Alternative schemes for measurement-device-independent quantum key distribution

Xiongfeng Ma[1,2,3,*] and Mohsen Razavi[3,†]

[1]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing, China*
[2]*Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, Ontario, Canada*
[3]*School of Electronic and Electrical Engineering, University of Leeds, Leeds, United Kingdom*

Practical schemes for measurement-device-independent quantum key distribution using phase and path or time encoding are presented. In addition to immunity to existing loopholes in detection systems, our setup employs simple encoding and decoding modules without relying on polarization maintenance or optical switches. Moreover, by employing a modified sifting technique to handle the dead-time limitations in single-photon detectors, our scheme can be run with only two single-photon detectors. With a phase-post-selection technique, a decoy-state variant of our scheme is also proposed, whose key generation rate scales linearly with the channel transmittance.

I. INTRODUCTION

Quantum key distribution (QKD) enables two remote parties to securely exchange cryptographic keys [1,2]. Despite the theoretically provable security of QKD protocols [3–5], achieving security with realistic devices is still a challenge [6–10]. In fact, before any security proofs can be applied to practical scenarios, various device imperfections should be carefully examined. For example, the detector efficiency mismatch can be exploited by eavesdroppers to implement the efficiency mismatch attack [11] or the time-shift attack [12,13]. Lately, other imperfections, such as the detector's after-gate pulses and the dead time, have also been exploited in hacking strategies [14–17]. Although, in each case, certain countermeasures have been proposed [18,19], to fully remove such attacks one must deal with their fundamental root, i.e., the detection efficiency loophole. In this paper, we build on recent progress on measurement-device-independent QKD (MDI-QKD) [20,21] to propose alternative practical schemes resilient to detection loopholes, thence shielding out all the aforementioned attacks in QKD systems.

The security loopholes in QKD systems essentially stem from the existing issues in Bell's inequality tests. There are three major loopholes, corresponding to the three assumptions in Bell's inequality tests:

(1) locality loophole [22], which is related to the assumption that two test parties are spacelike separated;

(2) efficiency loophole [23], which is related to the fair-sampling assumption [24]; and

(3) randomness (free-will) loophole, which is related to the assumption that measurement bases are chosen randomly.

In the context of QKD, some of these loopholes have proved to be more harmful than the others. For instance, it is reasonable to assume that the information in the two legitimate parties of QKD, Alice and Bob, is protected from the eavesdropper, Eve. Thus, the locality loophole does not necessarily lead to hacking strategies. With recent developments in quantum random number generators [25,26],

the randomness loophole may not introduce security issues either. The efficiency loophole, however, opens up to many quantum attacks. In fact, the aforementioned attacks all fall into this category.

One approach to overcome device imperfections is by using device-independent QKD (DIQKD) schemes [27–30]. The underlying assumptions of security in these schemes are relaxed to only a few, such as no, or little, direct leakage of key information out of QKD users. Unfortunately, DIQKD schemes impose severe constraints on the required specifications for physical devices in use. For example, the tolerable error rate is 7.1% and the minimum required transmittance is 92.4% [31], which make its experimental demonstration extremely challenging.

In order to relax the above constraints, several detection-device-independent QKD schemes have been proposed [32, 33]. The main additional assumption is that the source is trustful. In practice, many QKD schemes use simple source setups, which can be monitored in real time [34,35]. The detection system, on the other hand, is more vulnerable to attacks [11–17]. In [32], for instance, a higher error rate of 11% and a lower transmittance of 65.9% are allowed. We emphasize that the scheme presented in [32] uses a partial self-testing technique to overcome loopholes in detection. However, as pointed out in [24], the time-shift attack puts an ultimate bound of 50% on the transmittance. This is due to the random bit assignment to no-click events in [32]. Recently, Lo, Curty, and Qi proposed an MDI-QKD scheme [36] that is able to essentially avoid random bit assignments, hence going beyond the 50% efficiency limit [20]. By relying on entanglement swapping techniques [37] and reverse EPR schemes [38], the MDI-QKD scheme [20] (see also [39]) can achieve similar performance to traditional QKD systems, while shielding out detection loopholes.

Thus far, three schemes for MDI-QKD have been proposed, two of which rely on phase encoding [21], and the original one uses polarization encoding [20]. The latter requires polarization maintenance over the quantum channel, which makes its implementation over optical fibers challenging. The phase-encoding scheme I in [21] essentially follows the coherent-state QKD scheme without phase randomization [40], and its key rate decays quadratically with the channel

---

*xma@tsinghua.edu.cn
†m.razavi@leeds.ac.uk

transmission efficiency [41]. Scheme II in [21] relies on the relative phase between two weak pulses. In order to perform entanglement swapping, in [21], this phase information is converted to polarization states before being measured by a set of four single-photon detectors. Both phase-encoding schemes require fast optical switches in the measurement unit. We remark that scheme I in [21] is more robust against some imperfections of the state preparation, which may offer benefits in certain practical situations. Note that experimental demonstrations of the MDI-QKD scheme were presented recently [42–44].

In this paper, we propose alternative phase-encoding schemes. Comparing to the one proposed in Ref. [21], our schemes do not require optical switches in the setups. Moreover, the proposed schemes can be implemented with only two single-photon detectors, which makes them even more cost effective. By introducing a proper postselection technique, in the two-detector setup, we can minimize the effects of the dead time. Our schemes do not require polarization maintenance, and, if implemented with single-photon sources, they do not require a phase reference between Alice and Bob. The decoy-state versions of our setup are, however, sensitive to the choice of encoding bases, and in some cases require a mutual phase reference. By introducing a phase-post-selection technique, we can, however, reduce the error rate in the decoy-state protocols. Note that the security of the proposed phase-post-selection technique needs to be further investigated.

The rest of this paper is organized as follows. In Sec. II, we propose a path-phase-encoding MDI-QKD scheme with single-photon states. We simplify our setup in Sec. III and generalize it to coherent-state sources in Sec. IV. We conclude the paper in Sec. V.

II. SINGLE-PHOTON MDI-QKD

In this section, we present an alternative MDI-QKD scheme using path and phase-encoding techniques [45–47]. A key component of our scheme is still a partial Bell-state measurement (BSM) module implemented by 50:50 beam splitters and single-photon detectors; see the Eve or Charlie's box in Fig. 1. In this section, we assume that perfect single-photon (qubit) sources are used by Alice and Bob. We use the setup in Fig. 1 to illustrate how our scheme works. In Sec. III, we will present a more practical setup for implementation purposes.

Our path-encoding MDI-QKD scheme works as follows. Alice and Bob, in Fig. 1, each prepares a single-photon state and passes them through 50:50 beam splitters. The resulting two modes are referred to as reference and signal modes, denoted, respectively, by a_r and a_s on Alice's side, and b_r and b_s on Bob's side. In order to generate the four states of the BB84 protocol, phase modulators, respectively, introduce relative phase shifts θ_a and θ_b between the reference and signal modes of Alice and Bob to obtain the following state:

$$\left(|1\rangle_{a_r}|0\rangle_{a_s} + e^{i\theta_a}|0\rangle_{a_r}|1\rangle_{a_s}\right) \otimes \left(|1\rangle_{b_r}|0\rangle_{b_s} + e^{i\theta_b}|0\rangle_{b_r}|1\rangle_{b_s}\right), \tag{1}$$

where normalization factors are neglected for now. To follow the BB84 protocol, Alice and Bob randomly choose θ_a and θ_b from the two basis sets of $\{0,\pi\}$ and $\{\pi/2,3\pi/2\}$. Phase values
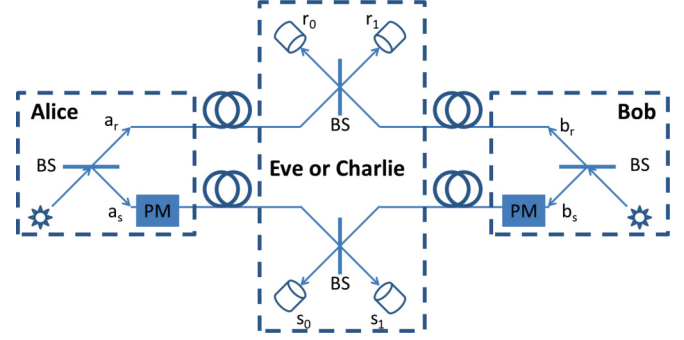

FIG. 1. (Color online) A schematic diagram for the path-phase-encoding MDI-QKD scheme. Here, BS stands for 50:50 beam splitter and PM stands for phase modulator. Alice and Bob each encodes their qubits by introducing a relative phase shift between their reference and signal beams. The phase shifts are applied to the signal modes using PMs, chosen from the set $\{0,\pi/2,\pi,3\pi/2\}$. A partial BSM, possibly performed by an untrusted party, Eve or Charlie, on the two reference and the two signal modes would establish correlations between the raw key bits of Alice and Bob. Provided that they use the same phase basis, a joint click on detectors r_0 and s_0 implies identical bits for Alice and Bob, so does a joint click on r_1 and s_1. A joint click on r_0 and s_1 or r_1 and s_0 would imply complement bits.

0 and $\pi/2$ represent bit 1 and the other two represent bit 0. When single-photon sources are used, the overall phase has no effect on the final result and will be neglected here.

To better understand how the setup in Fig. 1 works, let us first neglect the channel loss and dark count effects, which will be addressed in Appendix A. We also assume that the relative phase between the reference and signal modes is preserved; we will see that, in the next section, how this can practically be achieved. A successful partial BSM in Fig. 1 occurs when one, and only one, of r_0 and r_1, and one, and only one, of s_0 and s_1 click. All other detection events, such as the case when both r_0 and r_1 click, are discarded. Conditioned on a successful BSM outcome, the relevant terms in the joint state of Alice and Bob are given by

$$|1\rangle_{a_r}|0\rangle_{a_s}|0\rangle_{b_r}|1\rangle_{b_s} + e^{i(\theta_a-\theta_b)}|0\rangle_{a_r}|1\rangle_{a_s}|1\rangle_{b_r}|0\rangle_{b_s}. \tag{2}$$

The above state will go through two 50:50 beam splitters, which remove any which-way information, in the BSM module resulting in

$$|01+10\rangle_{r_0r_1}|01-10\rangle_{s_0s_1} + e^{i(\theta_a-\theta_b)}|01-10\rangle_{r_0r_1}|01+10\rangle_{s_0s_1}$$

$$= |0101-0110+1001-1010\rangle_{r_0r_1s_0s_1} + e^{i(\theta_a-\theta_b)}|0101$$

$$+0110-1001-1010\rangle_{r_0r_1s_0s_1}, \tag{3}$$

where r_0, r_1, s_0, and s_1 represent the input modes to the corresponding detectors in Fig. 1, and we have used the following transformation for the two beam splitters:

$$|1\rangle_{a_r}|0\rangle_{b_r} \mapsto |0\rangle_{r_0}|1\rangle_{r_1} + |1\rangle_{r_0}|0\rangle_{r_1},$$
$$|0\rangle_{a_r}|1\rangle_{b_r} \mapsto |0\rangle_{r_0}|1\rangle_{r_1} - |1\rangle_{r_0}|0\rangle_{r_1},$$
$$|1\rangle_{a_s}|0\rangle_{b_s} \mapsto |0\rangle_{s_0}|1\rangle_{s_1} + |1\rangle_{s_0}|0\rangle_{s_1},$$
$$|0\rangle_{a_s}|1\rangle_{b_s} \mapsto |0\rangle_{s_0}|1\rangle_{s_1} - |1\rangle_{s_0}|0\rangle_{s_1}. \tag{4}$$

In the above equation, we assume that the photons arriving at the relay are indistinguishable. This can be guaranteed by

applying filters [48] before the $50:50$ beam splitters in the measurement box.

If $\theta_a - \theta_b = 0$, then the state in Eq. (3) becomes

$$|0101 - 1010\rangle_{r_0 r_1 s_0 s_1}; \tag{5}$$

that is, either detectors r_0 and s_0, and only these two, click or r_1 and s_1 click. Otherwise, if $\theta_a - \theta_b = \pm\pi$, then the state in Eq. (3) becomes

$$|0110 - 1001\rangle_{r_0 r_1 s_0 s_1}, \tag{6}$$

which means that either detectors r_0 and s_1 click, or r_1 and s_0 click. In all other cases, where $\theta_a - \theta_b = \pm\pi/2$, two random detectors out of four will click, and then Alice and Bob's qubits are independent of each other. Such events will be ruled out by a standard basis-sift procedure. Detection events on only reference (signal) detectors will be ruled out as well, justifying the choice of relevant terms in Eq. (2). In the end, Alice and Bob's bits, determined by relative phases θ_a and θ_b, will be correlated or anticorrelated conditioned on the detection events in the relay.

Similar to the single-photon case of the original MDI-QKD scheme [20], the key rate formula for our MDI-QKD scheme follows Shor-Preskill's result [5,6]

$$R \geqslant Y_{11}[1 - fH(e_{11}) - H(e_{11})], \tag{7}$$

where Y_{11} is the successful detection (trigger in the relay) rate provided that Alice and Bob send out single photons; e_{11} is the quantum bit error rate (QBER); f is the error correction inefficiency (see, e.g, [49]; normally, $f \geqslant 1$ with the Shannon limit of $f = 1$); and $H(x)$ is the binary entropy function, $H(x) = -x \log_2(x) - (1-x) \log_2(1-x)$. In Appendix A, we derive the relevant terms in Eq. (7) when loss and other nonidealities are taken into account [see Eqs. (A9) and (A11)].

Our single-photon MDI-QKD scheme offers certain advantages over similar schemes in [20,21]. A key difference of our scheme with the original MDI-QKD scheme in [20] lies on their encoding procedures. In the scheme of Fig. 1, the qubit information is encoded in the relative phases of two orthogonal optical modes. The original scheme, on the other hand, relies on polarization encoding, which requires sharing a polarization reference between all three parties and polarization maintenance along the channel. As compared to the MDI-QKD scheme II in [21], if used with single photons, both schemes use similar phase encoding, and are resilient to overall phase errors. In our case, the detection setup is simpler: it does not rely on optical switches and, as we will show in the next section, it can operate by using only two detectors. Note that, for the partial BSM part, all schemes require indistinguishable photons, hence filtering before the BSM modules is necessary.

The scheme in Fig. 1 relies on single-photon states for its proper operation. In practice, on-demand single-photon sources can be implemented using parametric down-conversion processes [50], or by relying on quasiatomic systems such as quantum dots [51]. In these scenarios, one must consider the effect of multiple photons on system performance, which will be addressed in a separate publication. With recent advancements in compact cost-effective single-photon sources, the reliance on single-photon states in our scheme is not necessarily a setback, especially when considering the

simplicity of the BSM module as compared to those proposed in [20,21]. Nevertheless, in Sec. IV, we present the decoy-state version of our protocol, which does not rely on single-photon sources.

The setup in Fig. 1 requires two optical channels for each user, which seems redundant and requires relative phase maintenance between the two channels. In the following section, we show that, by using a simple time-multiplexing trick, one can resolve both issues.

III. MDI-QKD WITH TIME MULTIPLEXING

Instead of path encoding, Alice and Bob can use time multiplexing to separate their reference and signal modes. That can be achieved by using Mach-Zehnder interferometers at the transmitter, as shown in Fig. 2. That would result in both reference and signal pulses traveling along the same physical channel. Moreover, if the time delay between the two modes is sufficiently short, we can reliably assume that the relative phase between the reference and signal modes is well preserved along the channel, as required in Fig. 1. The BSM module in Fig. 2 is also simpler than that of Fig. 1, as we are only using two, rather than four, single-photon detectors. It is also simpler than the proposed BSM modules in [20,21], as it does not require optical switches or phase-to-polarization converters. Similar to any other schemes, time synchronization is required to ensure that the corresponding reference and signal modes will arrive at the right time and properly interfere with each other.

The main problem that must be addressed in this time-multiplexed scheme is the dead time of single-photon detectors. That is, after detection, a detector will be nonresponsive (dead) for a period of time until it resets. The dead time of a detector is caused by the after-pulse effect in avalanche photodiode single-photon detectors. In the time-multiplexed scheme, the detectors are required to detect photons in two consecutive pulses, whose time difference could be short. The dead time of detectors then ultimately limits the repetition rate of the proposed scheme. Here, we propose proper postselection methods to address the dead-time problem.

For the postselection of events, at the BSM module of Fig. 2, we consider two scenarios. In the first scenario, we assume that the dead time of single-photon detectors is shorter than the delay in Mach-Zehnder interferometers. In this case, we can use exactly the same postselection technique as described in Sec. II. The only difference would be that for the time slot corresponding to signal pulses, detectors r_0 and r_1 in Fig. 2 resemble detectors s_0 and s_1 in Fig. 1. With recent advances in single-photon detectors with ultrashort dead times [52,53],
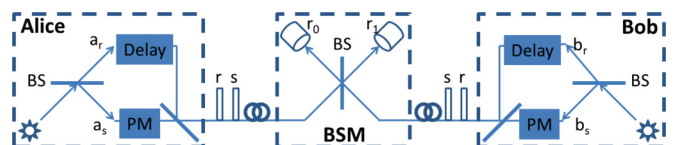

FIG. 2. (Color online) A schematic diagram of the time-multiplexed MDI-QKD protocol. Alice and Bob each encodes their qubits onto relative phases of two optical modes separated in time, a_r, a_s, b_r and b_s, respectively. The partial BSM, using a $50:50$ BS, is performed in the relay owned by a possibly untrusted party.

one can use a repetition rate as high as 500 MHz with our scheme. In order to go to higher repetition rates, one must use a delay possibly shorter than the detector's dead times. From the discussion of Eqs. (5) and (6), we notice that only when Alice and Bob's results are correlated (they have used the same phase), is the dead-time issue problematic. In order to resolve this issue, Alice and Bob can further sift out those detection events resulting from the terms in Eq. (5). That is, by accepting a factor of 1/2 loss in the final key rate, we will only keep measurement results in which both r_0 and r_1 click, each at a different time slot corresponding to the arrival of the reference or signal beams. With the above modified postselection technique, the setup in Fig. 2 provides comparable secret key generation rates to other single-photon MDI-QKD schemes, while offering a simple and cost-effective structure.

The setup in Fig. 2 can be easily modified to implement encoding in all three Pauli bases. If we represent the standard basis vectors, i.e., eigenvectors of the Z operator, by a single-photon state in the reference mode and a single-photon state in the signal mode, the encodings implemented by the setup of Fig. 2 are that of X and Y bases. If one replaces the first beam splitter in the encoder with a polarizing beam splitter, and uses horizontally or vertically polarized light at the source [54], we can use the same setup for Z-basis encoding as well. In the case of single-photon sources, which of two bases to choose for the QKD protocol is arbitrary. Once we consider the decoy-state version of our protocol, however, the choice of bases is more crucial. In fact, it turns out that X and Y bases are prone to a larger value of QBER than the Z basis. That is why, in the experimental setup of [42,44], Z- and X-basis encoding is used. A brief analysis of the decoy-state version of the MDI-QKD protocol with Z- and X-basis encoding is given in [20], which we will rederive within our own setup in Appendix B. In the next section, however, we will consider the more challenging X- and Y-basis encoding for the decoy-state protocol and propose postselection techniques to reduce the QBER in such a scenario.

IV. DECOY-STATE MDI-QKD

In this section, the decoy-state version of our scheme is presented. A weak laser pulse is perhaps the easiest way to approximate a single-photon state. Due to the multiple-photon component in a laser pulse, in the context of QKD, coherent-state sources are considered to be basis dependent [55]. For a basis-dependent source, one can apply decoy-state technique to monitor the channel transmittance of the single-photon component in the source [40,56–58].

In the security proof of the decoy-state scheme, the overall phase of the coherent-state source is assumed to be randomized [40,59]. The main problem with using phase-randomized coherent states, in the setup of Fig. 1, is that the probability of a single photon coming out of Alice's source and a single photon from Bob's source is on the same order as the case of having two photons at Alice's or Bob's, and no photon out of the other source. The former is what we need to generate a secret key bit, whereas the latter could result in random clicks. In fact, the QBER, in the scheme of Fig. 1, could be over 20% if we use a standard decoy-state protocol. In order to resolve this issue, in this section, we assume that Alice and Bob have

a common overall phase reference. We then use an improved phase-post-selection technique to enhance the efficiency of error correction. We remark that a full security proof of this technique is yet to be addressed.

A. Key rate

The security analysis for our scheme with decoy states follows from that of [20,21], which rely on the photon-number channel model used in [40]. The key rate for the original decoy-state QKD is given by [40,60]

$$R \geqslant q\{-Q_\mu f H(E_\mu) + Q_1[1 - H(e_1)] + Q_0\}, \quad (8)$$

where q is the basis sift factor; the subscript μ denotes the average number of photons per pulse; Q_μ and E_μ are, respectively, the overall gain and QBER; Q_1 and e_1 are, respectively, the gain and the error rate of the single-photon components; and Q_0 is the gain of the vacuum state (from background).

There are certain details to be considered before applying Eq. (8) to our case. The basis sift factor q is equal to $1/2$ in the original BB84 protocol due to the fact that half of the time the bases chosen by Alice and Bob disagree. In the efficient BB84 protocol [61], however, the factor q can approach 1 in the infinite-size key limit. In our MDI-QKD scheme, there is an extra factor of $1/2$ due to the partial BSM described in Sec. II. If one uses the correlation sift technique to handle the dead-time problem as discussed in Sec. III, another factor of $1/2$ must also be accounted for. In our key-rate analysis, described in Appendix B, we merge this factor q into other gain factors to obtain

$$R \geqslant Q_{11}[1 - H(e_{11})] + Q'_{0\mu_b} - I_{ec},$$
$$I_{ec} = Q_{\mu_a \mu_b} f H(E_{\mu_a \mu_b}), \quad (9)$$

where I_{ec} is the cost of error correction; $Q_{\mu_a \mu_b}$ ($E_{\mu_a \mu_b}$) is the overall gain (QBER) when Alice and Bob, respectively, use an average photon number of μ_a and μ_b; Q_{11} (e_{11}) is the gain (QBER) when both sources generate single-photon states; and $Q'_{0\mu_b} = \exp(-\mu_a)Q_{0\mu_b}$ is the probability that there is no photon from Alice's side *and* a successful BSM occurs. Appendix B provides detailed definitions for the above parameters.

Here, we assume that Alice and Bob use forward classical communication (Alice to Bob) for error correction and privacy amplification, which leads to the $Q'_{0\mu_b}$ term in the key rate formula in Eq. (9). The security argument behind it is that when Alice sends out vacuum states, Eve gains nothing about Alice's qubits by measuring the state in the channel [60,62]. Of course, one can assume that Alice and Bob perform reverse reconciliation, in which case $Q'_{0\mu_b}$ must be replaced with $Q'_{\mu_a 0} = \exp(-\mu_b)Q_{\mu_a 0}$. We emphasize that, because of relying on two photons for a successful BSM, $Q'_{0\mu_b}$ is on the same order of $Q_{\mu_a \mu_b}$ for coherent-state sources. Thus, its contribution is significant. On the contrary, for the key rate of a regular decoy-state QKD given by Eq. (8), the contribution from the vacuum state, Q_0, is insignificant due to the fact that normally the background count rate is much lower than Q_μ.

Note that, in MDI-QKD schemes, postprocessing can be performed separately on bit strings obtained from different

bases [63], or from different detection events (correlated and anticorrelated). In practice, this extra information may be useful for error correction [32].

B. MDI-QKD with phase postselection

As mentioned before, the intrinsic QBER in our decoy-state scheme can be very high if one uses a fully phase-randomized coherent source. Note that randomization of the overall phase over $[0,2\pi)$ can be regarded as randomization over one of the following N regions:

$$\left\{\left[\frac{m\pi}{N},\frac{(m+1)\pi}{N}\right)\cup\left[\frac{(m+N)\pi}{N},\frac{(m+N+1)\pi}{N}\right)\Big|m\right.$$
$$\left.=0,1,2,N-1\right\}. \qquad (10)$$

The choice of the region and the overall phase therein are random at the source. In the conventional decoy-state protocol, no information about the overall phase is exchanged between two users. In our scheme, before error correction, Alice and Bob would reveal which region they had used. They would only keep raw key bits for which they both have used the same phase region. This extra information would reduce the cost of error correction, because the QBER is different for the raw key from different regions. In fact, in Fig. 3, we can see that by using $N=4$ and $N=8$, corresponding to, respectively, two and three bits of classical information, the QBER has been reduced to below 5% and 1.3%. In Fig. 3, we have assumed that $\eta_a\mu_a=\eta_b\mu_b$, where η_a and η_b are, respectively, the total transmission efficiency for Alice and Bob's paths. In Appendix B, we show that the QBER $E_{\mu_a\mu_b}$ is minimized under this condition. Note that Alice and Bob do not need to control the phases of coherent states precisely, which is practically
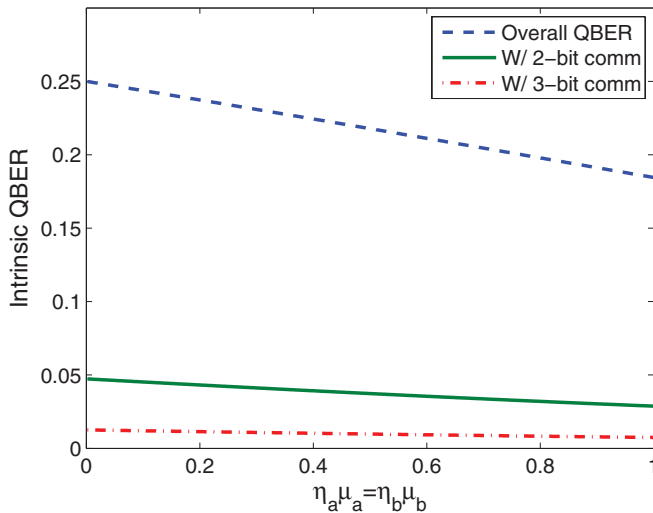

FIG. 3. (Color online) QBER for the MDI-QKD scheme in Fig. 1 with coherent-state sources, conditioned on partial knowledge of the overall phase. The overall QBER, calculated by Eq. (B15), represents the case where no phase information is shared. Curves labeled "W/2(3)-bit comm" represent cases where Alice and Bob postselect states coming from the same phase region, out of $N=4(8)$ phase bands in Eq. (10). The conditional QBER is calculated numerically using Eq. (B20). No background noise or misalignment is assumed.

challenging. Instead, as long as they know the phase partition in Eq. (10) with a high probability, the phase postselection method proposed here can be implemented. We leave the case where Alice and Bob do not exactly know the phase values for future study.

Conditioned on the classical bits Alice sends to Bob, the cost of error correction in Eq. (9) is given by

$$I_{\rm ec}=\sum_m Q^m f H(E^m), \qquad (11)$$

where m is the partition index in Eq. (10), and Q^m and E^m are the corresponding conditional gain and QBER [see Eqs. (B19) and (B20)].

Our numerical calculations show that the key rate given by Eqs. (9) and (11) is not positive for the parameter set listed in Table I. If, however, one assumes the gain and error rates of single-photon states are evenly distributed over the partitions of Eq. (10), the key rate formula, Eq. (9), becomes

$$R\geqslant\frac{1}{N}Q_{11}[1-H(e_{11})]-Q^m f H(E^m)|_{m=0}, \qquad (12)$$

where we take the lower bound of $Q'_{0\mu_b}\geqslant 0$. Here, we only keep the term corresponding to $m=0$ in Eq. (11), in which case E^m is minimized.

C. Key-rate comparison

In this section, we numerically compare the secret key generation rate for the MDI-QKD schemes proposed here using single-photon and decoy-coherent states with that of [20]. For fair comparison, we use the same parameter values used in [20] for our numerical evaluation, which follow the experiment reported in [64] (see also [65]). The numerical parameters used are listed in Table I. We have used Eq. (12) and formulas in Appendices A and B to evaluate the key rate of our decoy-state scheme.

Figure 4 shows the secret key generation rate for the three schemes mentioned above. The middle curve corresponds to that of the original MDI-QKD scheme [20], obtained from Eq. (B27). It can be seen that while our single-photon scheme can outperform the original MDI-QKD scheme, our decoy-state protocol falls short of achieving the same performance. Nevertheless, both our schemes offer simpler BSM modules than what proposed in [20,21]. One of the reasons why the key rate of our scheme is lower than the original scheme is the additional phase postselection factor of $N=8$.

The key rate in our scheme (and the original scheme [20]) scales better with distance than that of scheme I in [21]. The

TABLE I. List of experimental parameters used in numerical results: p_d is the background count rate per detector; f is the error correction inefficiency; and e_d is the misalignment error between Alice and Bob, which characterizes the stability of the relative phases at the encoders and through the channel. Note that two detectors are used in the original experiment [64], thus p_d should be roughly half of the total background count rate.

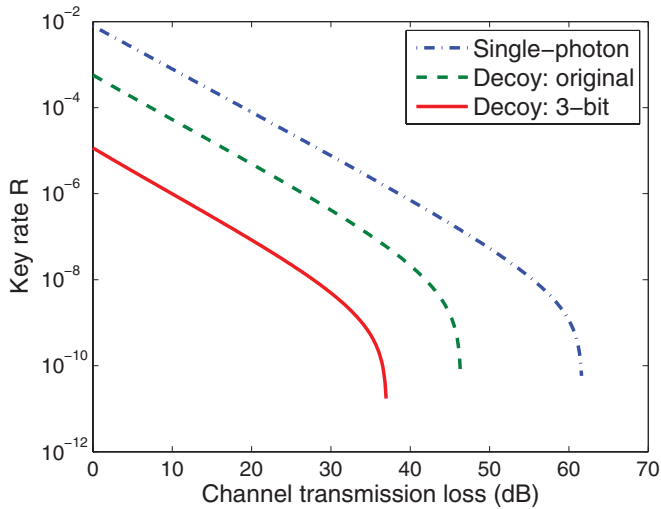| Quantum efficiency	p_d	f	e_d
14.5%	3.0×10^{-6}	1.16	1.5%

FIG. 4. (Color online) Key rate comparison for single-photon and decoy-state MDI-QKD schemes. The setup parameters are listed in Table I. The solid line indicates the key rate for the X–Y-basis-encoding scheme with decoy states plus three-bit communication for overall phase postselection, shown in Eq. (12). The dashed line shows the performance of the original MDI-QKD with X–Z-basis encoding. The related formulas for simulation can be found in Appendices A and B. The μ's are optimized for the two decoy-state curves.

latter yields a key rate scaling quadratically with the channel transmittance, whereas in our scheme, it scales linearly. This is because the optimal μ of scheme I is on the same order of the transmission efficiency as shown in [21], whereas the optimal μ in our scheme is on the order of 1, as shown in Fig. 5.

From Fig. 5, one can see that the optimal μ in our scheme is smaller than the one given by the original MDI-QKD. This is because in our scheme, multiphoton states would introduce false triggers in the BSM relay, which causes an error rate of
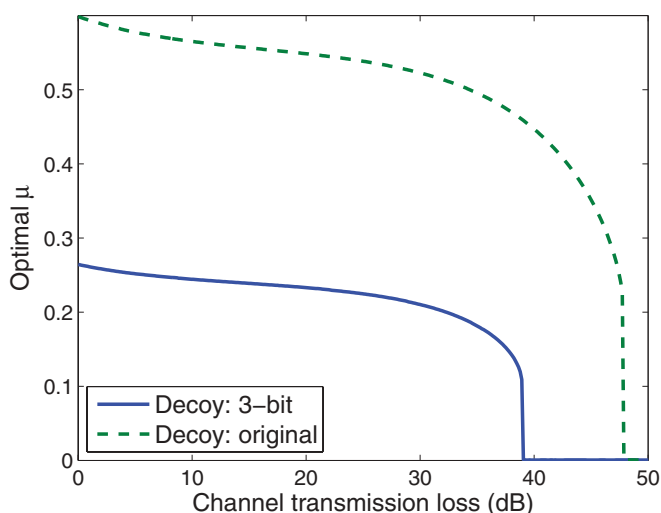

FIG. 5. (Color online) Optimal average photon number of coherent state for the X–Y-basis-encoding scheme (solid line) and the original MDI-QKD scheme (dashed line, X–Z encoding) with decoy states. The setup parameters are listed in Table I and the related formulas can be found in Appendix B.

$1/2$. In order to reduce such an effect, a smaller μ should be used. This is another reason why the key rate of our decoy-state scheme is lower than the original one, as shown in Fig. 4. We remark that the key rate is quite stable with certain changes of μ, except for the regime where the channel loss is close to the maximal tolerable one.

V. CONCLUDING REMARKS

Measurement-device-independent schemes have been proposed to close the detection loopholes in QKD systems. In this paper, we presented phase-encoding MDI-QKD setups that could offer certain practical advantages over previously proposed schemes in [20,21]. If implemented with single-photon states, our scheme enjoys a simple detection setup, consisting of only two single-photon detectors and a 50 : 50 beam splitter, with little or no compromise on the performance. Polarization or overall phase maintenance through quantum channels is not required in our schemes, either. This is an advantage over the polarization scheme in [20] or the phase-encoding schemes in [21]. There are different decoy-state versions one can implement using our setup. The original MDI-QKD is effectively using an X–Z-basis encoding, with a lower QBER for the Z basis. Here we showed that, by a proper overall phase selection scheme, we could achieve positive secret key rates even if we used X and Y bases for encoding over a moderately long range of distances. We remark that the security of the phase postselection technique described in Appendix B 2 needs to be further investigated. Similar questions were raised for DIQKD schemes [32].

For a full key rate analysis, finite-key effects and statistical fluctuations must also be considered. That would include fluctuation analysis for decoy states [57] as well as phase error estimations [63,66]. We remark that the statistical fluctuation analysis for the MDI-QKD with decoy states has been recently presented [54]. Other finite-key effects, such as authentication, are expected to be negligible compared to the above two effects in a large parameter set [63].

In the current MDI-QKD realizations [20,21], including the one we propose here, we assume Alice and Bob use the same source settings. It is interesting to study the case where two source settings are different. For instance, one of the parties uses coherent states with the decoy-state protocol and the other one uses single-photon states.

We finally remark that our proposed scheme can be easily adapted to quantum network settings [67,68]. For a single-hop network, the switching center is a collection of several BSM modules along with switching and controlling devices. For longer distances, one can connect two switching centers with quantum repeaters [46,47,69–72] and effectively enable any two users to exchange secret keys. One of the key advantages of such a setup is the simplicity and the low cost of local users' equipment (the optical source), while the more expensive part, i.e., detectors, are shared among all users.

APPENDIX A : MDI-QKD WITH SINGLE-PHOTON STATES

In this appendix, we will consider channel losses, background counts, and misalignment errors for the scheme introduced in Sec. II. The initial joint state of Alice and Bob is given by Eq. (1). After passing through lossy channels, modeled by beam splitters with transmissivities η_a and η_b, and considering the normalization factors, the state in Eq. (1) becomes a mixed state as follows:

$$
\frac{\eta_a \eta_b}{4} |\psi_{11}\rangle\langle\psi_{11}| + \frac{\eta_a(1-\eta_b)}{2}|\psi_{10}\rangle\langle\psi_{10}|
$$
$$
+ \frac{(1-\eta_a)\eta_b}{2}|\psi_{01}\rangle\langle\psi_{01}| + (1-\eta_a)(1-\eta_b)|\psi_{00}\rangle\langle\psi_{00}|,
$$
$$(A1)$$

where

$$
\begin{aligned}
|\psi_{11}\rangle &= |1010\rangle + e^{i\theta_a}|0110\rangle + e^{i\theta_b}|1001\rangle + e^{i(\theta_a+\theta_b)}|0101\rangle, \\
|\psi_{10}\rangle &= |1000\rangle + e^{i\theta_a}|0100\rangle, \\
|\psi_{01}\rangle &= |0010\rangle + e^{i\theta_b}|0001\rangle, \\
|\psi_{00}\rangle &= |0000\rangle.
\end{aligned}
$$
$$(A2)$$

Here, as a shorthand notation, in the above equation $|abcd\rangle$ represents the joint number state $|abcd\rangle_{a_r a_s b_r b_s}$.

The state in Eq. (A1) will then pass through beam splitters in the relay, as described in Eq. (4). The state $|\psi_{11}\rangle$ is transformed to

$$
[|1010\rangle + e^{i\theta_a}|0110\rangle + e^{i\theta_b}|1001\rangle + e^{i(\theta_a+\theta_b)}|0101\rangle]
$$
$$
\mapsto \frac{1}{\sqrt{2}}|02-20\rangle|00\rangle + \frac{1}{2}e^{i\theta_a}|01-10\rangle|01+10\rangle
$$
$$
+ \frac{1}{2}e^{i\theta_b}|01+10\rangle|01-10\rangle + \frac{1}{\sqrt{2}}e^{i(\theta_a+\theta_b)}|00\rangle|02-20\rangle,
$$
$$(A3)$$

where the optical modes a_r, a_s, b_r, and b_s are mapped to r_0, r_1, s_0, and s_1. Here, we used the following transformations corresponding to a 50 : 50 beam splitter:

$$
\begin{aligned}
|0\rangle_{a_r}|0\rangle_{b_r} &\mapsto |0\rangle_{r_0}|0\rangle_{r_1}, \\
|1\rangle_{a_r}|1\rangle_{b_r} &\mapsto [|0\rangle_{r_0}|2\rangle_{r_1} - |2\rangle_{r_0}|0\rangle_{r_1}]/\sqrt{2}, \\
|0\rangle_{a_s}|0\rangle_{b_s} &\mapsto |0\rangle_{s_0}|0\rangle_{s_1}, \\
|1\rangle_{a_s}|1\rangle_{b_s} &\mapsto [|0\rangle_{s_0}|2\rangle_{s_1} - |2\rangle_{s_0}|0\rangle_{s_1}]/\sqrt{2},
\end{aligned}
$$
$$(A4)$$

where the arrived photons are assumed to be indistinguishable, say, by passing through proper filters, such as polarization and frequency filters, before the partial BSM.

Similarly, other states in Eq. (A2) are transformed to

$$
\begin{aligned}
|1000\rangle + e^{i\theta_a}|0100\rangle &\mapsto [|01+10\rangle|00\rangle \\
&\quad + e^{i\theta_a}|00\rangle|01+10\rangle]/\sqrt{2}, \\
|0010\rangle + e^{i\theta_b}|0001\rangle &\mapsto [|01-10\rangle|00\rangle \\
&\quad + e^{i\theta_a}|00\rangle|01-10\rangle]/\sqrt{2}, \\
|0000\rangle &\mapsto |0000\rangle.
\end{aligned}
$$
$$(A5)$$

Define a successful partial BSM event to be the case when exactly one of the two detectors in each mode of the relay (that is, r_0 and s_0, r_0 and s_1, r_1 and s_0, or r_1 and s_1) clicks, as shown in Fig. 1. The yield Y_{11} is defined as the probability to have a successful measurement event, given that both Alice and Bob send out single-photon states and choose the same basis (that is, $\theta_a - \theta_b = 0, \pi$).

When Alice and Bob's bits are correlated ($\theta_a - \theta_b = 0$), Eq. (A3) becomes

$$
[|1010\rangle + e^{i\theta_a}|0110\rangle + e^{i\theta_b}|1001\rangle + e^{i(\theta_a+\theta_b)}|0101\rangle]
$$
$$
\mapsto \frac{1}{\sqrt{2}}|02-20\rangle|00\rangle + e^{i\theta_a}|0101-1010\rangle
$$
$$
+ \frac{1}{\sqrt{2}}e^{2i\theta_a}|00\rangle|02-20\rangle,
$$
$$(A6)$$

where the second term on the right-hand side is the postselected term mentioned in Eq. (5).

With Eqs. (A1), (A2), (A5), and (A6), we can calculate the probability for a single click in each mode when $\theta_a - \theta_b = 0$,

$$
\begin{aligned}
{}_0Y_{11}^{r_0 s_0} = {}_0Y_{11}^{r_1 s_1} &= (1-p_d)^2 \Bigg[\frac{\eta_a \eta_b}{4} + \left(\frac{\eta_a + \eta_b}{2} - \frac{3\eta_a\eta_b}{4} \right) p_d \\
&\quad + (1-\eta_a)(1-\eta_b)p_d^2 \Bigg], \\
{}_0Y_{11}^{r_0 s_1} = {}_0Y_{11}^{r_1 s_0} &= (1-p_d)^2 \Bigg[\left(\frac{\eta_a + \eta_b}{2} - \frac{3\eta_a\eta_b}{4} \right) p_d \\
&\quad + (1-\eta_a)(1-\eta_b)p_d^2 \Bigg],
\end{aligned}
$$
$$(A7)$$

where p_d is the background rate for one detector ($p_d \approx Y_0/2$). Due to the symmetry, the probabilities for the case when $\theta_a - \theta_b = \pi$ are similar:

$$
\begin{aligned}
{}_\pi Y_{11}^{r_0 s_0} = {}_\pi Y_{11}^{r_1 s_1} &= {}_0Y_{11}^{r_0 s_1}, \\
{}_\pi Y_{11}^{r_0 s_1} = {}_\pi Y_{11}^{r_1 s_0} &= {}_0Y_{11}^{r_0 s_0}.
\end{aligned}
$$
$$(A8)$$

Thus the yield Y_{11}, defined as the total probability to have a successful measurement event when Alice and Bob use the same basis, is given by the summation of the terms in Eq. (A7) [or Eq. (A8)] as follows:

$$
\begin{aligned}
Y_{11} &= {}_0Y_{11}^{r_0 s_0} + {}_0Y_{11}^{r_1 s_1} + {}_0Y_{11}^{r_0 s_1} + {}_0Y_{11}^{r_1 s_0} \\
&= (1-p_d)^2 \Bigg[\frac{\eta_a \eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_d \\
&\quad + 4(1-\eta_a)(1-\eta_b)p_d^2 \Bigg].
\end{aligned}
$$
$$(A9)$$

When $p_d = 0$, $Y_{11} = \eta_a\eta_b/2$, which is reasonable because the probability of the two optical modes each containing exactly one photon is $1/2$.

An error may occur when $\theta_a - \theta_b = 0$ but an anticorrelated detection signal comes out; that is, detectors r_0 and s_1, or r_1 and s_0 click. Thus, the error rate due to background noise is given by

$$
\begin{aligned}
e'_{11} Y_{11} = {}_0 Y_{11}^{r_0 s_1} + {}_0 Y_{11}^{r_1 s_0} &= (1 - p_d)^2 \left[\left(\eta_a + \eta_b - \frac{3\eta_a \eta_b}{2} \right) p_d \right. \\
&\quad + \left. 2(1 - \eta_a)(1 - \eta_b) p_d^2 \right] \\
&= e_0 (1 - p_d)^2 \left[(2\eta_a + 2\eta_b - 3\eta_a \eta_b) p_d \right. \\
&\quad + \left. 4(1 - \eta_a)(1 - \eta_b) p_d^2 \right],
\end{aligned} \tag{A10}
$$

where $e_0 = 1/2$ is the error rate of a random (background) noise. Now considering possible phase errors, i.e., the deviation of $\Delta_\theta = \theta_a - \theta_b$ from its nominal value, the total error rate is given by

$$
\begin{aligned}
e_{11} Y_{11} &= (1 - p_d)^2 \left[e_d \frac{\eta_a \eta_b}{2} + e_0 (2\eta_a + 2\eta_b - 3\eta_a \eta_b) p_d \right. \\
&\quad + \left. 4 e_0 (1 - \eta_a)(1 - \eta_b) p_d^2 \right] \\
&= e_0 Y_{11} - (e_0 - e_d)(1 - p_d)^2 \frac{\eta_a \eta_b}{2},
\end{aligned} \tag{A11}
$$

where e_d is approximately the variance of Δ_θ, accounting for channel relative-phase distortions (misalignment).

APPENDIX B : MDI-QKD WITH DECOY STATES

In this appendix, we calculate the key parameters in Eq. (9). As pointed out in [20], with an infinite number of decoy states, these parameters can be accurately estimated. One of the key assumptions in decoy-state analysis is the phase randomization at the source [57]. According to the photon channel model [40], with phase randomization, a coherent state can be regarded as a mixture of Fock states. In fact, any state can be treated as a mixture of Fock states when the phase of the Fock state component is randomized. In this appendix, we first consider the case when the phase is randomized over $[0, 2\pi)$, and then consider our phase postselection technique. For simplicity, we only consider the limit of the efficient BB84 scheme, where the basis-sift factor is approaching 1 [61]. That is, the difference between relative phases set by Alice and Bob in Fig. 1 is either 0 or π almost surely.

1. Coherent states with full phase randomization

Now, let us consider the case where phase-randomized coherent states are used [73]. According to the Poisson distribution of photon numbers in a coherent state, the gain of single-photon states Q_{11} defined as the probability that both Alice and Bob send out single-photon states with the same basis and obtain a successful partial BSM is given by

$$
Q_{11} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}, \tag{B1}
$$

where the yield Y_{11} is given by Eq. (A9).

Next, we evaluate the overall gain and QBER. Alice and Bob prepare coherent states with intensities μ_a and μ_b,

respectively, and randomize the phases

$$
\left| e^{i\phi_a} \sqrt{\mu_a} \right\rangle_a \left| e^{i\phi_b} \sqrt{\mu_b} \right\rangle_b, \tag{B2}
$$

where ϕ_a and ϕ_b are the overall randomized phases. Then, the photon sources are split into two orthogonal optical modes, labeled by r and s, by $50:50$ beam splitters, as described in Sec. II,

$$
\left| e^{i\phi_a} \sqrt{\frac{\mu_a}{2}} \right\rangle_{a_r} \left| e^{i(\theta_a + \phi_a)} \sqrt{\frac{\mu_a}{2}} \right\rangle_{a_s} \left| e^{i\phi_b} \sqrt{\frac{\mu_b}{2}} \right\rangle_{b_r} \left| e^{i(\theta_b + \phi_b)} \sqrt{\frac{\mu_b}{2}} \right\rangle_{b_s}, \tag{B3}
$$

where θ_a and θ_b are the relative phases Alice and Bob want to encode, as shown in Fig. 1. Transmitting through lossy channels, modeled by beam splitters, the joint state arrived at the relay can be expressed by

$$
\begin{aligned}
&\left| e^{i\phi_a} \sqrt{\frac{\eta_a \mu_a}{2}} \right\rangle_{a_r} \left| e^{i(\theta_a + \phi_a)} \sqrt{\frac{\eta_a \mu_a}{2}} \right\rangle_{a_s} \left| e^{i\phi_a} \sqrt{\frac{\eta_b \mu_b}{2}} \right\rangle_{b_r} \\
&\otimes \left| e^{i(\theta_b + \phi_b)} \sqrt{\frac{\eta_b \mu_b}{2}} \right\rangle_{b_s}.
\end{aligned} \tag{B4}
$$

After passing through the beam splitters in the relay, the state is transformed into, according to Eq. (4), four detection modes r_0, r_1, s_0 and s_1,

$$
\begin{aligned}
&\left| e^{i\phi_a} \frac{\sqrt{\eta_a \mu_a}}{2} + e^{i\phi_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right\rangle_{r_0} \left| e^{i\phi_a} \frac{\sqrt{\eta_a \mu_a}}{2} - e^{i\phi_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right\rangle_{r_1} \\
&\otimes \left| e^{i(\theta_a + \phi_a)} \frac{\sqrt{\eta_a \mu_a}}{2} + e^{i(\theta_b + \phi_b)} \frac{\sqrt{\eta_b \mu_b}}{2} \right\rangle_{s_0} \\
&\otimes \left| e^{i(\theta_a + \phi_a)} \frac{\sqrt{\eta_a \mu_a}}{2} - e^{i(\theta_b + \phi_b)} \frac{\sqrt{\eta_b \mu_b}}{2} \right\rangle_{s_1}.
\end{aligned} \tag{B5}
$$

Therefore, the detection probabilities for the four detectors are given by

$$
\begin{aligned}
D_{r_0} &= 1 - (1 - p_d) \exp \left(- \left| e^{i\phi_a} \frac{\sqrt{\eta_a \mu_a}}{2} + e^{i\phi_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right|^2 \right), \\
D_{r_1} &= 1 - (1 - p_d) \exp \left(- \left| e^{i\phi_a} \frac{\sqrt{\eta_a \mu_a}}{2} - e^{i\phi_b} \frac{\sqrt{\eta_b \mu_b}}{2} \right|^2 \right), \\
D_{s_0} &= 1 - (1 - p_d) \\
&\quad \times \exp \left(- \left| e^{i(\theta_a + \phi_a)} \frac{\sqrt{\eta_a \mu_a}}{2} + e^{i(\theta_b + \phi_b)} \frac{\sqrt{\eta_b \mu_b}}{2} \right|^2 \right), \\
D_{s_1} &= 1 - (1 - p_d) \\
&\quad \times \exp \left(- \left| e^{i(\theta_a + \phi_a)} \frac{\sqrt{\eta_a \mu_a}}{2} - e^{i(\theta_b + \phi_b)} \frac{\sqrt{\eta_b \mu_b}}{2} \right|^2 \right).
\end{aligned} \tag{B6}
$$

For simplicity, we use the following notations:

$$
\begin{aligned}
\mu' &= \eta_a \mu_a + \eta_b \mu_b, \\
\Delta_\phi &= \phi_b - \phi_a, \\
x &= \sqrt{\eta_a \mu_a \eta_b \mu_b}/2, \\
y &= (1 - p_d) e^{-\mu'/4}.
\end{aligned} \tag{B7}
$$

Here, μ' denotes the average number of photons reaching the relay, and Δ_ϕ denotes the difference between the random

overall phases set by Alice and Bob, which should be integrated over $[0, 2\pi)$. Then, Eq. (B6) can be simplified to

$$
\begin{aligned}
D_{r_0} &= 1 - y e^{-x \cos \Delta_\phi}, \\
D_{r_1} &= 1 - y e^{x \cos \Delta_\phi}, \\
D_{s_0} &= 1 - y e^{-x \cos(\Delta_\phi + \theta_a - \theta_b)}, \\
D_{s_1} &= 1 - y e^{x \cos(\Delta_\phi + \theta_a - \theta_b)}.
\end{aligned}
\tag{B8}
$$

The gain $Q_{\mu_a \mu_b}$ is defined as the probability that Alice and Bob choose the same basis and obtain a successful measurement, and is given by

$$
Q_{\mu_a \mu_b} = \left[D_{r_0}(1 - D_{r_1}) + (1 - D_{r_0})D_{r_1} \right] \left[D_{s_0}(1 - D_{s_1}) \right. \\
\left. + (1 - D_{s_0})D_{s_1} \right].
\tag{B9}
$$

Strictly speaking, Eq. (B9) should be averaged over random phases ϕ_a and ϕ_b, and different values for θ_a and θ_b. We delay this averaging until the last stage. By substituting Eq. (B8) into Eq. (B9), we have

$$
Q_{\mu_a \mu_b} = y^2 (e^{-x \cos \Delta_\phi} + e^{x \cos \Delta_\phi} - 2y)^2,
\tag{B10}
$$

where we use the fact that $|\theta_a - \theta_b| = 0, \pi$ when Alice and Bob choose the same basis. For a small μ' (thus, $\sqrt{\eta_a \mu_a \eta_b \mu_b} \leqslant \mu'/2$ is also small) and $p_d = 0$, the gain, Eq. (B10), will be approximated by

$$
Q_{\mu_a \mu_b} \to \left(\frac{\mu'}{2} \right)^2.
\tag{B11}
$$

Note that Eq. (B11) is independent of Δ_ϕ, which can be understood as follows. In the weak coherent-state limit ($\eta_a \mu_a \approx \eta_b \mu_b \ll 1$), there are two dominant terms in the relay: single-photon states on both sides versus a vacuum state on one arm and a two-photon state on the other. The vacuum state is not affected by the phase shift, and then the phase of the two-photon state will behave like an overall phase, which does not affect the measurement result. Also, as shown in Sec. II, the randomized phase does not affect the partial BSM of single-photon states. Thus, Eq. (B11) is independent of Δ_ϕ.

Now, we take the integral of Δ_ϕ for Eq. (B10),

$$
Q_{\mu_a \mu_b} = 2y^2 [1 + 2y^2 - 4y I_0(x) + I_0(2x)],
\tag{B12}
$$

where $I_0(x)$ is the modified Bessel function of the first kind. For small values of x, one can take the first-order approximation to $I_0(x) \approx 1 + x^2/4$ to verify that Eq. (B12) approaches Eq. (B11), when $p_d = 0$ and μ' is small. Note that in this weak coherent-state limit, the overall gain $Q_{\mu_a \mu_b}$ *cannot* be approximated by the gain of single-photon states, Q_{11} in Eq. (B1), because two-photon states cannot be neglected in this case. This is different from regular decoy-state QKD [57], where a coherent state can be approximated as a single-photon state when the intensity is low enough. We remark that this property will make the statistical fluctuation analysis more complicated for MDI-QKD.

Using Eq. (B12), we calculate $Q'_{0\mu_b}$ as follows:

$$
\begin{aligned}
Q'_{0\mu_b} &= e^{-\mu_a} Q_{0\mu_b} = 4(1 - p_d)^2 e^{-(1/2)\eta_b \mu_b - \mu_a} \\
&\quad \times [1 - (1 - p_d) e^{-(1/4)\eta_b \mu_b}]^2.
\end{aligned}
\tag{B13}
$$

The term $Q'_{0\mu_b}$ appears as an additive term in the key rate formula of Eq. (9) because we assume a forward classical

communication (Alice to Bob) is used for postprocessing [60,62]. The intuition behind it is that, when Alice sends out a vacuum state as an information carrier, no one (including Eve) can get any information about the final key (Alice's bit) by measuring the signals in the channel.

The overall QBER $E_{\mu_a \mu_b}$ is defined as the error rate in the sifted data. Similar to the derivation of Eq. (A11), due to symmetry, we only need to consider the case of $\theta_a - \theta_b = 0$. Without loss of generality, we assume $\theta_a = \theta_b = 0$, which leads to $D_{r_0} = D_{s_0}$ and $D_{r_1} = D_{s_1}$ in Eq. (B6). In this case, an error happens when the relay announces anticorrelated bits corresponding to clicks on r_1–s_0 and r_0–s_1 detectors. The intrinsic error rate, due to background noise and multiphoton states, is then given by

$$
\begin{aligned}
E'_{\mu_a \mu_b} Q_{\mu_a \mu_b} &= 2 D_{r_0}(1 - D_{r_1})(1 - D_{s_0}) D_{s_1} \\
&= 2y^2 (y - e^{x \cos \Delta_\phi})(y - e^{-x \cos \Delta_\phi}).
\end{aligned}
\tag{B14}
$$

It can be verified that Eq. (B14) is a decreasing function of x. The minimum of $E'_{\mu_a \mu_b} Q_{\mu_a \mu_b}$ is then obtained when $\eta_a \mu_a = \eta_b \mu_b$. Averaging over Δ_ϕ in Eq. (B10), we have

$$
E'_{\mu_a \mu_b} Q_{\mu_a \mu_b} = 2y^2 [1 + y^2 - 2y I_0(x)],
\tag{B15}
$$

where x and y are defined in Eq. (B7). Finally, considering relative-phase distortion errors, in a similar way to Eq. (A11), we obtain

$$
E_{\mu_a \mu_b} Q_{\mu_a \mu_b} = e_0 Q_{\mu_a \mu_b} - 2(e_0 - e_d) y^2 [I_0(2x) - 1].
\tag{B16}
$$

2. Phase randomization with postselection

If Alice and Bob randomly set the overall phases of their coherent sources, a large intrinsic QBER is accrued (see Fig. 3). From Eq. (B14), the intrinsic QBER is 0 if $\Delta_\phi = 0$, $\mu_a \eta_a = \mu_b \eta_b$, and $p_d = 0$. The condition $\Delta_\phi = 0$ implies that Alice and Bob must use the same overall phase value, which jeopardizes the security assumption that requires random-phase values. In order to reduce the cost of error correction, they can, however, inform each other at the sifting stage, the phase region they used in Eq. (10). We remark that this improved data postprocessing is originated from the one proposed in [32].

Let us take a look at a simple example where Alice sends Bob two-bit classical information for phase postselecting. Then, according to Eq. (10), they can divide the phase in $[0, 2\pi)$ into four partitions:

$$
\begin{aligned}
&\left\{ \left[\frac{m\pi}{4}, \frac{(m+1)\pi}{4} \right) \cup \left[\frac{(m+4)\pi}{4}, \frac{(m+5)\pi}{4} \right) \right| m \\
&= 0, 1, 2, 3 \Big\}.
\end{aligned}
\tag{B17}
$$

The two classical bits for each pulse are used to identify which partition they use for their random phases. Then, the cost of error correction is given by Eq. (9),

$$
I_{\text{ec}} = \sum_{m=0}^{3} Q^m f H(E^m),
\tag{B18}
$$

where, due to the symmetry, we can assume Alice picks up m from $\{0, 1, 2, 3\}$ randomly and Bob always uses $m = 0$.

The gain $Q_{\mu_a\mu_b}$ in Eq. (B10) should be averaged over Δ_ϕ from $m\pi/N$ to $(m+1)\pi/N$, yielding

$$Q^m = \frac{N}{\pi}\int_0^{\pi/N} d\phi_b \frac{1}{\pi}\int_{m\pi/N}^{(m+1)\pi/N} d\phi_a \, y^2$$
$$\times (e^{-x\cos\Delta_\phi} + e^{x\cos\Delta_\phi} - 2y)^2. \qquad (B19)$$

Similarly, for the QBER $E'_{\mu_a\mu_b}Q_{\mu_a\mu_b}$, one should take the integral of Eq. (B14) to obtain

$$E'^m Q^m = \frac{N}{\pi}\int_0^{\pi/N} d\phi_b \frac{1}{\pi}\int_{m\pi/N}^{(m+1)\pi/N} d\phi_a \, 2y^2$$
$$\times (y - e^{x\cos\Delta_\phi})(y - e^{-x\cos\Delta_\phi}). \qquad (B20)$$

The intrinsic QBERs for $m=0$ with two cases, $k=2$ and $k=3$, are shown in Fig. 3, where $k = \log_2 N$.

Let us consider the case when $\eta_a\mu_a = \eta_b\mu_b$, which minimizes the intrinsic QBER of Eq. (B14), hence $\mu' = 2\eta_a\mu_a$, $x = \eta_a\mu_a = \mu'/2$, and $y = (1-p_d)e^{-x}$. Assuming $p_d < \mu' \ll 1$, and using the first-order approximation to Eq. (B10), we obtain

$$Q^m = \frac{4}{N}y^2(1-y)^2 + O(\mu'^3), \qquad (B21)$$

which is independent of m, and for Eq. (B14),

$$E'^m Q^m = \frac{2}{N}y^2(1-y)^2 - \frac{2x^2y^3N}{\pi^2}$$
$$\times \int_0^{\pi/N} d\phi_b \int_{m\pi/N}^{(m+1)\pi/N} d\phi_a \cos^2\Delta_\phi + O(\mu'^3)$$
$$= \frac{2}{N}y^2(1-y)^2 - \frac{x^2y^3}{N} - \frac{x^2y^3N}{4\pi^2}A_{m,N} + O(\mu'^3), \qquad (B22)$$

where

$$A_{m,N} \equiv -\cos\left[\frac{2(-1+m)\pi}{N}\right] + 2\cos\left[\frac{2m\pi}{N}\right]$$
$$-\cos\left[\frac{2(1+m)\pi}{N}\right] \qquad (B23)$$

and we use the fact that $1 - y = O(\mu')$. From the numerical evaluation, we notice that Eq. (B22) gives a slightly higher value for QBER than the integral in Eq. (B20). Finally, similar to Eq. (B16), the overall QBER is given by

$$E^m Q^m \approx e_0 Q_{\mu_a\mu_b} - (e_0 - e_d)\left(\frac{2x^2y^3}{N} + \frac{x^2y^3N}{2\pi^2}A_{m,N}\right). \qquad (B24)$$

3. Randomized but equal overall phase

Assume Alice and Bob can somehow manage to meet $\Delta_\phi = 0$. Then, using Eq. (B9), the gain is given by

$$Q_{\mu_a\mu_b} = y^2(e^{-x} + e^x - 2y)^2, \qquad (B25)$$

and from Eq. (B14) the corresponding QBER is given by

$$E_{\mu_a\mu_b}Q_{\mu_a\mu_b} = e_0 Q_{\mu_a\mu_b} - (e_0 - e_d)y^2(e^x - e^{-x})^2. \qquad (B26)$$

One can evaluate the key rate using Eq. (9) by taking the lower bound of $Q'_{0\mu_b} = 0$. We numerically verified that the key rate obtained from Eqs. (B25) and (B26) is close to that of the original MDI-QKD scheme in [20] for the parameter set given in Table I.

4. The original MDI-QKD scheme

In our path-phase encoding scheme of Fig. 1, the four BB84 states are encoded by the relative phases of two orthogonal optical modes, r and s. If we think of single-photon states in r and s modes as a standard basis for qubit representation, our encoding uses the basis vectors of X and Y Pauli operators. In our setup, one can also encode key information directly onto modes r and s as the third basis (Z basis) for QKD. In fact, the rectilinear basis in the original MDI-QKD can be regarded as using this third basis. The diagonal basis in [20] is then equivalent to the X basis in our scheme.

Using the above correspondence, we reproduce the key rate formula for the original MDI-QKD scheme in [20], which is given by

$$R \geqslant Q_{11}[1 - H(e_{11})] - Q_{\text{rect}}f(E_{\text{rect}})H(E_{\text{rect}}), \qquad (B27)$$

where Q_{11} and e_{11} are, respectively, given by Eqs. (B1) and (A11), and Q_{rect} and E_{rect} are, respectively, the gain and the QBER in the rectilinear basis. The latter two are the only terms that we need to calculate here, as described below. Note that Q_{11} is the same for both rectilinear and diagonal bases.

In the rectilinear basis, Alice chooses one of the two r and s modes and sends a phase-randomized coherent state $|e^{i\phi_a}\sqrt{\mu_a}\rangle$. Similarly, Bob sends $|e^{i\phi_b}\sqrt{\mu_b}\rangle$ in one of the two modes. If different modes are chosen by Alice and Bob, then a click on one of the r detectors, in Fig. 1, as well as a click on one of the s detectors, correctly indicate the exchange of anticorrelated bits by Alice and Bob. If, however, they choose similar modes, and such a two-click event occurs, they mistakenly assign different bits to their raw keys, and that will be a source of error. The overall gain in the rectilinear basis is then given by the sum of detection probabilities in the above scenarios as follows:

$$Q_{\text{rect}} = Q_{\text{rect}}^{(C)} + Q_{\text{rect}}^{(E)}, \qquad (B28)$$

where

$$Q_{\text{rect}}^{(C)} = 2(1-p_d)^2 e^{-\mu'/2}[1 - (1-p_d)e^{-\eta_a\mu_a/2}]$$
$$\times [1 - (1-p_d)e^{-\eta_b\mu_b/2}] \qquad (B29)$$

represents the detection probability in the first scenario, and

$$Q_{\text{rect}}^{(E)} = 2p_d(1-p_d)^2 e^{-\mu'/2}[I_0(2x) - (1-p_d)e^{-\mu'/2}] \qquad (B30)$$

represents the detection probability in the second scenario, where μ' and x are defined in Eq. (B7). Note that the above equation also includes averaging over the randomized overall phase.

Finally, considering misalignment errors, we obtain

$$E_{\text{rect}}Q_{\text{rect}} = e_d Q_{\text{rect}}^{(C)} + (1 - e_d)Q_{\text{rect}}^{(E)}. \qquad (B31)$$

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] D. Mayers, J. ACM **48**, 351 (2001).

[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[7] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[9] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[10] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[11] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).

[12] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 073 (2007).

[13] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).

[14] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[15] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, New J. Phys. **13**, 013043 (2011).

[16] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).

[17] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[18] Z. Yuan, J. Dynes, and A. Shields, Nat. Photonics **4**, 800 (2010).

[19] Z. Yuan, J. Dynes, and A. Shields, Appl. Phys. Lett. **98**, 231104 (2011).

[20] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[21] K. Tamaki, H. K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

[22] D. Bohm and Y. Aharonov, Phys. Rev. **108**, 1070 (1957).

[23] P. M. Pearle, Phys. Rev. D **2**, 1418 (1970).

[24] X. Ma, T. Moroder, and N. Lütkenhaus, arXiv:0812.4301.

[25] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. **71**, 1675 (2000).

[26] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).

[27] D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE, Computer Society Press, Los Alamitos, 1998), p. 503.

[28] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[29] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[30] M. McKague and M. Mosca, in *Proceedings of the Fifth Conference on Theory of Quantum Computation, Communication, and Cryptography*, TQC'10 (Springer-Verlag, Berlin, Heidelberg, 2011), pp. 113–130.

[31] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[32] X. Ma and N. Lütkenhaus, Quantum Inf. Comput. **12**, 0203 (2012).

[33] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Phys. Rev. A **85**, 010301 (2012).

[34] Y. Zhao, B. Qi, and H. K. Lo, Phys. Rev. A **77**, 052327 (2008).

[35] X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, Opt. Lett. **33**, 2077 (2008).

[36] The two terminologies, detection-device independent and measurement-device independent, have the same meaning. In order to avoid possible confusion with the full device-independent case, we often use the term measurement-device independent.

[37] R. Kaltenbaek, R. Prevedel, M. Aspelmeyer, and A. Zeilinger, Phys. Rev. A **79**, 040302 (2009).

[38] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[39] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[40] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[41] In the security proof of the decoy-state scheme, the phases of quantum signals are assumed to be randomized [40]. Scheme I in [21], however, relies on nonrandom and identical phase reference for Alice and Bob [58]. The application of the decoy-state scheme to this setting is still an open question.

[42] A. Rubenok, J. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, arXiv:1204.0738.

[43] T. da Silva, D. Vitoreti, G. Xavier, G. Temporão, and J. von der Weid, arXiv:1207.6345.

[44] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, Q. Zhang, and J.-W. Pan, arXiv:1209.6178.

[45] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[46] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).

[47] N. Sangouard, C. Simon, J. Minar, H. Zbinden, H. de Riedmatten, and N. Gisin, Phys. Rev. A **76**, 050301 (2007).

[48] The three main dimensions that might need filtering are polarization, frequency, and time.

[49] G. Brassard and L. Salvail, in *Advances in Cryptology EUROCRYPT '93*, edited by G. Goos and J. Hartmanis (Springer-Verlag, Berlin, 1993).

[50] J. H. Shapiro and F. N. Wong, Opt. Lett. **32**, 2698 (2007).

[51] M. B. Ward, O. Z. Karimov, D. C. Unitt, Z. L. Yuan, P. See, D. G. Gevaux, A. J. Shields, P. Atkinson, and D. A. Ritchie, Appl. Phys. Lett. **86**, 201111 (2005).

[52] Z. Yuan, B. Kardynal, A. Sharpe, and A. Shields, Appl. Phys. Lett. **91**, 041114 (2007).

[53] A. R. Dixon, J. F. Dynes, Z. L. Yuan, A. W. Sharpe, A. J. Bennett, and A. J. Shields, Appl. Phys. Lett. **94**, 231113 (2009).

[54] X. Ma, C.-H. F. Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[55] X. Ma, C.-H. F. Fung, and H. K. Lo, Phys. Rev. A **76**, 012307 (2007).

[56] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[57] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[58] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005). Phys. Rev. A **72**, 012322 (2005).

[59] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 0431 (2007).

[60] H.-K. Lo, Quantum Inf. Comput. **5**, 413 (2005).

[61] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).

[62] M. Koashi, New J. Phys. **11**, 045018 (2009).

[63] X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. Chau, Comput. Secur. **30**, 172 (2011).

[64] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Öemer, M. Füerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Nat. Phys. **3**, 481 (2007).

[65] X. Ma and H.-K. Lo, New J. Phys. **10**, 073018 (2008).

[66] C.-H. F. Fung, X. Ma, and H. F. Chau, Phys. Rev. A **81**, 012318 (2010).

[67] H. J. Kimble, Nature (London) **453**, 1023 (2008).

[68] M. Razavi, IEEE Trans. Commun. **60**, 3071 (2012).

[69] M. Razavi and J. H. Shapiro, Phys. Rev. A **73**, 042303 (2006).

[70] J. Amirloo, M. Razavi, and A. H. Majedi, Phys. Rev. A **82**, 032304 (2010).

[71] M. Razavi, M. Piani, and N. Lütkenhaus, Phys. Rev. A **80**, 032301 (2009).

[72] N. Lo Piparo and M. Razavi, arXiv:1210.8042.

[73] Any other states can be applied here with certain modifications in the formulas, mainly in the photon-number distribution.