

[47] X. Sixto, V. Zapatero, and M. Curty, Security of decoy-state quantum key distribution with correlated intensity fluctuations (to be published).

[48] J. Eli Bourassa, Ignatius William Primaatmaja, Charles Ci, Wen Lim, and Hoi-Kwong Lo, Loss-tolerant quantum key distribution with mixed signal states, Phys. Rev. A **102**, 062607 (2020).

[49] Shuang Wang, Zhen-Qiang Yin, De-Yong He, Wei Chen, Rui-Qiang Wang, Peng Ye, Yao Zhou, Guan-Jie Fan-Yuan, Fang-Xiang Wang, Wei Chen, Yong-Gang Zhu, Pavel V. Morozov, Alexander V. Divochiy, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[50] Jie Gu, Xiao-Yu Cao, Yao Fu, Zong-Wu He, Ze-Jie Yin, Hua-Lei Yin, and Zeng-Bing Chen, Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources, Sci. Bull. **67**, 2167 (2022).

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

[52] Margarida Pereira, Go Kato, Akihiro Mizutani, Marcos Curty, and Kiyoshi Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).

[53] Akihiro Mizutani and Go Kato, Security of round-robin differential-phase-shift quantum-key-distribution protocol with correlated light sources, Phys. Rev. A **104**, 062611 (2021).

[54] Víctor Zapatero, Álvaro Navarrete, Kiyoshi Tamaki, and Marcos Curty, Security of quantum key distribution with intensity correlations, Quantum **5**, 602 (2021).

[55] Álvaro Navarrete, Margarida Pereira, Marcos Curty, and Kiyoshi Tamaki, Practical Quantum Key Distribution that is Secure Against Side Channels, Phys. Rev. Appl. **15**, 034072 (2021).

[56] Particularly in high-speed QKD systems, each emitted signal could be correlated in a setting-choice-dependent correlation (SCDC) manner, which means that setting-choice information propagates to subsequent pulses. Some security proofs accommodate this type of correlation; intensity correlations are accommodated in Refs. [51,54], and pulse correlations in terms of Alice's bit choice information are taken into account in Refs. [52,53,55].

[57] Sunil K. Jha and R. D. S. Yadava, Denoising by singular value decomposition and its application to electronic nose data processing, IEEE Sens. J **11**, 35 (2011).

[58] Tsegaselassie Workalemahu, Singular value decomposition in image noise filtering and reconstruction, Master's thesis, Georgia State University, 2008.