Phase-Matching Quantum Key Distribution

Xiongfeng Ma,[*] Pei Zeng, and Hongyi Zhou

Center for Quantum Information, Institute for Interdisciplinary Information Sciences,
Tsinghua University, Beijing 100084, China

Quantum key distribution allows remote parties to generate information-theoretic secure keys. The bottleneck throttling its real-life applications lies in the limited communication distance and key generation speed, due to the fact that the information carrier can be easily lost in the channel. For all the current implementations, the key rate is bounded by the channel transmission probability η. Rather surprisingly, by matching the phases of two coherent states and encoding the key information into the common phase, this linear key-rate constraint can be overcome—the secure key rate scales with the square root of the transmission probability $O(\sqrt{\eta})$, as proposed in twin-field quantum key distribution [M. Lucamarini *et al.* *Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters*, Nature (London) **557**, 400 (2018)]. To achieve this, we develop an optical-mode-based security proof that is different from the conventional qubit-based security proofs. Furthermore, the proposed scheme is measurement device independent; i.e., it is immune to all possible detection attacks. The simulation result shows that the key rate can even exceed the transmission probability η between two communication parties. In addition, we apply phase postcompensation to devise a practical version of the scheme without phase locking, which makes the proposed scheme feasible with the current technology. This means that quantum key distribution can enjoy both sides of the world—practicality and security.

Subject Areas: Quantum Information

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is the most successful application in quantum information science, whose security was proved at the end of the last century [3–5]. Since then, there has been a tremendous interest in developing this quantum technology for real-life applications, starting from the first 32-cm demonstration in the early 1990s [6] to the recent satellite QKD over 1200 km [7]. In these implementations, photons are used as information carriers, owing to their fast transmission speed and robustness against decoherence from the environment. Also, optical quantum communication can be easily integrated with the current telecommunication network infrastructure.

Now, the transmission loss of photons has become a major obstacle in practical implementations. The quantum channel transmission efficiency is characterized by the transmittance η, defined as the probability of a photon being successfully transmitted through the channel and being detected. For most of the current implemented schemes, such as the well-known Bennet-Brassard 1984 (BB84) protocol [1], single-photon sources [8] are employed for key information encoding. Since the photon carries the quantum information, when it is lost in the channel, no secure key can be distributed. Thus, the transmittance η becomes a natural upper bound of the key generation rate. A more strict derivation shows a linear key-rate bound with respect to the transmittance [9–11], $R \leq O(\eta)$. Since the transmittance η decays exponentially with the communication distance in the fiber-based network, this linear key-rate bound severely limits the key generation rate.

The following two approaches to overcome this rate limit have been considered: quantum repeaters [12–14] and trusted relays. Unfortunately, using quantum repeater schemes with current technology is infeasible because they require high-quality quantum memory and complicated local entanglement distillation operations. The trusted-relay approach, however, relies on the assumption that the quantum relays between two users are trustworthy, which is difficult to ensure or verify practically; this severely undermines the primary goal of QKD, i.e., security. In 2012, the measurement-device-independent quantum key distribution (MDI-QKD) scheme was proposed to close all the detection loopholes [15], which enhances the security of a practical QKD system. Nevertheless, the key rate of the

---

[*]xma@tsinghua.edu.cn

   Published by the American Physical Society

MDI-QKD scheme is still bounded by $O(\eta)$. Therefore, the linear key-rate bound [10,11] was widely believed to hold for practical QKD systems without relays.

Significant efforts have been devoted to improve the key rate by proposing different schemes. Recently, Lucamarini *et al.* proposed a novel phase-encoding QKD protocol, called twin-field quantum key distribution (TF-QKD) [16], which shows the possibility to overcome the key-rate limit and make a quadratic improvement over phase-encoding MDI-QKD [17]. In both schemes, single-photon detection is used, whereas coincident detection is required in other MDI-QKD schemes [15,18]. From a technical point of view, the single-photon detection is the key reason for the quadratic improvement. Unfortunately, a rigorous security proof is still missing at the moment. In fact, as shown later, the widely used photon number channel model [19] used in the security proof of MDI-QKD is proven to be invalid for this kind of setting.

Following the TF-QKD scheme [16], we investigate phase-encoding MDI-QKD schemes with single detection [17] and propose a phase-matching quantum key distribution (PM-QKD) scheme that can surpass the linear key-rate bound, inspired by the relative phase-encoding Bennett-1992 [20], phase-encoding MDI-QKD [17,18], and passive differential-phase-shift QKD [21]. The two communication parties prepare two coherent states independently, encode the key information onto the common phase, and match phases via interference detection at an untrusted measurement site. Details are given in Sec. II. By developing an optical-mode-based security proof, we show that the key rate of the proposed scheme scales with the square root of the transmittance, $R = O(\sqrt{\eta})$, in Sec. III, with technical details given in Appendix A. Also, the proposed phase-matching scheme falls into the MDI framework, which is immune to all possible detection attacks. Our security proof can be directly applied to TF-QKD. In Sec. IV, we deal with related practical issues and develop a phase postcompensation technique to ease the experimental requirements. In Sec. V, we simulate the key-rate performance of PM-QKD and compare it to former QKD protocols, with all the practical factors taken into account. Finally, in Sec. VI, we discuss possible future work directions.

II. PM-QKD PROTOCOL

In PM-QKD, the two communication parties, Alice and Bob, generate coherent state pulses independently. For a d-phase PM-QKD protocol, Alice and Bob encode their key information κ_a, $\kappa_b \in \{0, 1, ..., d-1\}$, into the phases of the coherent states, respectively, and send them to an untrusted measurement site that could be controlled by Eve, as shown in Fig. 1(a). Eve is expected to perform interference detection. Define a successful detection as the case where one and only one of the two detectors clicks, denoted by L click and R click. This interference
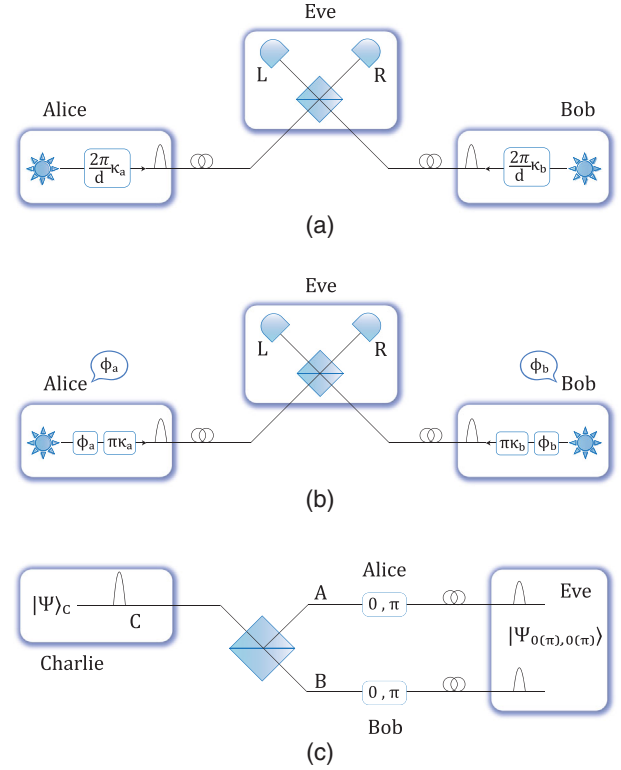

FIG. 1. (a) Schematic diagram of PM-QKD. Alice generates a coherent state, $|\sqrt{\mu_a}e^{2\pi i\kappa_a/d}\rangle$, where $\kappa_a \in \{0, 1, ..., d-1\}$. Similarly, Bob generates $|\sqrt{\mu_b}e^{2\pi i\kappa_b/d}\rangle$. The two coherent states are sent and interfered at an untrusted measurement site. (b) Schematic diagram of PM-QKD with $d = 2$ plus phase randomization. Alice prepares $|\sqrt{\mu_a}e^{i(\phi_a+\pi\kappa_a)}\rangle$ and Bob prepares $|\sqrt{\mu_b}e^{i(\phi_b+\pi\kappa_b)}\rangle$. The two coherent states interfere at an untrusted measurement site. If the phase difference $|(\phi_a + \pi\kappa_a) - (\phi_b + \pi\kappa_b)|$ is 0, detector L clicks; if the phase difference is π, detector R clicks. After Eve announces her measurement result, Alice and Bob publicly announce ϕ_a and ϕ_b. (c) Equivalent scenario for the postselected signals with $\phi_a = \phi_b$. A trusted party (Charlie) prepares $|\Psi\rangle_C$, splits it, and sends it to both Alice and Bob. Without loss of generality, we consider the case where Alice and Bob both modulate this by the same phase 0 or π to create the systems A and B. If $|\Psi\rangle_C$ only contains odd- or even-photon number components, we can see that $|\Psi_0\rangle = |\Psi_\pi\rangle$.

measurement would match the phases of Alice and Bob's signals. Conditioned on Eve's announcement, Alice and Bob's key information is correlated.

In this work, we mainly focus on PM-QKD with $d = 2$ and phase randomization. That is, Alice and Bob add extra random phases on their coherent state pulses before sending these pulses to Eve. After Eve's announcement, Alice and Bob announce the extra random phases and postselect the signals based on the random phases. This PM-QKD scheme is detailed below and shown in Fig. 1(b). For simplicity, by using the name "PM-QKD" in the text below, we refer to the case of $d = 2$ plus phase randomization.

State preparation.—Alice randomly generates a key bit κ_a and a random phase $\phi_a \in [0, 2\pi)$ and then prepares the coherent state $|\sqrt{\mu_a}e^{i(\phi_a + \pi\kappa_a)}\rangle_A$. Similarly, Bob generates κ_b and $\phi_b \in [0, 2\pi)$ and then prepares $|\sqrt{\mu_b}e^{i(\phi_b + \pi\kappa_b)}\rangle_B$.

Measurement.—Alice and Bob send their optical pulses, A and B, to an untrusted party, Eve, who is expected to perform an interference measurement and record the detector (L or R) that clicks.

Announcement.—Eve announces her detection results. Then, Alice and Bob announce the random phases ϕ_a and ϕ_b, respectively.

Sifting.—Alice and Bob repeat the above steps many times. When Eve announces a successful detection (a click from exactly one of the detectors L or R), Alice and Bob keep κ_a and κ_b as their raw key bits. Bob flips his key bit κ_b if Eve's announcement was an R click. Then, Alice and Bob keep their raw key bit only if $|\phi_a - \phi_b| = 0$ or π. Bob flips his key bit κ_b if $|\phi_a - \phi_b| = \pi$.

Parameter estimation.—For all the raw data that they have retained, Alice and Bob analyze the gains Q_μ and quantum bit error rates E_μ^Z. They then estimate E_μ^X using Eq. (2).

Key distillation.—Alice and Bob perform error correction and privacy amplification on the sifted key bits to generate a private key.

Notations.—Denote a coherent state in mode A to be $|\sqrt{\mu}e^{i\phi}\rangle_A$, where μ is the intensity and ϕ is the phase; $\mu_a = \mu_b = \mu/2$; Alice's (Bob's) key bit $\kappa_{a(b)} \in \{0, 1\}$; total gain Q_μ; phase error rate E_μ^X; and bit error rate E_μ^Z.

The above implementation of the PM-QKD protocol clearly resembles the phase-encoding MDI-QKD protocol [17,18], where the key bits are encoded in the relative phase of two coherent pulses (the reference and signal pulses). However, in the PM-QKD protocol, the reference pulse can be regarded as being shared by Alice and Bob. Therefore, they no longer need to send the reference pulse, and the key becomes the global phase of the coherent signal pulses. Another significant difference between PM-QKD and the former phase-encoding MDI-QKD scheme is that no basis switching is required. In this respect, it resembles the Bennett-1992 [20] and passive DPS [21] QKD protocols. Note that, a similar protocol has been proposed named "MDI-B92" protocol [22]. With the decoy-state method, the quantum part of PM-QKD would be similar to that of the TF-QKD protocol without basis sifting.

III. SECURITY OF PM-QKD

To provide an intuitive understanding of the manner in which PM-QKD works, we demonstrate its security by considering an equivalent scenario shown in Fig. 1(c). Here, a trusted party (Charlie) prepares a pure state $|\Psi\rangle_C$, splits it using a 50–50 beam splitter, and sends it to Alice

and Bob separately. Alice and Bob encode their key information κ_a and κ_b into systems A and B by modulating the phases, and then they send these to Eve, who is supposed to tell whether $|\kappa_a - \kappa_b| = 0$ or 1. Thus, the four possible output states that could be sent to Eve can be expressed as $|\Psi_{0,0}\rangle$, $|\Psi_{0,\pi}\rangle$, $|\Psi_{\pi,0}\rangle$, and $|\Psi_{\pi,\pi}\rangle$.

Without the loss of generality, we consider the following case in which both encoded key bits are the same, $\kappa_a = \kappa_b$. Eve attempts to learn the key bit $\kappa_{a(b)}$ from the state sent to her, which is either $|\Psi_{0,0}\rangle$ or $|\Psi_{\pi,\pi}\rangle$. Here, the phase, controlled by κ_a and κ_b and modulated into A and B, has become the "global phase" of the combined system A and B. If $|\Psi\rangle_C$ is a Fock state $|k\rangle_C$ with k photons, then $|\Psi_{0,0}\rangle = |\Psi_{\pi,\pi}\rangle$, since the global phases of Fock states are meaningless. In this case, Eve cannot tell in principle whether the modulated phases are 0 or π and can only learn that $\kappa_a = \kappa_b$.

In our PM-QKD protocol, both Alice and Bob transmit weak coherent pulses, $|\sqrt{\mu_a}e^{i(\phi_a + \pi\kappa_a)}\rangle_A$ and $|\sqrt{\mu_b}e^{i(\phi_b + \pi\kappa_b)}\rangle_B$ to Eve. The phase postselection condition $\phi_a = \phi_b = \phi$ is equivalent to imagining that Charlie employs a source state of $|\Psi\rangle_C = |\sqrt{\mu}e^{i\phi}\rangle_C$ in Fig. 1(b). For a phase-randomized state $|\sqrt{\mu}e^{i\phi}\rangle_C$, it is equivalent for Charlie to prepare a Fock state $|\Psi\rangle_C = |k\rangle_C$ with a probability of $P(k) = e^{-\mu}\mu^k/k!$. Thus, the PM-QKD protocol is secure if Eve cannot learn the phase ϕ. However, in the real PM-QKD protocol, the phase ϕ will eventually be announced during the sifting process. When this happens, Charlie's source $|\Psi\rangle_C$ can no longer be regarded as combinations of different photon-number states $|k\rangle_C$. The key challenge of the security proof of PM-QKD lies in the fact that the quantum source cannot be regarded as a mixture of photon number states, after Alice and Bob announce the phases, ϕ_a and ϕ_b. That is, the photon number channel model [19] and the "tagging" method used in the security proof by Gottsman *et al.* (GLLP security proof) [23] can no longer be applied here. In Appendix C, a beam-splitting attack is proposed to show that the GLLP formula is incorrect after the phase announcement. Therefore, one cannot simply reduce a randomized-phase coherent state protocol to a single-photon-based protocol.

Our security proof of PM-QKD is based on analyzing the distillable entanglement of its equivalent entanglement-based protocol. Following the Shor-Preskill security argument [5], the key rate of PM-QKD protocol (for the sifted signals) is given by

$$r_{\text{PM}} \geq 1 - H(E_\mu^Z) - H(E_\mu^X), \qquad (1)$$

where E_μ^Z is the quantum bit error rate (QBER) that can be directly estimated in the experiment; E_μ^X is the phase error rate, which reflects the information leakage; and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. We demonstrate in Appendix A that E_μ^X can be bounded by

$$E_\mu^X \le e_0^Z q_0 + \sum_{k=0}^{\infty} e_{2k+1}^Z q_{2k+1} + \left(1 - q_0 - \sum_{k=0}^{\infty} q_{2k+1}\right). \quad (2)$$

Here, q_k is the estimated ratio of the "k-photon signal" to the full detected signal:

$$q_k = \frac{(e^{-\mu}\mu^k/k!)Y_k}{Q_\mu}, \quad (3)$$

where Q_μ is the total gain of the pulses, and Y_k and e_k^Z are the yield and bit error rate, respectively, if Charlie's light source is a k-photon number state. Alice and Bob can estimate the yield and bit error rate via the decoy-state method [24–26]. Note that the parameters Y_k and e_k^Z can still be used to characterize Eve's behavior even though the source is not actually a combination of photon-number states.

Unlike most of the existing security analysis of discrete-variable QKD, our analysis is not single-qubit based. For a long time, the sources in QKD implementations, such as weak coherent sources and spontaneous parametric down-conversion sources, have been fabricated as an approximation of single qubit, following the BB84 protocol [1]. Here, we show the security of PM-QKD with a coherent light source by directly applying the Lo-Chau entanglement distillation argument [4] on analyzing the optical modes. This technique could be helpful for both a new QKD scheme design and security analysis.

In the equivalent scenario considered above, shown in Fig. 1(b), a trusted party Charlie is introduced. We need to emphasize that the virtual Charlie will be removed in the real implementation in Sec. IV. If Charlie does exist, Eve may inject some probes after Charlie's outputs, and then she measures them at the output of Alice and Bob to learn their operations. This is the main problem of detection-device-independent QKD [27,28]. In the PM-QKD protocol shown in Fig. 1(a), Alice and Bob can simply isolate their light source and modulators in an optical circulator to prevent such Trojan-horse-like attacks. Hence, the PM-QKD scheme, like other MDI-QKD schemes, is secure against Trojan-horse-like attacks.

IV. PRACTICAL IMPLEMENTATION

Now we address a few practical issues. In the protocol shown in Fig. 1, Alice and Bob only retain their signals when their announced phases ϕ_a and ϕ_b are either exactly the same or with a π difference. However, since the announced phases are continuous, the successful sifting probability tends to zero. Moreover, we assume that Alice's and Bob's laser sources are perfectly locked, such that their phase references meet, but it is very challenging in practice to achieve such phase locking.

To address these practical issues, we employ a phase postcompensation method [18], where Alice and Bob first
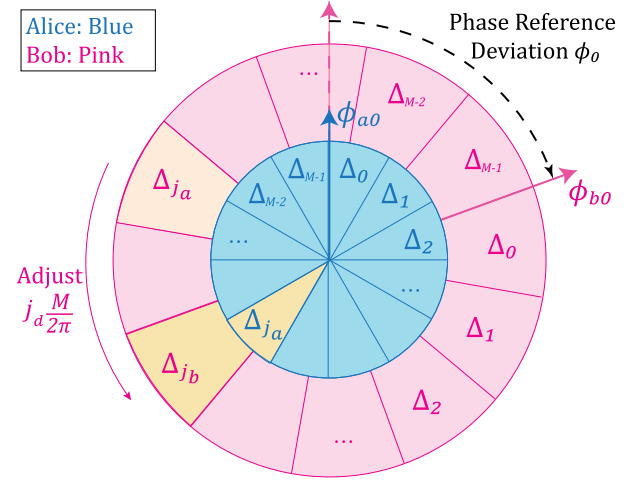

FIG. 2. Phase postcompensation. Without loss of generality, here we consider the case $\kappa_a = \kappa_b$. Denote the phase references of Alice and Bob as ϕ_{a0} and ϕ_{b0}, and, hence, the reference deviation is $\phi_0 = \phi_{b0} - \phi_{a0}$ mod 2π. Bob can figure out the proper phase compensation offset j_d by minimizing the QBER from random sampling as follows. Bob sets up a j_d, sifts the bits by $|j_b + j_d - j_a| = 0$, and evaluates the sample QBER. He tries all possible $j_d \in \{0, 1, ..., M-1\}$ and figures out the proper j_d to minimize the sample QBER. Then, he announces the sifted locations of unsampled bits to Alice. As shown in the figure, we set $M = 12$, and the reference deviation $\phi_0 = 70°$; hence, Bob can set $j_d = 2$ to compensate the effect of ϕ_0.

divide the phase interval $[0, 2\pi)$ into M slices $\{\Delta_j\}$ for $0 \le j \le M - 1$, where $\Delta_j = [2\pi j/M, 2\pi(j+1)/M)$. Instead of comparing the exact phases, Alice and Bob only compare the slice indexes. This makes the phase-sifting step practical, but introduces an intrinsic misalignment error. Also, Alice and Bob do not perform the phase sifting immediately in each round, and instead, they do it in data postprocessing. In the parameter estimation step, they perform the following procedures, as shown in Fig. 2.

(1) For each bit, Alice announces the phase slice index j_a and randomly samples a certain amount of key bits and announces them for QBER testing.

(2) In the phase postcompensation method, given an offset compensation $j_d \in \{0, 1, ..., M/2 - 1\}$, Bob sifts the sampled bits with the phase postselection condition $|j_b + j_d - j_a|$ mod $M = 0$ or $M/2$. For the case of $M/2$, Bob flips the key bit κ_b. After sifting, Bob calculates the QBER E^Z with Alice's sampling key bits. Bob tries all possible $j_d \in \{0, 1, ..., M-1\}$ and figures out the proper j_d to minimize the sampling QBER. Using the phase postselection condition with the proper j_d, Bob sifts (and flips if needed) the unsampled bits and announces the locations to Alice. Alice sifts her key bits accordingly.

(3) Alice and Bob analyze the overall gain Q_{μ_i} and QBER $E_{\mu_i}^Z$ for different values of intensities $\mu_a = \mu_b = \mu_i/2$. They estimate the phase error rate $E_\mu^{(X)}$ by Eq. (2).

Here, in the phase postcompensation step, Bob does not need to fix a j_d for the whole experiment. Bob can group the raw data into data blocks, and then he is able to adjust the offset j_d for different data blocks. Alternatively, Bob can also adjust j_d in real time based on a prediction via data-fitting samples nearby. A detailed description of the operations and security arguments is presented in Appendix A 6. We emphasize that the fluctuation of phases will only introduce additional bit errors, but not affect the security.

An alternative method to phase postcompensation is that Alice and Bob can generate strong pulses independent of quantum signals for phase calibration. The two pulses are interfered at the measurement site so that Alice and Bob can identify the phase fluctuations between two channels. Note that the strong pulses can be set in an optical mode slightly deviated from the quantum signals to reduce cross-talks. According to the phase difference measured from the strong calibration pulses, Alice and Bob can estimate the offset j_d accurately. This is a feasible way to replace the phase postcompensation method. The main difference of this phase calibration method from the usual phase-locking method [29] is that no active feedback is required. Alice and Bob learn the phase difference only for phase sifting in data postprocessing.

Note that similar ideas of phase postcompensation and phase calibration have already been adopted in some continuous-variable QKD protocols, such as the Gaussian-modulated coherent-state protocol [30,31] and the self-referenced protocol [32].

Another important issue is how Alice and Bob set random phases ϕ_a, ϕ_b. In practice, it would be experimentally challenging to continuously set an accurate phase to a coherent state. As discussed above, they only need to set the slice indexes j_a, j_b instead of exactly modulating phases. There are two methods to achieve this.

(i) Alice and Bob first generate strong laser pulses with (unknown) randomized phases, either by turning on/off the lasers or active phase randomization. They then split the pulses and apply homodyne detection on one beam to measure the phase ϕ_a, ϕ_b accurately enough to determine the slice indexes j_a, j_b. They use the rest beam for further quantum encoding.

(ii) Alice and Bob first generate pulses with stable phases. Then, they actively randomize the phase using phase modulators. Alice and Bob can record the corresponding random numbers as for slice indexes j_a, j_b. Note that the phase randomization can be discrete, which has been proven to be secure and efficient with a few discrete phases [33].

In order to optimize the estimated phase slice shift j_d for minimizing the bit error rate, the phase compensation or calibration should be resettled with respect to phase drift. In practice, there are two major factors which may cause phase drift. One is the laser linewidth $\Delta\nu$, which causes a

dispersion effect on the output pulse. The phase varies randomly with respect to the coherent time $T_{\rm coh} \approx (\Delta\nu)^{-1}$. To alleviate the dispersion, a CW laser source with a long coherence time should be employed. The other major factor for phase drift is the variation of optical path length ΔL. In a recent work of TF-QKD [16], Lucamarini *et al.* experimentally tested the phase drift in a MDI setting. The results show that the phase drift follows a Gaussian distribution with zero mean and a standard deviation of about $6.0 \, \rm rad\,ms^{-1}$ for a total distance of 550 km. To enhance the performance of PM-QKD protocol, former works on phase stabilization of optical fibers [34–36] can be employed.

With all the practical factors taken into account, the final key-rate formula can be expressed as

$$R_{\rm PM} \geq \frac{2}{M} Q_\mu [-fH(E_\mu) + 1 - H(E_\mu^X)], \qquad (4)$$

where the phase error rate E_μ^X is given by Eq. (2), $2/M$ is the sifting factor, and f is the error correction efficiency.

V. SIMULATION RESULTS

We simulate the performance of PM-QKD with the parameters given in Table I, assuming a lossy channel that is symmetrical for Alice and Bob. The dark count rate p_d is from Ref. [37], and the other parameters are set to be typical values. The simulation formulas for Q_μ, E_μ^Z, and E_μ^X of PM-QKD are given in Eqs. (B14), (B22), and (B27), respectively, in Appendix B 2. The simulation formulas for BB84 and MDI-QKD are listed in Appendix B 3.

The simulation results are shown in Fig. 3(a). From the figure, one can see that PM-QKD is able to exceed the linear key-rate bound when $l > 250$ km with practical settings such as dark counts, misalignment errors, and sifting factors. Compared with MDI-QKD, PM-QKD can achieve a longer transmission distance of $l = 450$ km, and the key rate is increased by approximately 4–6 orders of magnitude when $l > 300$ km. Moreover, if we set up a cutoff line of key rate $R = 10^{-8}$ as real-life consideration, then the longest practical transmission distance of PM-QKD is over 400 km, whereas the ones of BB84 and MDI-QKD are all lower than 250 km.

Several QKD schemes are compared in Table II. The comparison shows that the PM-QKD scheme outperforms

TABLE I.   Parameters used for simulation.

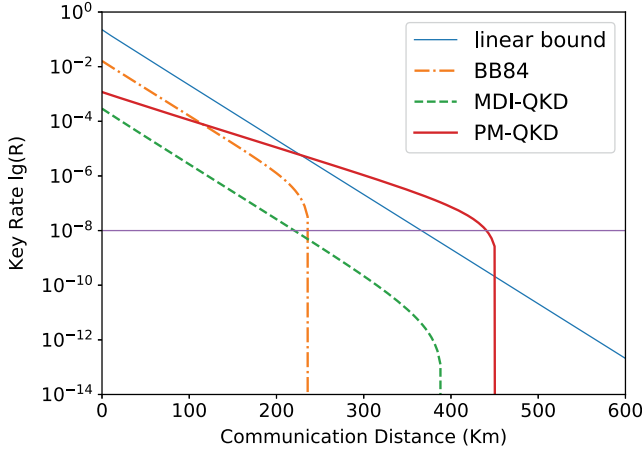| Parameters	Values
Dark count rate p_d	8×10^{-8}
Error correction efficiency f	1.15
Detector efficiency η_d	14.5%
Number of phase slices M	16
Misalignment error e_d	1.5%

FIG. 3. Simulation of our PM-QKD protocol. For the considered simulation parameters, the key rate of PM-QKD surpasses that of the conventional BB84 protocol when $l > 120$ km, and it exceeds the linear key-rate bound by Pirandola et al. (PLOB bound) [11] when $l > 250$ km. In addition, our protocol is also able to achieve a long transmission distance of $l = 450$ km.

the existing protocols in the following aspects. First, the PM-QKD scheme has a quadratic improvement of key rate, $O(\sqrt{\eta})$. In the security aspect, PM-QKD enjoys the measurement-device-independent nature that is immune to all detection attacks. In the practical aspect, it removes the requirement of the basis switch, which can simplify the experiment apparatus and reduce the randomness consumption.

Here, we would like to clarify that the linear key-rate bound [11] is derived for point-to-point QKD protocols. In the PM-QKD or other MDI-QKD schemes, there is an untrusted relay held by Eve. The quadratic improvement in PM-QKD seems unsurprising if we regard the untrusted middle node as a quantum repeater.

TABLE II. Comparison of different QKD protocols: PM-QKD; TF-QKD [16]; MDI-QKD [15]; passive differential phase-shift (DPS) QKD [21]; Bennett-1992 (B92) QKD [20]. Key rate: dependence of the key rate on the channel transmittance η; Detection loophole: whether the protocol is immune to all detection loopholes; Qubit based: whether the security analysis is based on the single-qubit case; Basis switch: whether the source (measurement device) must prepare (measure) states in complementary bases; Phase locking: whether the protocol requires a fixed phase reference frame for the two users.

Protocol	PM	TF	MDI	Passive DPS	B92
Key rate	$O(\sqrt{n})$	$O(\sqrt{n})$[a]	$O(\eta)$	$O(\eta)$	$O(\eta^2)$
Detection loophole	No	No[a]	No	Yes	Yes
Qubit based	No	Yes	Yes	Yes	Yes
Basis switch	No	Yes	Yes	No	No
Phase locking	No	Yes	No	Yes	No

[a]Our security proof and performance analysis apply to TF-QKD if the basis information X, Y is ignored.

Note that the security of recently proposed TF-QKD protocol [16] can be reduced to the security of PM-QKD protocol if the information for the two bases X, Y is ignored in TF-QKD. It remains an open problem whether we can reach a higher key rate by taking advantage of the basis information together.

VI. OUTLOOK

There are a few interesting directions on PM-QKD. First, it is interesting to work out the security of the general d-phase PM-QKD protocol shown in Fig. 1(a) with and without phase randomization. Meanwhile, in the above discussions, PM-QKD in Fig. 1(b) is treated as a single-basis scheme with phase randomization. In a dual viewpoint, we can regard the different global phases ϕ_a, ϕ_b as different bases and naturally treat the phase-sifting step as basis sifting. This is interesting, since it shows the advantage of QKD using multi-nonorthogonal bases. Moreover, this multibases view may help us to generalize the phase-matching scheme to, for example, a polarization-based one.

Second, the phase-sifting factor $2/M$ is very small, which undermines the advantage of PM-QKD for near-distance (i.e., $l < 120$ km) communication. One possible solution is to apply a biased phase randomization; i.e., the $\phi_{a(b)}$ is not uniformly randomized in $[0, 2\pi)$.

Third, we bound the total phase error E_μ^X by pessimistically considering the phase errors e_k^X for even photon number components to be 1 in Eq. (A33), as shown in Appendix A 5. There may be a scope to improve the bound of total phase error E_μ^X. For example, the two-photon error e_2^Z and e_2^X can be better estimated with more decoy states, which leads to a tighter bounds of E_μ^X.

Finally, since we can overcome the key-rate linear bound, it is interesting to investigate a repeaterless secret key capacity bound for QKD, for example, whether it is possible to push the key rate to $R = O(\eta^{1/3})$ or $O(\eta^{1/4})$ without repeaters. Note that the key-rate bound has been derived for the single-repeater case [38], $-\log(1 - \sqrt{\eta})$, which is close to $\sqrt{\eta}$ when η is small. So far, our key rate, Eq. (4), is still far away from this bound. It is an interesting direction to improve the PM-QKD protocol to approach this bound.

APPENDIX A: SECURITY PROOF OF PM-QKD

In this section, we provide a security proof for the PM-QKD protocol with $d = 2$ via entanglement distillation [39]. Note that the existing security proofs of discrete-variable QKD assume qubit (or qudit) states transmitted through the channel. Here, we develop a new security proof by exploring continuous optical modes directly.

The organization of the proof is presented as follows. First, we briefly review the main results of the Lo-Chau [4] and Shor-Preskill [5] security proofs in Appendix A 1. Then, we provide a virtual entanglement-based protocol (Protocol I) in Appendix A 2 and present a key result as Lemma 1. In Appendix A 3, we employ a few equivalency arguments, and eventually, we prove the security of PM-QKD in Appendix A 4. In Appendix A 5, we employ the decoy-state method to give tight bounds on phase error rates. In Appendix A 6, we solve the phase-reference issue with the phase postcompensation technique.

Here, we introduce some definitions and notations for later discussions. For an optical mode A, whose creation operator is $a^\dagger$, its Hilbert space is denoted as $\mathcal{H}^A$. Let $\mathcal{D}(\mathcal{H}^A)$ denote the space of density operators acting on $\mathcal{H}^A$ and $\mathcal{L}(\mathcal{H}^A)$ denote the space of linear operators acting on $\mathcal{H}^A$. A Fock state $|k\rangle_A$ with k photons in mode A is defined as

$$|k\rangle_A \equiv \frac{(a^\dagger)^k}{\sqrt{k!}} |0\rangle_A, \qquad (A1)$$

where $|0\rangle_A$ is the vacuum state. A coherent state $|\alpha\rangle_A$ is defined as

$$|\alpha\rangle_A \equiv e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle_A$$
$$= e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha a^\dagger)^k}{k!} |0\rangle_A$$
$$= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha a^\dagger} |0\rangle_A. \qquad (A2)$$

The photon number of $|\alpha\rangle_A$ follows a Poisson distribution,

$$P(k) = e^{-\mu} \frac{\mu^k}{k!}, \qquad (A3)$$

where $\mu = |\alpha|^2$ is the mean photon number or the light intensity.

Define the odd subspace $\mathcal{H}^A_{\text{odd}} \subseteq \mathcal{H}^A$, which is spanned by the odd Fock states $\{|k\rangle_A\}$, where all the photon numbers k are odd. Similarly, define the even subspace $\mathcal{H}^A_{\text{even}} \subseteq \mathcal{H}^A$, where the photon numbers are even. Name a state $\rho \in \mathcal{D}(\mathcal{H}^A_{\text{odd}})$ to be the odd state and a state $\rho \in \mathcal{D}(\mathcal{H}^A_{\text{even}})$ to be the even state. Name a state $\rho \in \mathcal{D}(\mathcal{H}^A_{\text{odd}})$ or $\rho \in \mathcal{D}(\mathcal{H}^A_{\text{even}})$ to be the parity state. Denote

$$|\alpha_{\text{odd}}\rangle_A \equiv \frac{1}{2\sqrt{c_{\text{odd}}}} (|\alpha\rangle_A - |-\alpha\rangle_A)$$
$$= \frac{1}{\sqrt{c_{\text{odd}}}} e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha)^{2k+1}}{\sqrt{(2k+1)!}} |2k+1\rangle_A,$$

$$|\alpha_{\text{even}}\rangle_A \equiv \frac{1}{2\sqrt{c_{\text{even}}}} (|\alpha\rangle_A + |-\alpha\rangle_A)$$
$$= \frac{1}{\sqrt{c_{\text{even}}}} e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha)^{2k}}{\sqrt{(2k)!}} |2k\rangle_A, \qquad (A4)$$

where

$$c_{\text{odd}} = e^{-\mu} \sum_{k=0}^{\infty} \frac{\mu^{2k+1}}{(2k+1)!} = e^{-\mu} \sinh \mu,$$

$$c_{\text{even}} = e^{-\mu} \sum_{k=0}^{\infty} \frac{\mu^{2k}}{(2k)!} = e^{-\mu} \cosh \mu \qquad (A5)$$

are the normalization factors with $c_{\text{odd}} + c_{\text{even}} = 1$, and $\mu = |\alpha|^2$ is the light intensity. It is not hard to see that $|\alpha_{\text{odd}}\rangle_A \in \mathcal{H}^A_{\text{odd}}$ and $|\alpha_{\text{even}}\rangle_A \in \mathcal{H}^A_{\text{even}}$.

Denote the photon number measurement $\{M_k\}_k$ as

$$M_k \equiv |k\rangle_A \langle k|. \qquad (A6)$$

Denote the parity measurement $\{M_{\text{odd}}, M_{\text{even}}\}$ as

$$M_{\text{odd}} \equiv \sum_{k=0}^{\infty} |2k+1\rangle_A \langle 2k+1|,$$

$$M_{\text{even}} \equiv \sum_{k=0}^{\infty} |2k\rangle_A \langle 2k|. \qquad (A7)$$

For a beam splitter (BS), we express the input optical modes as A, B, with creation operators $a^\dagger$, $b^\dagger$, respectively, and the output optical modes as C, D, with creation operators $c^\dagger$, $d^\dagger$, respectively. The BS transforms modes A and B to C and D according to

$$\begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix}. \qquad (A8)$$

For a qubit system A', the Hilbert space is denoted by $\mathcal{H}^{A'}$. The Pauli operators on $\mathcal{H}^{A'}$ are denoted as $X_{A'}$, $Y_{A'}$, and $Z_{A'}$. The eigenstates of $X_{A'}$, $Y_{A'}$, and $Z_{A'}$ are denoted by $\{|\pm\rangle_{A'}\}$; $\{|\pm i\rangle_{A'}\}$; and $\{|0\rangle_{A'}, |1\rangle_{A'}\}$, respectively. The X-basis measurement is denoted by $M_X : \{|+\rangle_{A'}\langle+|, |-\rangle_{A'}\langle-|\}$. The Z-basis measurement is denoted by $M_Z : \{|0\rangle_{A'}\langle0|, |1\rangle_{A'}\langle1|\}$.

A control-phase gate C_π, from a qubit A' to an optical mode A, is defined as

$$C_\pi \equiv |0\rangle_{A'}\langle0| \otimes U_A(0) + |1\rangle_{A'}\langle1| \otimes U_A(\pi), \qquad (A9)$$

where $U_A(\phi) \equiv e^{i\phi a^{\dagger} a}$ is a ϕ-phase shifter operation on the mode A.

Definition 1. Two QKD protocols are equivalent if the following criteria are satisfied:

(1) The quantum states transmitted in the channel are the same.

(2) All announced classical information is the same.

(3) Alice and Bob perform the same measurement on the same quantum states to obtain the raw key bits.

(4) Alice and Bob use the same postprocessing to extract secure key bits.

Obviously, equivalent QKD protocols will lead to identical key rates.

1. Security proof via entanglement distillation

Here, we briefly review the security proof based on entanglement distillation [4,5]. Suppose that, in QKD, Alice generates an l-bit key string S, and Bob generates an estimate of the key string S'. Denote the space of S as $\mathcal{S}$, whose dimension is 2^l. An adversary Eve attempts to learn about S from the information leakage.

After QKD, Alice and Bob should share the *same* key *privately*. A key S is called "correct," if $S' = S$ for any strategy of Eve, and is called "ϵ_{cor}-correct," if

$$Pr[S' \neq S] \leq \epsilon_{\text{cor}}. \quad (A10)$$

To define a private key, consider the quantum state ρ_{AE} that describes the correlation between Alice's classical key S and Eve's system E (for any attacks). A key S is called "ϵ_{sec} private" from E if [40,41]

$$\min_{\sigma_E} \frac{1}{2} \|\rho_{AE} - \omega_A \otimes \sigma_E\|_1 \leq \epsilon_{\text{sec}}, \quad (A11)$$

where $\omega_A = (|\mathcal{S}|)^{-1} \sum_{S=0}^{|\mathcal{S}|-1} |S\rangle_A \langle S|$ is the equally mixed key state over all possible keys in space $\mathcal{S}$ and $\| \cdot \|_1$ is the trace norm. A QKD protocol is called "secure" if the generated key is both correct and private. It is called "ϵ-secure" if the generated key is ϵ_{cor}-correct and ϵ_{sec} private with $\epsilon = \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$.

Here, we consider the case where Alice and Bob share an m-pair-of-qubits gigantic state $\rho_{A'B'}^{(m)}$. If we can show that

$$F(\rho_{A'B'}^{(m)}, |\Phi^+\rangle_{A'B'}^{(m)}) \geq \sqrt{1 - \epsilon_l^2}, \quad (A12)$$

where $|\Phi^+\rangle_{A'B'}^{(m)}$ is the state of m perfect EPR pairs $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, and $0 \leq \epsilon_l \leq 1$, then it can be shown that it is ϵ_l private and ϵ_l-correct, and then it is $2\epsilon_l$-secure. That is, to show the security of a QKD protocol, we only need to show that the state for key extraction $\rho_{A'B'}^{(m)}$ is close to the perfect Einstein-Podolsky-Rosen (EPR) pairs $|\Phi^+\rangle_{A'B'}^{(m)}$.

Here is the intuition of the Lo-Chau security proof [4]. Suppose Alice and Bob share an n-pair-of-qubit gigantic state $\rho_{A'B'}^{(n)}$ at the beginning. If they perform an efficient entanglement distillation protocol (EDP) to distill m EPR pairs, then they will be able to share nearly m bit correct and private keys. Now the task becomes how to find the right EDP.

Bennett, DiVincenzo, Smolin, and Wootters (BDSW) show that [39], if an n-pair-of-qubit state $\rho_{A'B'}^{(n)}$ can be written as a classical mixture of Bell state products,

$$\rho_{A'B'}^{(n)} = \sum_{b_1,b_2,\dots,b_n} p_{b_1,b_2,\dots,b_n} |b_1,b_2,\dots,b_n\rangle\langle b_1,b_2,\dots,b_n|,$$

$$|b_1,b_2,\dots b_n\rangle = \bigotimes_{i=1}^{n} |\Phi_{b_i}^{(i)}\rangle, \quad (A13)$$

where $|\Phi_{b_i}^{(i)}\rangle$ is one of the four Bell states labeled by $b_i \in \{0,1,2,3\}$ on the ith qubit, then one can distill entanglement by employing EDPs. In the one-way hashing method [39], a specific type of one-way EDP, Alice measures a series of commuting operators based on some random-hashing matrix on her n qubits, and she sends the results to Bob. Bob measures the same operators on his n qubits and infers the locations and types of the errors from the difference in the measurement results. After that, Alice and Bob correct the errors and obtain m ($m \leq n$, almost perfect) EPR pairs.

In general, of course, the initial state $\rho_{A'B'}^{(n)}$ can deviate from Bell-diagonal states and become highly entangled between different pairs. In the Lo-Chau security proof [4], it has been shown that, for the one-way hashing EDP introduced above, the error syndrome and EDP performance of such $\rho_{A'B'}^{(n)}$ is the same as that of the state after dephasing between pairs,

$$\rho_{A'B',\text{dep}}^{(n)} \equiv W\rho_{A'B'}^{(n)}W,$$

$$W = \sum_{b_1,b_2,\dots,b_n} |b_1,b_2,\dots,b_n\rangle\langle b_1,b_2,\dots,b_n|, \quad (A14)$$

where $|b_1,b_2,\dots,b_n\rangle$ is defined in Eq. (A13). Therefore, one can reduce the EDP for general $\rho_{A'B'}^{(n)}$ (i.e., the case with coherent attacks) to the case in Eq. (A13).

In the Shor-Preskill security proof [5], the one-way EDP protocol is reduced to a "prepare-and-measure" QKD protocol, by employing the CSS code [42]. Later, other techniques of decoupling X-error correction and Z-error correction are introduced for this reduction. For a one-way EDP protocol based on the CSS code, the distillation rate of EPR pairs, $r \equiv \lim_{n\to\infty} m/n$, is given by

$$r = 1 - H(E^Z) - H(E^X), \quad (A15)$$

where E^Z and E^X are the Z-error rate and X-error rate, respectively, and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is

the binary Shannon entropy function. The error rates can defined as measurement results on $\rho_{A'B'}^{(n)}$,

$$E^Z \equiv \mathrm{Tr}\left[\bigoplus_{j=1}^{n} \frac{1}{2}(1 - Z_{A'}^{(j)} \otimes Z_{B'}^{(j)})\rho_{A'B'}^{(n)}\right],$$

$$E^X \equiv \mathrm{Tr}\left[\bigoplus_{j=1}^{n} \frac{1}{2}(1 - X_{A'}^{(j)} \otimes X_{B'}^{(j)})\rho_{A'B'}^{(n)}\right], \qquad \text{(A16)}$$

where $X_{A'(B')}^{(j)}$ is the Pauli X operator and $Z_{A'(B')}^{(j)}$ is the Pauli Z operator, on the jth pair-of-qubits system $A'(B')$. Since the bit value is measured in the Z-basis and the phase value is measured in the X-basis, we also call the Z-basis error the "bit error" and the X-basis error the "phase error."

Following the Shor-Preskill security proof, distillable entanglement of the one-way EDP protocol is the key rate for some prepare-and-measure QKD protocols such as BB84 [1]. In the BB84 protocol, we can estimate E^Z, E^X by randomly measuring the qubits in the X- and Z-basis. In the PM-QKD protocol, on the other hand, Alice and Bob can only measure in the Z-basis. In the following sections, we will introduce entanglement-based PM-QKD protocols and discuss how to infer the value of E^X.

2. Entanglement-based PM-QKD protocol

We first introduce an entanglement-based PM-QKD protocol, called Protocol I, as shown in Fig. 4.

Protocol I

(1) State preparation: A trusted party, Charlie, picks a state ρ on optical mode C; splits ρ into two pulses A and B; and sends them to Alice and Bob, respectively. Alice and Bob initialize their qubits in $|+i\rangle$. Alice applies the control gate C_π, defined in Eq. (A9), to qubit A' and optical pulse A. Similarly, Bob applies C_π to B' and B.

(2) Measurement: The two optical pulses A and B are sent to an untrusted party, Eve, who is supposed to perform interference measurement and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection result, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the qubits of systems A' and B'. In addition, Bob applies a Pauli Y-gate to his qubit if Eve's announcement is R click.

(5) Parameter estimation: After many rounds of the above steps, Alice and Bob end up with a joint $2n$-qubit state, denoted by $\rho_{A'B'}^{(n)}$. They then perform random sampling on the remaining $\rho_{A'B'}^{(n)}$ to estimate E^Z and infer E^X by Eq. (A24).

(6) Key distillation: Alice and Bob apply a standard EDP when the error rates are below a certain threshold. The distillation ratio r is given by Eq. (A15). Once Alice and Bob obtain nr (almost) pure EPR pairs, they both perform local Z measurements on the qubits to generate private keys.

Our first observation is that, if the state ρ prepared by Charlie is a parity state, namely, $\rho \in \mathcal{D}(\mathcal{H}_{\mathrm{odd}}^C)$ or $\rho \in \mathcal{D}(\mathcal{H}_{\mathrm{even}}^C)$, then the X-error rate and Z-error rate are correlated. Here, we denote the Z-error rate and X-error rate for an odd state ρ_{odd} as e_{odd}^Z and e_{odd}^X, respectively, and similarly, we denote them for an even state ρ_{even} as e_{even}^Z and e_{even}^X.

Lemma 1. In Protocol I, for $\rho \in \mathcal{D}(\mathcal{H}_{\mathrm{odd}}^C)$, $e_{\mathrm{odd}}^X = e_{\mathrm{odd}}^Z$, and for $\rho \in \mathcal{D}(\mathcal{H}_{\mathrm{even}}^C)$, $e_{\mathrm{even}}^X = 1 - e_{\mathrm{even}}^Z$.

Proof.—First consider the case when ρ is a Fock state $|k\rangle_C$, defined in Eq. (A1). After passing through the BS, as shown in Fig. 4, the state on modes A and B becomes

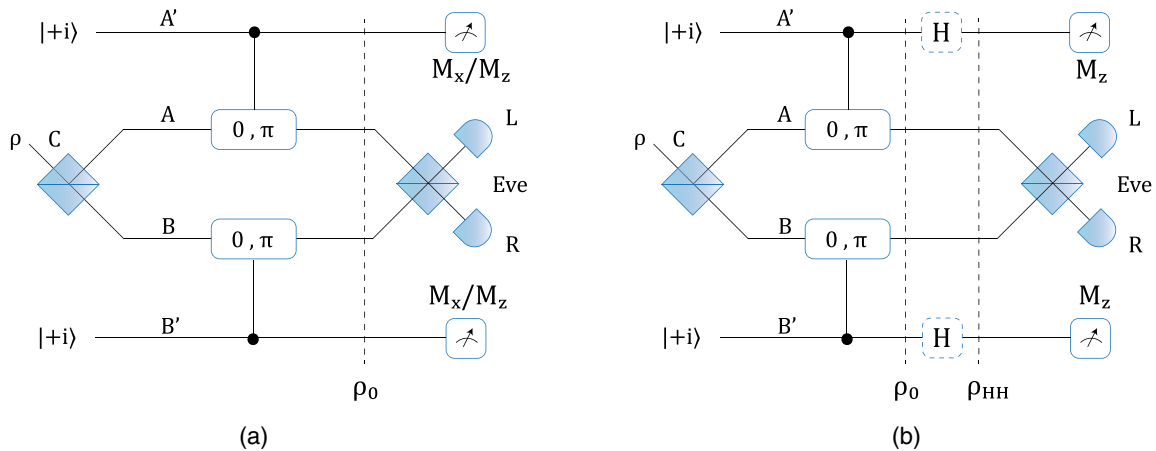$$\frac{1}{\sqrt{2^k k!}}(a^\dagger + b^\dagger)^k |00\rangle_{AB}. \qquad \text{(A17)}$$

FIG. 4.   (a) Schematic diagram of Protocol I. (b) Equivalent view of Protocol I, where the X-basis measurement on A' or B' is realized by a Hadamard gate followed by the Z-basis measurement.

The joint state on system A', B', A, B before the C_π operations is

$$\frac{1}{\sqrt{2^k k!}}|+i+i\rangle_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB} = \frac{1}{\sqrt{2^k k!}}\frac{1}{2}[(|00\rangle - |11\rangle) + i(|01\rangle + |10\rangle)]_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB}. \quad \text{(A18)}$$

After the C_π operations, this state becomes

$$|\Psi_0^{(k)}\rangle = \begin{cases} \frac{1}{2\sqrt{2^k k!}}[(|00\rangle + |11\rangle)_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB} + i(|01\rangle - |10\rangle)_{A'B'}(a^\dagger - b^\dagger)^k|00\rangle_{AB}], & \text{if } k \text{ is odd,} \\ \frac{1}{2\sqrt{2^k k!}}[(|00\rangle - |11\rangle)_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB} + i(|01\rangle + |10\rangle)_{A'B'}(a^\dagger - b^\dagger)^k|00\rangle_{AB}], & \text{if } k \text{ is even.} \end{cases} \quad \text{(A19)}$$

As shown in Fig. 4(b), the X-basis measurement on A' or B' is realized by a Hadamard gate followed by the Z-basis measurement. Denote the state after local Hadamard gates as $|\Psi_{HH}^{(k)}\rangle \equiv (H^{A'} \otimes H^{B'})|\Psi_0^{(k)}\rangle$; then,

$$|\Psi_{HH}^{(k)}\rangle = \begin{cases} \frac{1}{2\sqrt{2^k k!}}[(|00\rangle + |11\rangle)_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB} + i(|01\rangle - |10\rangle)_{A'B'}(a^\dagger - b^\dagger)^k|00\rangle_{AB}], & \text{if } k \text{ is odd,} \\ \frac{1}{2\sqrt{2^k k!}}[(|01\rangle + |10\rangle)_{A'B'}(a^\dagger + b^\dagger)^k|00\rangle_{AB} + i(|00\rangle - |11\rangle)_{A'B'}(a^\dagger - b^\dagger)^k|00\rangle_{AB}], & \text{if } k \text{ is even.} \end{cases} \quad \text{(A20)}$$

In other words, the X-error rate e_k^X can be understood as the error rate by performing the Z-basis measurement on the state of $|\Psi_{HH}^{(k)}\rangle$. The relation between the X- and Z-error rates can be obtained by comparing Eqs. (A19) and (A20). For the odd-photon-number case, since $|\Psi_{HH}^{(2k+1)}\rangle = |\Psi_0^{(2k+1)}\rangle$, we have $e_{2k+1}^X = e_{2k+1}^Z$. For the even-photon-number case, since $|\Psi_{HH}^{(2k)}\rangle = I^{A'} \otimes Y^{B'}|\Psi_0^{(2k)}\rangle$, we have $e_{2k}^X = 1 - e_{2k}^Z$.

Now, let us consider the case of pure parity states. For an odd state $|\psi_{\text{odd}}\rangle_C = \sum c_{2k+1}|2k+1\rangle_C$, where $\sum_k |c_{2k+1}|^2 = 1$, since the BS and C_π are unitary operations, the state after these operations can be written as

$$|\Psi_0^{(\text{odd})}\rangle = \sum_k c_{2k+1}|\Psi_0^{(2k+1)}\rangle. \quad \text{(A21)}$$

After local Hadamard gates, the state becomes $|\Psi_{HH}^{(\text{odd})}\rangle \equiv (H^{A'} \otimes H^{B'})|\Psi_0^{(\text{odd})}\rangle$. From Eqs. (A19)–(A21), we can see that $|\Psi_{HH}^{(\text{odd})}\rangle = |\Psi_0^{(\text{odd})}\rangle$, and hence $e_{\text{odd}}^Z = e_{\text{odd}}^X$. With the same argument, we have $e_{\text{even}}^Z = 1 - e_{\text{even}}^X$.

For general parity states, we can regard them as mixtures of pure parity states,

$$\rho_{\text{odd}} = \sum_i p_i |\psi_{\text{odd}}^{(i)}\rangle\langle\psi_{\text{odd}}^{(i)}|,$$

$$\rho_{\text{even}} = \sum_i p_i |\psi_{\text{even}}^{(i)}\rangle\langle\psi_{\text{even}}^{(i)}|. \quad \text{(A22)}$$

This is equivalent to Charlie sending out $|\psi_{\text{odd(even)}}^{(i)}\rangle$ with probability p_i. For each pure state component, we have $e_{\text{odd}(i)}^X = e_{\text{odd}(i)}^Z$ and $e_{\text{even}(i)}^X = 1 - e_{\text{even}(i)}^Z$. Thus, the relations hold for all (mixed) parity states.   □

In general, Charlie might not use a parity state. Consider the case that Charlie performs the parity measurement $\{M_{\text{odd}}, M_{\text{even}}\}$, defined in Eq. (A7), before sending to Alice and Bob. Denote the measurement outcome probabilities for the odd and even parity to be p_{odd} and p_{even}, respectively. This is equivalent to Charlie preparing an odd state ρ_{odd} and an even state ρ_{even} with probabilities p_{odd} and p_{even}, respectively. Then, the state can be written as

$$\rho = p_{\text{odd}}\rho_{\text{odd}} + p_{\text{even}}\rho_{\text{even}}, \quad \text{(A23)}$$

that is, $\rho \in \mathcal{D}(\mathcal{H}_{\text{odd}}^C \oplus \mathcal{H}_{\text{even}}^C)$.

Suppose Charlie announces the parity information publicly to Alice and Bob. Then, they can label the sifted qubits with "odd" and "even." Denote q_{odd} and q_{even}, with $q_{\text{odd}} + q_{\text{even}} = 1$, to be the fractions of odd- and even-labeled states in the sifted n-pairs of qubit states A', B', respectively. Then, according to Lemma 1, the total X-error rate can be calculated by

$$E^X = q_{\text{odd}}e_{\text{odd}}^X + q_{\text{even}}e_{\text{even}}^X$$
$$= q_{\text{odd}}e_{\text{odd}}^Z + q_{\text{even}}(1 - e_{\text{even}}^Z). \quad \text{(A24)}$$

Here, the parameters q_{odd}, q_{even}, e_{odd}^Z, and e_{even}^Z can be evaluated according to Charlie's parity announcement. When the parity information is missing, Alice and Bob need to estimate these parameters, which will be described later in Appendix A 5.

3. Coherent state protocol and equivalent process

From Protocol I to the PM-QKD protocol, there are a few practical issues that need to be addressed. First, the trusted party Charlie and the BS should be removed. In order to do this, we consider a special case where Charlie prepares a
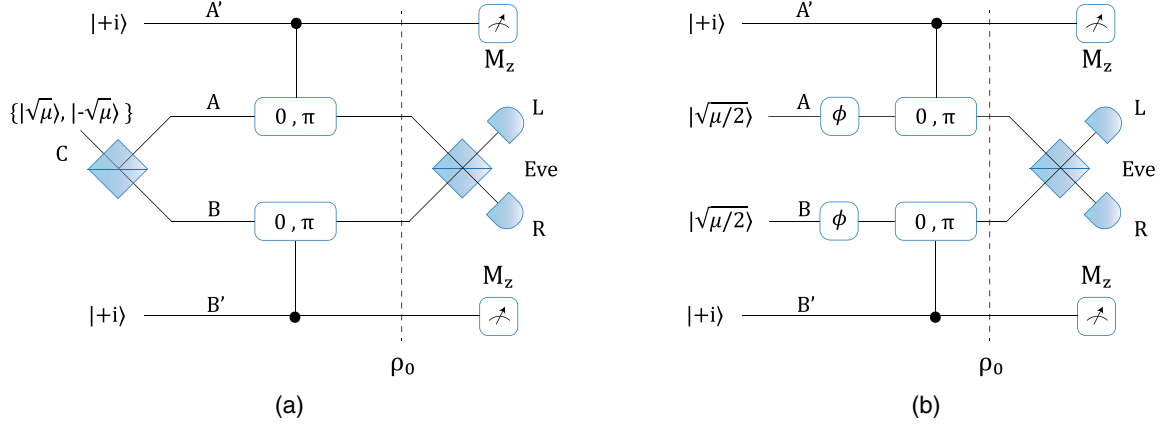
FIG. 5.   (a) A specific realization of Protocol I, where Charlie prepares $|\sqrt{\mu}\rangle$ and $|\sqrt{-\mu}\rangle$ with equal probabilities. (b) Schematic diagram of Protocol II, where Alice and Bob prepare $|\sqrt{\mu/2}\rangle$ and add the same random phase $\phi \in \{0, \pi\}$.

coherent state $|\sqrt{\mu}\rangle_C$ as the photon source. In addition, Charlie adds a random phase $\phi \in \{0, \pi\}$ with equal probabilities to the coherent state, so the density matrix can be written as

$$\rho(\alpha, -\alpha) = \frac{1}{2}(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|)$$

$$= c_{\text{odd}}|\alpha_{\text{odd}}\rangle\langle\alpha_{\text{odd}}| + c_{\text{even}}|\alpha_{\text{even}}\rangle\langle\alpha_{\text{even}}|, \quad (A25)$$

where $\alpha = \sqrt{\mu}$, and $|\alpha_{\text{odd}}\rangle$, $|\alpha_{\text{even}}\rangle$, c_{odd}, and c_{even} are defined in Eqs. (A4) and (A5). Clearly, one can see that $\rho(\alpha, -\alpha) \in \mathcal{D}(\mathcal{H}_{\text{odd}}^C \oplus \mathcal{H}_{\text{even}}^C)$.

Now, Alice and Bob want to prepare the state given in Eq. (A25) without Charlie's assistance. They first locally prepare two coherent states $|\sqrt{\mu/2}\rangle_{A(B)}$ and add the same random phase $\phi \in \{0, \pi\}$ to their states, as shown in Fig. 5(b). Then, the state becomes

$$\rho_{AB}(\sqrt{\mu}, -\sqrt{\mu}) = \frac{1}{2}(|\sqrt{\mu/2}\rangle_A\langle\sqrt{\mu/2}| \otimes |\sqrt{\mu/2}\rangle_B$$

$$\times \langle\sqrt{\mu/2}| + |\sqrt{-\mu/2}\rangle_A$$

$$\times \langle\sqrt{-\mu/2}| \otimes |\sqrt{-\mu/2}\rangle_B\langle\sqrt{-\mu/2}|).$$

$$(A26)$$

Apparently, $\rho_{AB}(\sqrt{\mu}, -\sqrt{\mu})$ is the state after $\rho(\alpha, -\alpha)$ defined in Eq. (A25) going through the BS. Thus, this new protocol (Protocol II) is equivalent to Protocol I with the input state $\rho(\sqrt{\mu}, -\sqrt{\mu})$. Protocol II runs as follows, as shown in Fig. 5(b). Here, $\mu_a = \mu_b = \mu/2$.

Protocol II

(1) State preparation: Alice and Bob prepare coherent states $|\sqrt{\mu_a}\rangle$ and $|\sqrt{\mu_b}\rangle$ on optical modes A and B, respectively. They initialize the qubits A' and B' in $|+i\rangle$. They add the same random phase $\phi \in \{0, \pi\}$ on the optical modes A and B. Alice applies the control gate C_π, defined in Eq. (A9), to qubit A' and

optical pulse A. Similarly, Bob applies C_π to B' and B.

(2) Measurement: The two optical pulses A and B are sent to an untrusted party, Eve, who is supposed to perform interference measurement and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection result, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the qubits of systems A' and B'. In addition, Bob applies a Pauli Y-gate to his qubit if Eve's announcement is an R click.

(5) Parameter estimation: After many rounds of the above steps, Alice and Bob end up with a joint $2n$-qubit state, denoted by $\rho_{A'B'}^{(n)}$. They then perform random sampling on the remaining $\rho_{A'B'}^{(n)}$ to estimate E^Z and infer E^X by Eq. (A24).

(6) Key distillation: Alice and Bob apply a standard EDP when the error rates are below a certain threshold. The distillation ratio r is given by Eq. (A15). Once Alice and Bob obtain nr (almost) pure EPR pairs, they both perform local Z measurements on the qubits to generate private keys.

From Protocol II to the PM-QKD protocol, there are still some missing links.

(1) Alice and Bob need to add the same random phase $\phi \in \{0, \pi\}$ to their states, which would cost them a private bit.

(2) They use Eq. (A24) to infer E^X, which needs information on the parameters of q_{odd}, q_{even}, e_{odd}^Z, and e_{even}^Z.

(3) The phase references of Alice and Bob's coherent states are locked. That is, the phases of the initial coherent states, $|\sqrt{\mu_a}\rangle$ and $|\sqrt{\mu_b}\rangle$, are the same, and hence remote phase locking is required.

We shall remove the simultaneous phase randomization requirement in Appendix A 4; bound q_{odd}, q_{even}, e_{odd}^Z, and
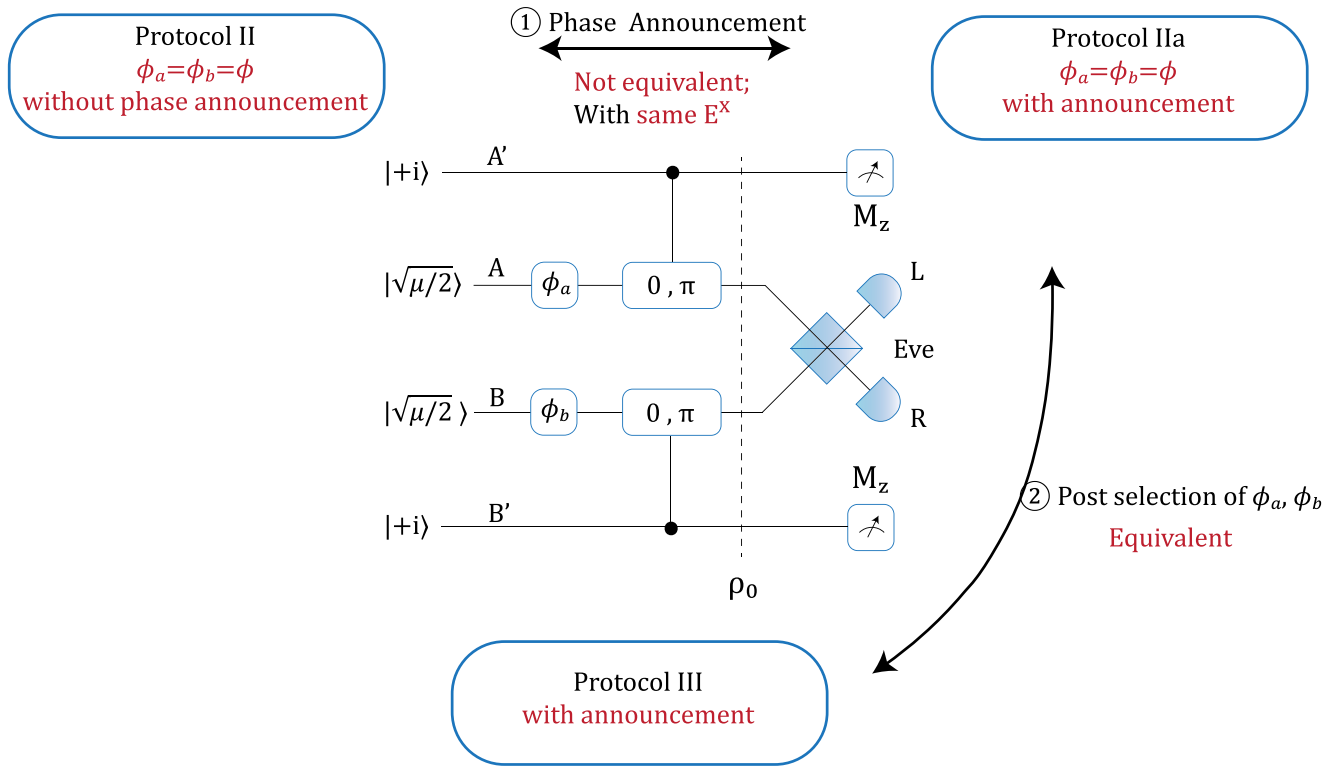
FIG. 6. The schematic diagram of protocols II, IIa, and III. In Protocol II, Alice and Bob add the same phase $\phi \in \{0, \pi\}$ on their coherent state $\sqrt{\mu/2}$. In Protocol IIa, Alice and Bob announce the phase ϕ after Eve's announcement. In Protocol III, Alice and Bob add phases ϕ_a and ϕ_b, independently. They announce ϕ_a and ϕ_b after Eve's announcement.

e_{even}^Z in Appendix A 5; and remove the phase-locking requirement in Appendix A 6.

4. Security with phase announcement

To remove the simultaneous phase randomization requirement in Protocol II, a straightforward idea is that Alice and Bob add random phases $\phi_{a(b)} \in \{0, \pi\}$ independently (with equal probability $1/2$); during the sifting step, they announce the phases ϕ_a, ϕ_b and postselect the bits only for $\phi_a = \phi_b$, as shown in Fig. 6. All the other steps remain unchanged. Here, there are two modifications that need to be analyzed, the phase announcement of ϕ_a, ϕ_b and postselection of $\phi_a = \phi_b$.

We deal with the phase announcement of ϕ_a, ϕ_b first. Consider Protocol IIa, as shown in Fig. 6, where Alice and Bob announce the random phase ϕ in Protocol II during postprocessing.

Protocol IIa

(1) State preparation: Same as Protocol II.
(2) Measurement: Same as Protocol II.
(3) Announcement: Same as Protocol II.
(4) Sifting: The first part is the same as Protocol II. After that, Alice and Bob announce the random phase ϕ.
(5) Parameter estimation: Same as Protocol II.
(6) Key distillation: Same as Protocol II.

Note that the only difference between Protocol II and IIa is that Alice and Bob announce their phase ϕ after Eve's announcement. Since the classical information announced during postprocessing is different, according to Definition 1, protocols II and IIa are not equivalent. In fact, from some specific attacks (see Appendix C), one can see that the security of the two protocols with and without phase announcement can be very different.

In Protocol II, as shown in Fig. 6, because of phase randomization, one can always assume that Alice and Bob (or Eve) perform the total parity measurement $\{M_{\text{odd}}^t, M_{\text{even}}^t\}$, which is defined as, similar to Eq. (A7),

$$M_{\text{odd}}^t \equiv \sum_{k_1 + k_2 \text{is odd}} |k_1 k_2\rangle_{AB} \langle k_1 k_2|,$$

$$M_{\text{even}}^t \equiv \sum_{k_1 + k_2 \text{is even}} |k_1 k_2\rangle_{AB} \langle k_1 k_2|. \tag{A27}$$

Here, $\{|k_1 k_2\rangle_{AB}\}$ are the Fock states on mode A, B, with k_1 photons on A and k_2 photons on B. That is, in Protocol II, the photon source can be regarded as a mixture of odd states and even states. The parity-state channel model is similar to the photon number channel used in the security proof of the decoy-state method [19,25].

In Protocol IIa, as shown in Fig. 6, on the other hand, no such parity measurement is allowed because it does not

commute with the phase announcement. That is, Eve can distinguish whether or not Alice and Bob perform $\{M^t_{\text{odd}}, M^t_{\text{even}}\}$ after the announcement of phases ϕ_a and ϕ_b. In other words, the quantum signals sent by Alice and Bob can no longer be regarded as a mixture of ρ_{odd} and ρ_{even} in Protocol IIa. To analyze the security of Protocol IIa, we notice the following observation.

Observation 1. The joint states $\rho^{(n)}_{A'B'}$ obtained in protocols I, II, and IIa are the same after sifting in Step 4.

Note that qubit systems A' and B' are local and never sent to Eve. Before the sifting step, these qubits are identical and sampled independently and the same for protocols I, II, and IIa. The state $\rho^{(n)}_{A'B'}$ is postselected by Eve's announcement. Of course, Eve can manipulate $\rho^{(n)}_{A'B'}$ by different measurement or announcement strategies. We emphasize that *Eve announces before the phase announcement in Protocol IIa.* Then, her strategy cannot depend on the phase announcement. Therefore, in all three protocols, the state $\rho^{(n)}_{A'B'}$ remains the same. This is crucial to our security analysis. From Observation 1, we can have the following Corollary.

Corollary 1. Both the X- and Z-error patterns of the joint states $\rho^{(n)}_{A'B'}$ in protocols II and IIa are the same. Then, the X-error rates E^X of protocols II and IIa are the same, as given by Eq. (A24).

Now, we deal with the postselection of $\phi_a = \phi_b$. Regardless of the values of ϕ_a, ϕ_b, because of control-phase gates C_π, the state ρ_{AB} sent to Eve is

$$\rho_{AB} = \rho_A(\sqrt{\mu/2}, -\sqrt{\mu/2}) \otimes \rho_B(\sqrt{\mu/2}, -\sqrt{\mu/2}), \quad (A28)$$

where $\rho(\sqrt{\mu/2}, -\sqrt{\mu/2})$ is defined in Eq. (A25). The state ρ_{AB} is independent of ϕ_a, ϕ_b; hence, Eve's attack cannot depend on ϕ_a, ϕ_b, and the sifted qubits are also independent of the value of $\phi_a(=\phi_b)$.

Furthermore, we notice that discarded qubits with $|\phi_a - \phi_b| = \pi$ can also be used for entanglement distillation. Here, adding a phase π to system B is equivalent to performing a Pauli Y-gate to system B' for a parity-state source in protocols I, II, and IIa. Thus, for the qubits with $|\phi_a - \phi_b| = \pi$, Bob performs a Y-gate on qubit B'.

Therefore, if Alice and Bob randomize their phases ϕ_a, $\phi_b \in \{0, \pi\}$ independently and perform phase-sifting operations after Eve's announcement, shown in Fig. 6, the modified protocol is equivalent to Protocol IIa. We call this Protocol III, which runs as follows, as shown in Fig. 6. Here, $\mu_a = \mu_b = \mu/2$.

Protocol III

(1) State preparation: Alice and Bob prepare coherent states $|\sqrt{\mu_a}\rangle$ and $|\sqrt{\mu_b}\rangle$ on optical modes A, B, separately. They initial their qubits A', B' in $|+i\rangle$. They independently add random phases ϕ_a, $\phi_b \in \{0, \pi\}$ on optical modes A, B. Alice applies the control gate C_π, defined in Eq. (A9), to qubit A' and optical pulse A. Similarly, Bob applies C_π to B' and B.

(2) Measurement: The two optical pulses, A and B, are sent to an untrusted party, Eve, who is supposed to perform an interference measurement and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection result, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the qubits of systems A' and B'. Bob applies a Pauli Y-gate to his qubit if Eve's announcement is R click. After Eve's announcement, Alice and Bob announce their encoded phase ϕ_a, ϕ_b. Bob applies a Pauli Y-gate to his qubit if $|\phi_a - \phi_b| = \pi$.

(5) Parameter estimation: After many rounds of the above steps, Alice and Bob end up with a joint $2n$-qubit state, denoted by $\rho^{(n)}_{A'B'}$. They then perform random sampling on the remaining $\rho^{(n)}_{A'B'}$ to estimate E^Z and infer E^X by Eq. (A24).

(6) Key distillation: Alice and Bob apply a standard EDP when the error rates are below a certain threshold. The distillation ratio r is given by Eq. (A15). Once Alice and Bob obtain nr (almost) pure EPR pairs, they both perform local Z measurements on the qubits to generate private keys.

5. Decoy-state method and phase randomization

Here, we introduce a method to estimate q_{odd}, q_{even}, e^Z_{odd}, and e^Z_{even}. Without loss of generality, we mainly discuss the decoy-state method in Protocol I. Similar arguments can be applied to protocols II, IIa, and III.

Recall that, in Protocol I, if Charlie prepares coherent state $|\sqrt{\mu}\rangle$ and adds a random phase $\{0, \pi\}$ on it, it is equivalent to preparing odd- and even-parity states with probabilities $p^\mu_{\text{odd}} = c_{\text{odd}}$ and $p^\mu_{\text{even}} = c_{\text{even}}$, respectively, as defined in Eq. (A5). Define the yield Y^μ_{odd} (Y^μ_{even}) as the probability of successful detection conditional on the odd-parity (even-parity) state. The fraction of odd- and even-parity states in the final detected signal is given by

$$q^\mu_{\text{odd}} = p^\mu_{\text{odd}} \frac{Y^\mu_{\text{odd}}}{Q_\mu},$$

$$q^\mu_{\text{even}} = p^\mu_{\text{even}} \frac{Y^\mu_{\text{even}}}{Q_\mu}, \quad (A29)$$

where Q_μ is the total gain of the signals. For signals with intensity μ, we have

$$Q^\mu = p^\mu_{\text{odd}} Y^\mu_{\text{odd}} + p^\mu_{\text{even}} Y^\mu_{\text{even}},$$

$$E^{Z,\mu} Q^\mu = e^{Z,\mu}_{\text{odd}} p^\mu_{\text{odd}} Y^\mu_{\text{odd}} + e^{Z,\mu}_{\text{even}} p^\mu_{\text{even}} Y^\mu_{\text{even}}, \quad (A30)$$

where E^Z_μ, $e^{Z,\mu}_{\text{odd}}$ ($e^{Z,\mu}_{\text{even}}$) are the quantum bit error rate (QBER) and the Z-error rate of odd-state (even-state) signals with total a intensity of μ, respectively.

If we directly estimate q_{odd}^μ, q_{even}^μ, $e_{\text{odd}}^{Z,\mu}$, and $e_{\text{even}}^{Z,\mu}$ from Eq. (A29), Eq. (A30), and the constraint that

$$q_{\text{odd}}^\mu, q_{\text{even}}^\mu, e_{\text{odd}}^{Z,\mu}, e_{\text{even}}^{Z,\mu}, Y_{\text{odd}}^\mu, Y_{\text{even}}^\mu \in [0,1], \qquad \text{(A31)}$$

then the estimation is too loose to bound the X-error E^X in Eq. (A24).

Now, we introduce a more efficient method to estimate q_{odd}, q_{even}, e_{odd}^Z, and e_{even}^Z. Essentially, we employ the idea of the decoy-state method [25]. That is, in Protocol I, Charlie adjusts the intensity μ of his prepared coherent lights. After Eve's announcement, Charlie announces the value of μ. Furthermore, Charlie randomizes the phase ϕ on state $|\sqrt{\mu}e^{i\phi}\rangle$ continuously from $[0, 2\pi)$. In this case, the state prepared by Charlie can be written as

$$\frac{1}{2\pi} \int_0^{2\pi} d\phi |\sqrt{\mu}e^{i\phi}\rangle\langle\sqrt{\mu}e^{i\phi}| = \sum_{k=0}^{\infty} P(k)|k\rangle\langle k|. \quad \text{(A32)}$$

That is, in Protocol I, if Charlie prepares $|\sqrt{\mu}e^{i\phi}\rangle$ with random phase ϕ, this is equivalent to preparing the Fock states $\{|k\rangle\}$ with probability $P(k)$. Obviously, Fock states $\{|k\rangle\}$ are parity states. Then, by directly applying Lemma 1, we can estimate the X-error by

$$E^X = \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z), \qquad \text{(A33)}$$

where q_0 is the detection caused by the vacuum signal (i.e., dark counts) and $e_0^Z = e_0 = 1/2$ is the vacuum Z-error rate.

The source components are Fock states $\{|k\rangle\}$, whose yields $\{Y_k\}$ and Z-error rates $\{e_k^Z\}$ are independent of μ. The fractions q_k^μ of the "k-photon component" in the final detected signals are given by

$$q_k^\mu = P^\mu(k)\frac{Y_k}{Q_\mu}. \qquad \text{(A34)}$$

The overall gain and QBER are given by

$$Q_\mu = \sum_{k=0}^{\infty} P^\mu(k) Y_k,$$

$$E_\mu^Z Q_\mu = \sum_{k=0}^{\infty} e_k^Z P^\mu(k) Y_k. \qquad \text{(A35)}$$

The main idea of the decoy-state method is that Alice and Bob can obtain a set of linear equations in the form of Eqs. (A34) and (A35) by using a few values of μ. When an infinite amount of decoy states is used, Alice and Bob can estimate all the parameters Y_k and e_k^Z accurately, with which they can estimate q_k^μ, e_k^Z and the upper bound of the X-error by Eq. (A33).

To apply the decoy-state method to protocols II and III, we modify the phase randomization requirements accordingly. In the decoy-state version of Protocol III, the phases ϕ_a, ϕ_b should be randomized independently in $[0, 2\pi)$ rather than $\{0, \pi\}$. Also, there will be an additional phase-sifting condition, $|\phi_a - \phi_b| = 0$ or π. Such random-phase announcement and postselection would not affect the security, with the following reasons, similar to the argument of the equivalence between protocols II and III. In particular, Observation 1 in Appendix A 4 still holds.

First, we want to argue that the random-phase postselection of $|\phi_a - \phi_b| = 0$ or π would not affect the security. In fact, any phase postselection would not be affected by Eve's announcement. Note that the random phases ϕ_a, ϕ_b are determined by Alice and Bob locally. Thus, the sifted qubit pairs $\rho_{A'B'}^{(n)}$ would be the same in the two cases: (1) Alice and Bob independently randomize the phases ϕ_a, ϕ_b and employ this phase postselection $|\phi_a - \phi_b| = 0$ or π; (2) Charlie randomizes the same phases, $\phi_a = \phi_b$, to A and B.

Second, we want to argue that the random-phase announcement would not affect the security. Eve announces the detection events before Alice and Bob's random-phase announcement. Thus, her hacking strategy cannot depend on the random phases. Note that with the postselection of $|\phi_a - \phi_b| = 0$ or π, the announced phase ϕ_a (or ϕ_b) can be regarded as the phase reference in Protocol III.

Third, we apply infinite decoy states to estimate q_k^μ and e_k^Z accurately. In practical implementations, it is interesting to explore if finite decoy states, such as the widely applied vacuum and weak decoy states, are enough to make a valid estimation.

Now, we can modify Protocol III with continuous phase randomization ϕ_a, ϕ_b and the decoy-state method, namely, Protocol IV, as shown in Fig. 7(a).

Protocol IV

(1) State preparation: Alice and Bob randomly select μ_a, μ_b from a given set $\{\mu_0, \mu_1, \ldots\}/2$. They prepare coherent state $|\sqrt{\mu_a}\rangle$ and $|\sqrt{\mu_b}\rangle$ on optical modes A, B separately. They initial their qubits A', B' in $|+i\rangle$ and independently add random phase ϕ_a, $\phi_b \in [0, 2\pi)$ on the optical modes A, B. Alice applies the control gate C_π, defined in Eq. (A9), to qubit A' and optical pulse A. Similarly, Bob applies C_π to B' and B.

(2) Measurement: The two optical pulses A and B are sent to an untrusted party, Eve, who is supposed to perform interference measurement and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection result, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the qubits of systems A' and B'. Bob applies a Pauli Y-gate to his qubit if Eve's announcement is R click. After Eve's announcement, Alice
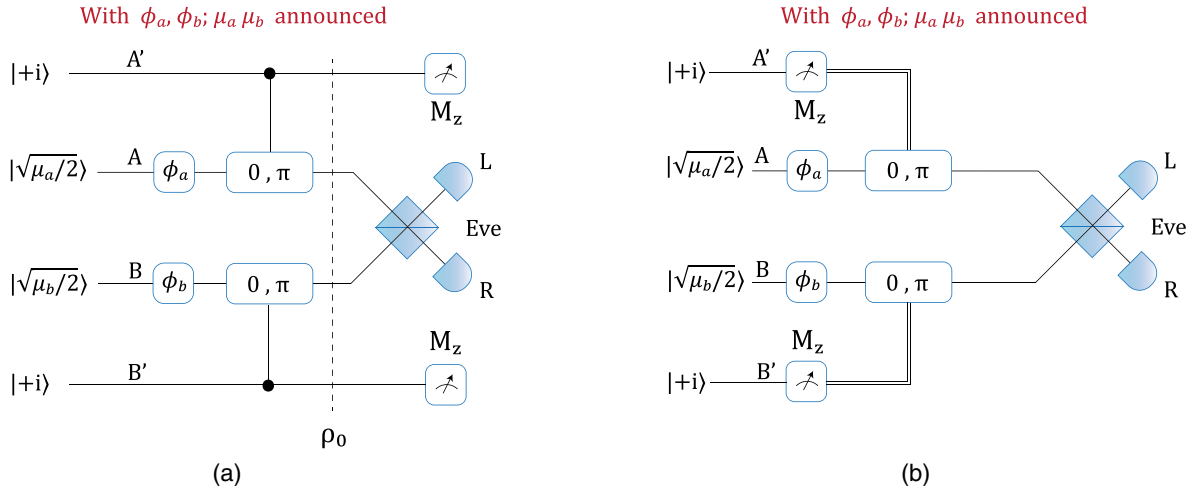
FIG. 7. (a) Schematic diagram of Protocol IV, where the decoy-state method is applied. The random phase ϕ_a, $\phi_b \in [0, 2\pi)$. (b) Schematic diagram of PM-QKD protocol.

and Bob announce their encoded intensities μ_a, μ_b and phases ϕ_a, ϕ_b. They keep the signal if $\mu_a = \mu_b$ and $|\phi_a - \phi_b| = 0$ (or π). Bob applies a Pauli Y-gate to his qubit if $|\phi_a - \phi_b| = \pi$.

(5) Parameter estimation: After many rounds of the above steps, Alice and Bob end up with a joint $2n$-qubit state, denoted by $\rho_{A'B'}^{(n)}$. They then perform random sampling on the remaining $\rho_{A'B'}^{(n)}$ to estimate E^Z and infer E^X by Eq. (A33).

(6) Key distillation: Alice and Bob apply a standard EDP when the error rates are below a certain threshold. The distillation ratio r is given by Eq. (A15). Once Alice and Bob obtain nr (almost) pure EPR pairs, they both perform local Z measurements on the qubits to generate private keys.

Finally, we need to reduce the entanglement-based protocol to a prepare-and-measure protocol. Following the Shor-Preskill argument, we move the key measurement in Step 6 before the EDP, the parameter estimation, and the C_π gates. That is, they measure the systems A' and B' at the beginning. Therefore, the entanglement-based protocol (Protocol IV) becomes the PM-QKD protocol, as shown in Fig. 7(b).

PM-QKD protocol

(1) State preparation: Alice randomly generates a key bit $\kappa_a \in \{0, 1\}$; a random phase $\phi_a \in [0, 2\pi)$; and a random intensity $\mu_a \in \{\mu/2, \mu_1/2, \mu_2/2, \cdots\}$. She prepares a coherent-state optical pulse $\left|\sqrt{\mu_a}e^{i(\phi_a + \pi\kappa_a)}\right\rangle_A$. Similarly, Bob generates a key bit κ_b and prepares $\left|\sqrt{\mu_b}e^{i(\phi_b + \pi\kappa_b)}\right\rangle_B$.

(2) Measurement: The two optical pulses A and B are sent to an untrusted party, Eve, who is supposed to perform interference measurement and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection result, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the key bits κ_a and κ_b. Bob flips his key bit κ_b if Eve's announcement is R click. After Eve's announcement, Alice and Bob announce their encoded intensities and phases μ_a, ϕ_a; μ_b, ϕ_b. They maintain the signal if $\mu_a = \mu_b$ and $|\phi_a - \phi_b| = 0$ or π. Bob applies a Pauli Y-gate to his qubit if $|\phi_a - \phi_b| = \pi$.

(5) Parameter estimation: After many rounds of the above steps, Alice and Bob end up with joint n pairs of the raw key. They then perform random sampling on this raw key. With Eqs. (A34) and (A35), they estimate q_k and e_k^Z.

(6) Key distillation: Alice and Bob apply classical communication for error correction and privacy amplification. The key distillation ratio r is given by Eq. (A15).

Note that the PM-QKD protocol mentioned above is the exact PM-QKD protocol mentioned in the main text with the decoy-state method contained.

Here, in Protocol IV and the PM-QKD protocol, there are some unrealistic assumptions remaining.

(1) The phase of Alice and Bob's coherent state is locked; that is, the phase reference of Alice's and Bob's coherent state is the same.

(2) The phase-sifting condition $\phi_a = \phi_b$ can be satisfied with an acceptable probability.

We will discuss how to remove these two requirements in Appendix A 6 and, hence, make the protocol practical.

6. Phase postcompensation

Here, we modify the PM-QKD protocol to remove the requirement of phase locking between Alice and Bob, and also relax the postselection condition of $|\phi_a - \phi_b| = 0$ or π. The method is shown in Fig. 2.

First, we relax the postselection condition of $|\phi_a - \phi_b| = 0$ or π by dividing the phase interval $[0, 2\pi)$ into M slices $\{\Delta_j\}$ for $0 \leq j \leq M-1$, where $\Delta_j = [2\pi j/M, 2\pi(j+1)/M)$. We change the phase postselection condition of $\phi_a = \phi_b$ to slice postselection $j_a = j_b$. Here, j_a, j_b are defined as

$$j_a = \left[\frac{\phi_a}{2\pi} M\right] \mod M,$$

$$j_b = \left[\frac{\phi_b}{2\pi} M\right] \mod M, \qquad (A36)$$

where $[\cdot]$ is the round function to output the nearest integer. That is, Alice announces the j_ath slice Δ_{j_a}, which her random phase ϕ_a falls into. Similarly, Bob announces j_b. The sifting condition is $|j_b - j_a| = 0$ or $M/2$. This technique is first used in the phase-encoding MDI-QKD [18]. Announcing the phase slices j_a and j_b rather than the exact phase ϕ_a and ϕ_b will only leak less information to Eve. Thus, all the security-proof results from previous subsections apply here. Applying Eq. (A15), we also need to add a phase-sifting factor $2/M$. Therefore, the final key rate is given by

$$R_{\mathrm{PM}} \geq \frac{2}{M} Q_\mu [1 - fH(E_\mu^Z) - H(E_\mu^X)], \qquad (A37)$$

where Q_μ is the total gain of the pulses, E_μ^Z is the overall QBER, the phase error rate E_μ^X is given by Eq. (A33), and f is the error correction efficiency. We need to point out that, when M is too small, the misalignment caused by phase slices Δ_{j_a} and Δ_{j_b} is big and results in a large QBER E_μ^Z.

Second, we remove the requirement of phase locking. In the phase postselection step, either Alice or Bob announces that the random phase is sufficient. Without loss of generality, we assume that Alice announces the phase and Bob performs the sifting of $|j_b - j_a| = 0$ or $M/2$. With less information announced, the key rate still holds.

Suppose that the difference between Alice's and Bob's phase references, denoted by $\phi_0 \in [0, 2\pi)$, is fixed but unknown. In sifting, Bob needs to figure out the value of ϕ_0. Define an offset, where $0 \leq j_0 \leq M-1$, as

$$j_0 \equiv \left[\frac{\phi_0}{2\pi} M\right] \mod M. \qquad (A38)$$

During sifting, Bob can estimate the offset j_0 for each pulse. The estimation accuracy would not affect the security. In fact, in the security proofs, we assume that Eve knows the phase references ahead. Suppose Bob compensates the offset by j_d, and he has the freedom to choose j_d from $\{0, 1, ..., M-1\}$. In a practical scenario, normally, the phase references (and, hence, the offset j_0) change slowly with time. Then, Bob can figure out the

proper phase compensation offset j_d by minimizing the QBER from random sampling, as shown in Fig. 2.

For the case where the phase reference difference ϕ_0 varies, we can treat the changing caused by Eve. Such deviation will introduce bit errors, but not help Eve learn key information, since the variation of ϕ_0 is independent of the key κ_a, κ_b. Note that, in the security proof, we assume that Eve knows the phase references accurately.

With all the modifications above, we propose the following practical version of PM-QKD protocol.

PM-QKD protocol with phase postcompensation

(1) State preparation: Alice randomly generates a key bit $\kappa_a \in \{0, 1\}$; a random phase $\phi_a \in [0, 2\pi)$; and a random intensity $\mu_a \in \{\mu/2, \mu_1/2, \mu_2/2, \cdots\}$. She prepares a coherent-state optical pulse $|\sqrt{\mu_a} e^{i(\phi_a + \pi\kappa_a)}\rangle_A$. Similarly, Bob generates a key bit κ_b and prepares $|\sqrt{\mu_b} e^{i(\phi_b + \pi\kappa_b)}\rangle_B$.

(2) Measurement: The optical pulses, systems A and B, are sent to an untrusted party, Eve, who is supposed to perform interference measure and record which detector (L or R) clicks.

(3) Announcement: Eve announces the detection results, L/R click or failure, for each round.

(4) Sifting: When Eve announces an L/R click, Alice and Bob keep the key bits κ_a and κ_b. Bob flips his key bit κ_b if Eve's announcement is R click. After Eve's announcement, Alice and Bob announce their encoded intensities μ_a and μ_b, respectively. They keep the bits if $\mu_a = \mu_b$.

(5) Parameter estimation: Alice and Bob run the above procedures many times and then run the following procedures.

   (a) For each bit, Alice announces the phase slice index j_a, given in Eq. (A36), and she randomly samples a certain amount of key bits and announces them for QBER testing.

   (b) In the phase postcompensation method, given an offset compensation $j_d \in \{0, 1, ..., M/2 - 1\}$, Bob sifts the sampled bits with the phase postselection condition $|j_b + j_d - j_a| \mod M = 0$ or $M/2$. For the case of $M/2$, Bob flips the key bit κ_b. After sifting, Bob calculates the QBER E^Z with Alice's sampling key bits. Bob tries all possible $j_d \in \{0, 1, ..., M-1\}$ and figures out the proper j_d to minimize the sampling QBER. Using the phase postselection condition with the proper j_d, Bob sifts (and flips if needed) the unsampled bits and announces the locations to Alice. Alice sifts her key bits accordingly.

   (c) Alice and Bob analyze the overall gain Q_{μ_i} and QBER $E_{\mu_i}^Z$ for different values of intensities $\mu_a = \mu_b = \mu_i/2$. They estimate the phase error rate $E_\mu^{(X)}$ by Eq. (A33).

(6) Key distillation: Alice and Bob apply error correction and privacy amplification. The key rate R is given by Eq. (A37).

Here, in the phase postcompensation, Bob does not need to fix a j_d for the whole experiment. Instead, he can adjust j_d in real time. Given the total number of slices M, define the phase-stable time τ_M to be the time period during which the phase fluctuation is smaller than π/M. Roughly speaking, Bob adjusts j_d for every τ_M. In practice, Bob would randomly sample some detections for tests. Here, in order to obtain a good estimation of j_d, Bob should sample enough detections for the offset test within τ_M. Then, the phase postcompensation method would put a requirement on the detection rate.

Now, we consider a practical example. Considering the slice number $M = 16$, the tolerable fluctuation should be about $\pi/M = 0.196$ rad. The phase of a continuous-wave (CW) laser pulse usually fluctuates randomly, and its behavior can be modeled as a random walk. In an experimental work of testing the phase drift for a 36.5-km Mach-Zehnder interferometer [43], within a time duration of 0.2 ms, the mean phase fluctuation is about 0.15 rad. In the data presented in recent TF-QKD [16], via the total transmission distance around 200 km, the phase drift rate is about 3 rad ms^{-1}. For a time period of 0.05 ms, the mean phase fluctuation is about 0.15 rad, which is less than π/M. Then, in this case, one can set $\tau_M = 0.05$ ms for testing. Considering a GHz QKD system, there are 5×10^4 signals sent out within τ_M. Using the same parameters for a longer transmission distance of 100 km from Alice to Eve (same distance for Bob) using a standard telecom fiber (0.2 dB/km), the transmission loss is $\eta = 20 \ dB = 10^{-2}$, and there will be 500 data left for postprocessing, which is sufficient for sampling tests. From here, one can see that our phase postcompensation method is feasible with current technology. For a longer transmission distance, the phase postcompensation method may not be sufficient. One can use the phase calibration method as an alternative, as introduced in the main text.

APPENDIX B: MODEL AND SIMULATION

Here, we show the details for the simulations of different QKD schemes. We mainly follow the simulation model used in the literature [19,44]. We calculate the detection probabilities of PM-QKD in Appendix B 1 and then evaluate the yields, gains, and error rates in Appendix B 2. In simulations, we also compare the performance of PM-QKD with the decoy-state BB84 [1], MDI-QKD [15], and the linear key-rate bound [11]. We list the used formulas and simulation parameters in Appendix B 3.

1. Detection probabilities

The channel is assumed to be a pure loss one and symmetric for Alice and Bob with transmittance η

(with detector efficiency η_d taken into account). We suppose that the lights from Alice and Bob faithfully interfered and measured with dark-count rate p_d. Without loss of generality, we only consider the case where $\kappa_a = \kappa_b = 0$, $j_a = j_b = 0$.

In PM-QKD, the global phases ϕ_a, ϕ_b are divided into M slices. Without phase locking, the phase references for Alice and Bob can differ. Therefore, even if the announced slices meet, $|j_a - j_b| = 0$, there may be a considerable difference $\phi_\delta \equiv \phi_b - \phi_a$ between the two global phases ϕ_a, ϕ_b.

First, for a fixed ϕ_δ, we calculate the detection probability in the single-photon case. After Alice and Bob's encoding, the state becomes

$$(e^{i\phi_a}a^\dagger + e^{i\phi_b}b^\dagger)|00\rangle_{A0,B0} = (a^\dagger + e^{i\phi_\delta}b^\dagger)|0\rangle. \quad \text{(B1)}$$

Here, the transmittance η includes channel losses and detection efficiencies, which transfer $a^\dagger$, $b^\dagger$ according to

$$a^\dagger \to \sqrt{\eta}a^\dagger + \sqrt{1-\eta}s^\dagger,$$
$$b^\dagger \to \sqrt{\eta}b^\dagger + \sqrt{1-\eta}t^\dagger, \quad \text{(B2)}$$

where $s^\dagger$, $t^\dagger$ are the modes coupled to the environment. Before Eve's interference, the state is

$$(\sqrt{\eta}(a^\dagger + e^{i\phi_\delta}b^\dagger) + \sqrt{1-\eta}(s^\dagger + e^{i\phi_\delta}t^\dagger))|0\rangle, \quad \text{(B3)}$$

and after Eve's interference, the state becomes

$$\left\{\sqrt{\frac{\eta}{2}}[(1+e^{i\phi_\delta})l^\dagger + (1-e^{i\phi_\delta})r^\dagger] + \sqrt{1-\eta}(s^\dagger + e^{i\phi_\delta}t^\dagger)\right\}|0\rangle, \quad \text{(B4)}$$

where $l^\dagger$ and $r^\dagger$ are the creation operators for the modes to L- and R-detectors, respectively. Then, the detection probabilities are given by

$$p_0^{(1)} = 1 - \eta,$$
$$p_l^{(1)} = \eta\cos^2\left(\frac{\phi_\delta}{2}\right),$$
$$p_r^{(1)} = \eta\sin^2\left(\frac{\phi_\delta}{2}\right),$$
$$p_{lr}^{(1)} = 0, \quad \text{(B5)}$$

where $p_0^{(1)}$, $p_l^{(1)}$, $p_r^{(1)}$, and $p_{lr}^{(1)}$ are, respectively, the probabilities for no click, L click, R click, and double click for the single-photon case.

Then, we consider the k-photon case, for which we regard as k identical and independent click events of the single-photon case; the click probabilities are given by

TABLE III. Probability table of clicks with dark counts present.

Dark count condition		Contributions to the overall click probabilities			
L-dark count	R-dark count	No-click $P_0^{(k)}$	L-click $P_L^{(k)}$	R-click $P_R^{(k)}$	Double-click $P_{LR}^{(k)}$
$(1-p_d)$	$(1-p_d)$	$p_0^{(k)}$	$p_l^{(k)}$	$p_r^{(k)}$	$p_{lr}^{(k)}$
$(1-p_d)$	p_d	0	0	$p_0^{(k)}+p_r^{(k)}$	$p_l^{(k)}+p_{lr}^{(k)}$
p_d	$(1-p_d)$	0	$p_0^{(k)}+p_l^{(k)}$	0	$p_r^{(k)}+p_{lr}^{(k)}$
p_d	p_d	0	0	0	1

$$p_0^{(k)} = (p_0^{(1)})^k,$$
$$p_l^{(k)} = (p_0^{(1)} + p_l^{(1)})^k - (p_0^{(1)})^k,$$
$$p_r^{(k)} = (p_0^{(1)} + p_r^{(1)})^k - (p_0^{(1)})^k,$$
$$p_{lr}^{(k)} = 1 - p_0^{(k)} - p_l^{(k)} - p_r^{(k)}$$
$$= 1 + (p_0^{(1)})^k - (p_0^{(1)} + p_l^{(1)})^k - (p_0^{(1)} + p_r^{(1)})^k, \quad \text{(B6)}$$

where $p_0^{(k)}$, $p_l^{(k)}$, $p_r^{(k)}$, and $p_{lr}^{(k)}$ are, respectively, the probabilities for no click, L click, R click, and double click for the k-photon case.

Now, we take into account the effects caused by the detector dark counts p_d. Since the dark counts are independent of the photon-click events, we can draw a table for all the cases, as shown in Table III. The final click probabilities for the k-photon case are given by

$$P_0^{(k)} = (1-p_d)^2 p_0^{(k)},$$
$$P_L^{(k)} = (1-p_d)^2 p_l^{(k)} + p_d(1-p_d)(p_0^{(k)} + p_l^{(k)})$$
$$= p_d(1-p_d)p_0^{(k)} + (1-p_d)p_l^{(k)},$$
$$P_R^{(k)} = (1-p_d)^2 p_r^{(k)} + p_d(1-p_d)(p_0^{(k)} + p_r^{(k)})$$
$$= p_d(1-p_d)p_0^{(k)} + (1-p_d)p_r^{(k)},$$
$$P_{LR}^{(k)} = (1-p_d)^2 p_{lr}^{(k)} + p_d(1-p_d)(p_l^{(k)} + p_r^{(k)} + 2p_{lr}^{(k)}) + p_d^2$$
$$= (1-p_d^2)p_{lr}^{(k)} + p_d(1-p_d)(p_l^{(k)} + p_r^{(k)}) + p_d^2. \quad \text{(B7)}$$

Similarly, we can derive the formulas for detection probabilities with coherent state inputs. The states sent out by Alice and Bob are $|\sqrt{\mu_a}e^{i\phi_a}\rangle$ and $|\sqrt{\mu_b}e^{i\phi_b}\rangle$, respectively, where $\mu_a = \mu_b = \mu/2$. After channel and detection losses, the states become $|\sqrt{\eta\mu_a}e^{i\phi_a}\rangle$ and $|\sqrt{\eta\mu_b}e^{i\phi_b}\rangle$. By going through the BS, the states become

$$|\alpha_L\rangle = \left|\frac{\sqrt{\eta\mu}}{2}(e^{i\phi_a} + e^{i\phi_b})\right\rangle = \left|\frac{\sqrt{\eta\mu}}{2}e^{i\phi_a}(1 + e^{i\phi_\delta})\right\rangle,$$
$$|\alpha_R\rangle = \left|\frac{\sqrt{\eta\mu}}{2}(e^{i\phi_a} - e^{i\phi_b})\right\rangle = \left|\frac{\sqrt{\eta\mu}}{2}e^{i\phi_a}(1 - e^{i\phi_\delta})\right\rangle. \quad \text{(B8)}$$

Then, the detection click probabilities are

$$P_\mu(\bar{L}) = (1-p_d)\exp(-|\alpha_L|^2)$$
$$= (1-p_d)\exp\left(-\eta\mu\cos^2\left(\frac{\phi_\delta}{2}\right)\right),$$
$$P_\mu(L) = 1 - P_\mu(\bar{L}),$$
$$P_\mu(\bar{R}) = (1-p_d)\exp(-|\alpha_R|^2)$$
$$= (1-p_d)\exp\left(-\eta\mu\sin^2\left(\frac{\phi_\delta}{2}\right)\right),$$
$$P_\mu(R) = 1 - P_\mu(\bar{R}), \quad \text{(B9)}$$

where $P_\mu(L)$ and $P_\mu(\bar{L})$ are the probabilities of the L click and no L click, respectively, and $P_\mu(R)$ and $P_\mu(\bar{R})$ are for the R-detector. These probabilities are similar to Eq. (B7). The difference is that the probabilities in Eq. (B7) are mutually exclusive, while in Eq. (B9), the probabilities $P_\mu(L)$ and $P_\mu(R)$ are independent.

All the above probability formulas are functions of the phase difference ϕ_δ. In the simulation, one needs to integrate ϕ_δ over its probability distribution $f_{\phi_\delta}(\phi)$. Recall that the phase reference deviation between Alice and Bob is ϕ_0. Here, with the phase postcompensation method introduced in Appendix A 6, we assume that ϕ_0 is uniformly distributed in $[-\pi/M, \pi/M)$, denoted by

$$\phi_0 \sim U[-\pi/M, \pi/M). \quad \text{(B10)}$$

In this case, ϕ_a and ϕ_b are uniformly distributed in $[0, 2\pi/M)$ and $[\phi_0, 2\pi/M + \phi_0)$, respectively,

$$\phi_a \sim U[0, 2\pi/M),$$
$$\phi_b \sim U[\phi_0, 2\pi/M + \phi_0). \quad \text{(B11)}$$

For a fixed ϕ_0, the probability distribution of the phase difference ϕ_δ is given by

$$f_{\phi_\delta}^{(\phi_0)}(\phi) = \begin{cases} \left(\frac{M}{2\pi}\right)^2 \left[\phi + \left(\frac{2\pi}{M} - \phi_0\right)\right] & \phi \in \left[\phi_0 - \frac{2\pi}{M}, \phi_0\right), \\ \left(\frac{M}{2\pi}\right)^2 \left[-\phi + \left(\frac{2\pi}{M} + \phi_0\right)\right] & \phi \in \left[\phi_0, \phi_0 + \frac{2\pi}{M}\right), \\ 0 & \text{otherwise.} \end{cases} \tag{B12}$$

Furthermore, in the simulation, one needs to take another integration of ϕ_0 over $[-\pi/M, \pi/M)$ to get the yields, gain, and error rates.

2. Yields, gain, and error rates

We first analyze the yield $\{Y_k\}$ for $k \geq 0$ and the total gain Q_μ according to the probability formulas given in Appendix B 1. Note that, in PM-QKD, both no-click and double-click events are regarded as failure detection. The yield Y_k of the k-photon state is given by Eqs. (B5)–(B7),

$$\begin{aligned} Y_k &= P_L^{(k)} + P_R^{(k)} = (1 - p_d)(p_l^{(k)} + p_r^{(k)}) + 2p_d(1 - p_d)p_0^{(k)} \\ &= (1 - p_d)\left[\left(1 - \eta\sin^2\left(\frac{\phi_\delta}{2}\right)\right)^k + \left(1 - \eta\cos^2\left(\frac{\phi_\delta}{2}\right)\right)^k\right] - 2(1 - p_d)^2(1 - \eta)^k \\ &\approx (1 - p_d)(1 + (1 - \eta)^k) - 2(1 - p_d)^2(1 - \eta)^k \\ &= (1 - p_d)[1 - (1 - 2p_d)(1 - \eta)^k] \\ &\approx 1 - (1 - 2p_d)(1 - \eta)^k. \end{aligned} \tag{B13}$$

Here, in the first approximation, we take the first order of a small ϕ_δ and ignore $\sin^2(\phi_\delta/2) = 0$. In the second approximation, we omit the higher-order term $p_d[1 - (1 - 2p_d)(1 - \eta)^k] = O(p_d^2 + p_d\eta)$, since normally p_d is small.

The total gain Q_μ is given by Eq. (B9),

$$\begin{aligned} Q_\mu &= P(L)P(\bar{R}) + P(\bar{L})P(R) \\ &= (1 - p_d)\exp\left(-\eta\mu\sin^2\left(\frac{\phi_\delta}{2}\right)\right)\left[1 - (1 - p_d)\exp\left(-\eta\mu\cos^2\left(\frac{\phi_\delta}{2}\right)\right)\right] \\ &\quad + (1 - p_d)\exp\left(-\eta\mu\cos^2\left(\frac{\phi_\delta}{2}\right)\right)\left[1 - (1 - p_d)\exp\left(-\eta\mu\sin^2\left(\frac{\phi_\delta}{2}\right)\right)\right] \\ &\approx (1 - p_d)[1 - (1 - p_d)\exp(-\eta\mu_b)] + p_d(1 - p_d)\exp(-\eta\mu_b) \\ &= (1 - p_d)[1 - (1 - 2p_d)e^{-\eta\mu}] \\ &\approx 1 - e^{-\eta\mu} + 2p_d e^{-\eta\mu}, \end{aligned} \tag{B14}$$

where the two approximations are the same as the ones used in Eq. (B13). Since ϕ_δ does not affect the yields Y_k and gain Q_μ much with the first-order approximation, the average yields Y_k and gain Q_μ over $\phi_\delta \in [-\pi/M, \pi/M)$ can be regarded as the ones when $\phi_\delta = 0$. Also, the results of Eqs. (B13) and (B14) are consistent with the ones presented in the regular QKD model [44], as shown in Eqs. (B29) and (B30).

Then, we calculate the bit error rate for the k-photon signal e_k^Z and the QBER E_μ^Z with coherent states input $\mu_a = \mu_b = \mu/2$. The bit error rate $e_k^Z(\phi_\delta)$ is given by

$$e_k^Z(\phi_\delta) = \frac{P_R^{(k)}}{P_L^{(k)} + P_R^{(k)}}, \tag{B15}$$

where $P_L^{(k)}$ and $P_R^{(k)}$ are given by Eqs. (B5)–(B7). The average bit error rate of e_k^Z over ϕ_δ is given by the following integral,

$$e_k^Z = \frac{M}{2\pi}\int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi\, f_{\phi_\delta}^{(\phi_0)}(\phi)e_k^Z(\phi), \tag{B16}$$

where $f_{\phi_\delta}^{(\phi_0)}(\phi)$ is given by Eq. (B12). For the case $k = 1$, we explicitly calculate the error rate e_1^Z, given by Eqs. (B5), (B6), (B7), and (B15),

$$\begin{aligned} e_1^Z(\phi_\delta) &= \frac{(1 - p_d)^2 p_l^{(1)} + p_d(1 - p_d)(p_0^{(1)} + p_l^{(1)})}{(1 - p_d)^2\eta + p_d(1 - p_d)(2 - \eta)} \\ &= \frac{\sin^2(\phi_\delta/2)\eta + p_d(1 - \eta)}{\eta + 2p_d(1 - \eta)}, \end{aligned} \tag{B17}$$

and integrate Eq. (B17) with Eq. (B16),

$$
\begin{aligned}
e_1^Z &= \frac{M}{2\pi} \int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi f_{\phi_\delta}^{(\phi_0)}(\phi) e_1^Z(\phi) \\
&= \frac{e_\delta \eta + p_d(1-\eta)}{\eta + 2p_d(1-\eta)},
\end{aligned}
\tag{B18}
$$

where

$$
e_\delta = \frac{\pi}{M} - \frac{M^2}{\pi^2} \sin^3\left(\frac{\pi}{M}\right)
\tag{B19}
$$

can be regarded as the misalignment error rate. Equation (B18) can be understood that, if a signal causes a click, the error rate is e_δ; and if a dark count causes a click, the error rate is $e_0 = 1/2$. Since the double-click events are discarded, when both a signal and a dark count cause clicks, the error rate is e_δ. Then, we can approximate e_k^Z with the same spirit, for the contributions in Y_k, given in Eq. (B13),

$$
e_k^Z \approx \frac{p_d(1-\eta)^k + e_\delta[1-(1-\eta)^k]}{Y_k}.
\tag{B20}
$$

Here, note that, in Eq. (B20), we ignore the double clicks caused by multiphoton signals, which would further reduce the misalignment error and, hence, the value of e_k^Z. The QBER $E_\mu^Z(\phi_\delta)$ for a given ϕ_δ is given by substituting Eq. (B9),

$$
\begin{aligned}
E_\mu^Z(\phi_\delta) &= \frac{P(\bar{L})P(R)}{P(\bar{L})P(R) + P(L)P(\bar{R})} \\
&= \frac{1}{Q_\mu}(1-p_d)\exp\left[-\eta\mu\cos^2\left(\frac{\phi_\delta}{2}\right)\right] \\
&\quad \times \left\{1-(1-p_d)\exp\left[-\eta\mu\sin^2\left(\frac{\phi_\delta}{2}\right)\right]\right\} \\
&= \frac{1}{Q_\mu}(1-p_d)\left\{\exp\left[-\eta\mu\cos^2\left(\frac{\phi_\delta}{2}\right)\right] - (1-p_d)e^{-\eta\mu}\right\} \\
&\approx \frac{e^{-\eta\mu}}{Q_\mu}\left[p_d + \eta\mu\sin^2\left(\frac{\phi_\delta}{2}\right)\right]
\end{aligned}
\tag{B21}
$$

similar to Eq. (B18),

$$
\begin{aligned}
E_\mu^Z &= \frac{M}{2\pi} \int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi f_{\phi_\delta}^{(\phi_0)}(\phi) E_\mu^Z(\phi_\delta) \\
&= \frac{(p_d + \eta\mu e_\delta)e^{-\eta\mu}}{Q_\mu},
\end{aligned}
\tag{B22}
$$

where e_δ is given in Eq. (B19). The results of Eqs. (B22) and (B18) are consistent with the one presented in the regular QKD model [44], as shown in Eqs. (B29) and (B30), with a slight difference. The difference is caused by how the double-click events are processed. In BB84, Alice

and Bob need to randomly assign a bit to double clicks, while in PM-QKD, double clicks are discarded.

Now, we can evaluate the key rate with the above model. Let us restate the key-rate formula, Eq. (A37),

$$
R_{\text{PM}} \geq \frac{2}{M} Q_\mu[1 - fH(E_\mu^Z) - H(E_\mu^X)],
\tag{B23}
$$

where the phase error rate is given by Eq. (A33),

$$
\begin{aligned}
E_\mu^X &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z), \\
&\leq q_0 e_0^Z + \sum_{k=0}^{\infty} e_{2k+1}^Z q_{2k+1} + (1 - q_0 - q_{\text{odd}}).
\end{aligned}
\tag{B24}
$$

In simulation, Q_μ and E_μ^Z are given by Eqs. (B14) and (B22). The fractions, $\{q_k\}$ with $k \geq 0$, of different photon components k contributing to the valid detections (L/R clicks) are given by

$$
q_k = \frac{P(k)Y_k}{Q_\mu} = e^{-\mu} \frac{\mu^k}{k!} \frac{Y_k}{Q_\mu}.
\tag{B25}
$$

For the odd-photon-number component, we have

$$
\begin{aligned}
q_{\text{odd}} &= \sum_{k=0}^{\infty} q_{2k+1} \\
&= \frac{1}{Q_\mu} \sum_{k=0}^{\infty} \frac{Y_{2k+1}\mu^{2k+1}e^{-\mu}}{(2k+1)!} \\
&= \frac{e^{-\mu}}{Q_\mu} \sum_{k=0}^{\infty} \left\{\frac{\mu^{2k+1}}{(2k+1)!} - (1-2p_d)\frac{[(1-\eta)\mu]^{2k+1}}{(2k+1)!}\right\} \\
&= \frac{e^{-\mu}}{Q_\mu} \{\sinh(\mu) - (1-2p_d)\sinh[(1-\eta)\mu]\}.
\end{aligned}
\tag{B26}
$$

To simplify the simulation, we explicitly calculate the e_k^Z and q_k for $0 \leq k \leq 5$. Further zooming into Eq. (B24), we have

$$
\begin{aligned}
E_\mu^X &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z), \\
&\leq q_0 e_0^Z + (q_1 e_1^Z + q_3 e_3^Z + q_5 e_5^Z) \\
&\quad + (1 - q_0 - q_1 - q_3 - q_5),
\end{aligned}
\tag{B27}
$$

where e_k^Z and q_k are given by Eqs. (B15) and (B25), respectively.

3. Simulation formulas for BB84 and MDI-QKD protocol and simulation parameters

We compare our derived key rate with that of the prepare-and-measure BB84 [1] protocol, whose key rate is given by the GLLP-decoy method [23].

The key rate of the decoy-state BB84 protocol is given by [25]

$$R_{BB84} = \frac{1}{2} Q_\mu \{-fH(E_\mu^Z) + q_1[1 - H(e_1^X)]\}, \quad (B28)$$

where $1/2$ is the basis sifting factor.

In the simulation, the yield and error rates of the k-photon component are given by [19]

$$Y_k = 1 - (1 - Y_0)(1 - \eta)^k,$$
$$e_k = e_d + \frac{(e_0 - e_d)Y_0}{Y_k}, \quad (B29)$$

where e_d is the intrinsic misalignment error rate caused by a phase reference mismatch. The gain and QBER are given by

$$Q_\mu = \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!} Y_k,$$
$$= 1 - (1 - Y_0)e^{-\eta\mu},$$
$$E_\mu = \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!} e_k Y_k,$$
$$= e_d + \frac{(e_0 - e_d)Y_0}{Q_\mu}, \quad (B30)$$

where $Y_0 = 2p_d$ and $e_0 = 1/2$.

The key rate of MDI-QKD is given by [15]

$$R_{MDI} = \frac{1}{2} \{Q_{11}[1 - H(e_{11})] - fQ_{rect}H(E_{rect})\}, \quad (B31)$$

where $Q_{11} = \mu_a \mu_b e^{-\mu_a - \mu_b} Y_{11}$, and $1/2$ is the basis sifting factor. We take this formula from Eq. (B27) in Ref. [18]. In simulation, the gain and error rates are given by

$$Y_{11} = (1 - p_d)^2 \left[\frac{\eta_a \eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a\eta_b)p_d \right.$$
$$\left. + 4(1 - \eta_a)(1 - \eta_b)p_d^2 \right],$$
$$e_{11} = e_0 Y_{11} - (e_0 - e_d)(1 - p_d^2)\frac{\eta_a \eta_b}{2},$$
$$Q_{rect} = Q_{rect}^{(C)} + Q_{rect}^{(E)},$$
$$Q_{rect}^{(C)} = 2(1 - p_d)^2 e^{-\mu'/2}[1 - (1 - p_d)e^{-\eta_a\mu_a/2}]$$
$$\times [1 - (1 - p_d)e^{-\eta_b\mu_b/2}],$$
$$Q_{rect}^{(E)} = 2p_d(1 - p_d)^2 e^{-\mu'/2}[I_0(2x) - (1 - p_d)e^{-\mu'/2}];$$
$$E_{rect}Q_{rect} = e_d Q_{rect}^{(C)} + (1 - e_d)Q_{rect}^{(E)}. \quad (B32)$$

Here,

$$\mu' = \eta_a\mu_a + \eta_b\mu_b,$$
$$x = \frac{1}{2}\sqrt{\eta_a\mu_a\eta_b\mu_b}, \quad (B33)$$

where μ' denotes the average number of photons reaching Eve's beam splitter, and $\mu_a = \mu_b = \mu/2$, $\eta_a = \eta_b = \eta$. We take these formulas from Eqs. (A9), (A11), (B7), and (B28)–(B31) in Ref. [18].

In 2014, Takeoka et al. derived an upper bound of the key rate of the point-to-point-type QKD protocols [10],

$$R_{TGW} = -\log_2\left(\frac{1 - \eta}{1 + \eta}\right). \quad (B34)$$

Later, Pirandola et al. established a tight upper bound [11],

$$R_{PLOB} = -\log_2(1 - \eta), \quad (B35)$$

which is the linear key-rate bound used in the main text. Note that Eq. (B35) is the secret key capacity of the pure loss channel, as it coincides with the lower bound previously known [45].

APPENDIX C: BEAM-SPLITTING ATTACK: INVALIDATION OF THE PHOTON NUMBER CHANNEL MODEL

Here, we argue that the tagging technique does not work for PM-QKD, by showing that the lower bound of the key rate from naively employing the tagging technique can be higher than an upper bound derived from a specific attack, in some parameter regime. The failure of the tagging technique stems from the failure of the photon number channel model used in the security proof [19]. In other words, the photon number channel model does not hold for the case when the random phases are announced during postprocessing.

1. Key rate with/without the photon number channel

Assuming the existence of the photon number channel model in PM-QKD, we can apply the tagging method and obtain a key-rate formula following the GLLP analysis [23,25],

$$r_{GLLP} = q_1[1 - H(e_1^X)] - fH(E_\mu^Z), \quad (C1)$$

where q_1 is the single-photon detection ratio, e_1^X and E_μ^Z are the single-photon phase error rate and total QBER, and f is the error correction efficiency.

As for comparison, our PM-QKD key-rate formula is given by Eq. (A15),

$$r_{PM} = 1 - H(E_\mu^Z) - H(E_\mu^X), \quad (C2)$$

where E_μ^X is bounded by Eq. (B27),

$$
\begin{aligned}
E_\mu^X &= \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z), \\
&\leq q_0 e_0^Z + (q_1 e_1^Z + q_3 e_3^Z + q_5 e_5^Z) \\
&\quad + (1 - q_0 - q_1 - q_3 - q_5).
\end{aligned}
\tag{C3}
$$

2. Beam-splitting attack

Now, we consider a beam-splitting attack, where Eve sets beam splitters with transmittance η on both Alice and Bob's side to simulate a lossy channel. She intercepts the pulses on A and B, regardless of the keys and bases of the pulses, and stores the reflected lights on her quantum memories, modes $A0$ and $B0$. Eve interferes the two transmitted pulses, modes $A1$ and $B1$, and announces the results. After Alice's and Bob's phase announcements, Eve performs an unambiguous state discrimination (USD) [46] on the states on modes $A0$ and $B0$ separately to guess the key information. Since the states on $A0(B0)$ and $A1(B1)$ are uncorrelated because of the beam splitting of coherent states, the beam-splitting attack will not introduce any error or other detectable effects. Apparently, this beam-splitting attack is an individual attack. We will calculate Eve's successful probability for guessing the key bits unambiguously, and calculate the mutual information $I(\kappa_{a(b)}:E)$, from which we can derive an upper bound on the secure key rate.

In PM-QKD, Alice and Bob prepare coherent states $\{|\sqrt{\mu_a}e^{i(\phi_a+\kappa_a)}\rangle_A$ and $|\sqrt{\mu_b}e^{i(\phi_b+\kappa_b)}\rangle_B\}$, where $\mu_a = \mu_b = \mu/2$, $\phi_a, \phi_b \in [0, 2\pi)$ are the random phases, and $\kappa_a, \kappa_b \in \{0, \pi\}$ are the key information. The states on system $A0$, $B0$ reflected by Eve's beam splitters are given by

$$
\begin{aligned}
|\sqrt{(1-\eta)\mu_a}e^{i(\phi_a+\kappa_a)}\rangle_{A0}, \\
|\sqrt{(1-\eta)\mu_b}e^{i(\phi_b+\kappa_b)}\rangle_{B0}.
\end{aligned}
\tag{C4}
$$

The two remaining pulses on the system $A1$, $B1$, used for interference, are given by

$$
\begin{aligned}
|\sqrt{\eta\mu_a}e^{i(\phi_a+\kappa_a)}\rangle_{A1}, \\
|\sqrt{\eta\mu_b}e^{i(\phi_b+\kappa_b)}\rangle_{B1}.
\end{aligned}
\tag{C5}
$$

Suppose Eve interferes systems $A1$ and $B1$; then the total gain Q_μ is given by

$$
Q_\mu = 1 - e^{-\eta\mu}.
\tag{C6}
$$

Here, we consider the signal with $\phi_a = \phi_b$, and Eve holds perfect single-photon detectors. Without loss of generality, we consider Eve's attack on system $A0$. If Eve cannot get the sifted phase information ϕ_a, then no matter the value of key phases κ_a, the state on $A0$ from Eve's perspective is

$$
\frac{1}{2\pi}\int_0^{2\pi} d\phi_a |\sqrt{(1-\eta)\mu_a}e^{i(\phi_a+\kappa_a)}\rangle_{A0}\langle\sqrt{(1-\eta)\mu_a}e^{i(\phi_a+\kappa_a)}|
$$

$$
= \sum_{k=0}^{\infty} P^{(1-\eta)\mu_a}(k)|k\rangle_{A0}\langle k|,
\tag{C7}
$$

where

$$
P^{(1-\eta)\mu_a}(k) = \frac{[(1-\eta)\mu_a]^k}{k!}e^{-(1-\eta)\mu_a}.
\tag{C8}
$$

In this case, Eve cannot obtain any information about κ_a. While in PM-QKD, the phase ϕ_a will be announced. In this case, Eve can first rotate the states on system $A0$ by $-\phi_a$. Now, the state becomes

$$
\begin{aligned}
\frac{1}{2}(&|\sqrt{(1-\eta)\mu_a}\rangle_{A0}\langle\sqrt{(1-\eta)\mu_a}| \\
&+ |-\sqrt{(1-\eta)\mu_a}\rangle_{A0}\langle-\sqrt{(1-\eta)\mu_a}|).
\end{aligned}
\tag{C9}
$$

Then, Eve only needs to determine whether the phase κ_a is 0 or π to obtain the key information. As shown in Ref. [46], if two pure states $|p\rangle$ and $|q\rangle$ are prepared with the same a priori $1/2$, the maximum probability of unambiguous discrimination is

$$
P_{\text{des}} = 1 - |\langle p|q\rangle|.
\tag{C10}
$$

Therefore, the probability of successfully distinguishing the states $|\sqrt{(1-\eta)\mu_a}\rangle$ and $|-\sqrt{(1-\eta)\mu_a}\rangle$ is given by

$$
P_{\text{suc}} = 1 - |\langle\sqrt{(1-\eta)\mu_a}|-\sqrt{(1-\eta)\mu_a}\rangle| = 1 - e^{-(1-\eta)\mu}.
\tag{C11}
$$

Note that Eve already know the value $\kappa_a - \kappa_b$ with interference results on $A1$, $B1$. Eve only needs to learn either of κ_a or κ_b. Thus, Eve's successful unambiguous measurement probability is

$$
P_{\text{BS}} = 1 - (1 - P_{\text{suc}})^2 = 1 - e^{-2(1-\eta)\mu}.
\tag{C12}
$$

If the light intensity μ is large enough, $P_{\text{BS}} = 1$, then Eve can learn the key information with a high probability.

With unambiguous state discrimination, the mutual information of Eve's measurement result (denoted by variable E) and Alice's and Bob's key $\kappa_{a(b)}$ is

$$
I(\kappa_{a(b)}:E) = P_{\text{BS}} = 1 - e^{-2(1-\eta)\mu}.
\tag{C13}
$$

Suppose that there is no extra error induced by other factors; then the beam-splitting attack provides an upper bound on the key rate,
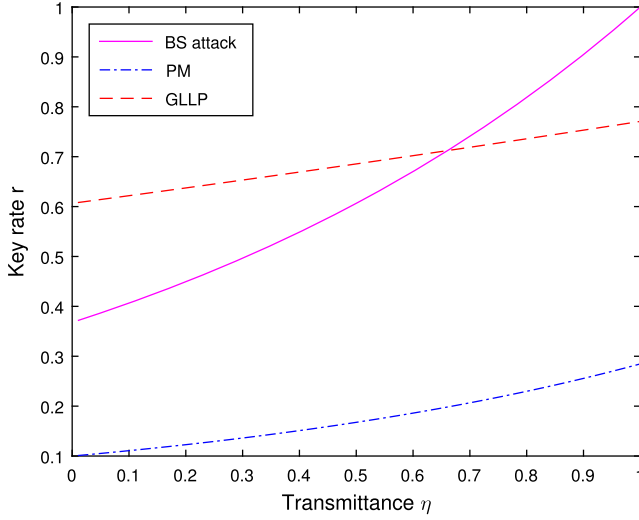
FIG. 8. Key-rate comparison with fixed light intensity $\mu = 0.5$. Here, we can see that the GLLP tagging formula for the single-photon component cannot hold under the beam-splitting attack when the transmittance $\eta < 0.6$.

$$r_{BS} = [1 - I(\kappa_{a(b)} : E)]$$
$$= e^{-2(1-\eta)\mu}$$
$$= \frac{e^{-2\mu}}{(1 - Q_\mu)^2}. \qquad (C14)$$

Here, the third equality is based on Eq. (C6).

3. Comparison

Now we make a simulation to compare the key rate in the following cases: with the "tagging" method, by our security proof, and the upper bound under the beam-splitting attack. In the discussion, we neglect the misalignment error and dark counts.

First, under the beam-splitting attack, the yield is given by

$$Y_k = 1 - (1 - \eta)^k, \qquad (C15)$$

and the fraction of the k-photon component is

$$q_k = \left(e^{-\mu} \frac{\mu^k}{k!} \right) \frac{Y_k}{Q_\mu} = [1 - (1 - \eta)^k] \frac{e^{-\mu} \mu^k}{k! Q_\mu}. \qquad (C16)$$

Note that $q_0 = 0$.

Second, in the beam-splitting attack scenario, Eve's operations will not introduce any error; hence,

$$e_k^Z = 0, \quad \forall \ k \geq 0,$$
$$E_\mu^Z = 0. \qquad (C17)$$

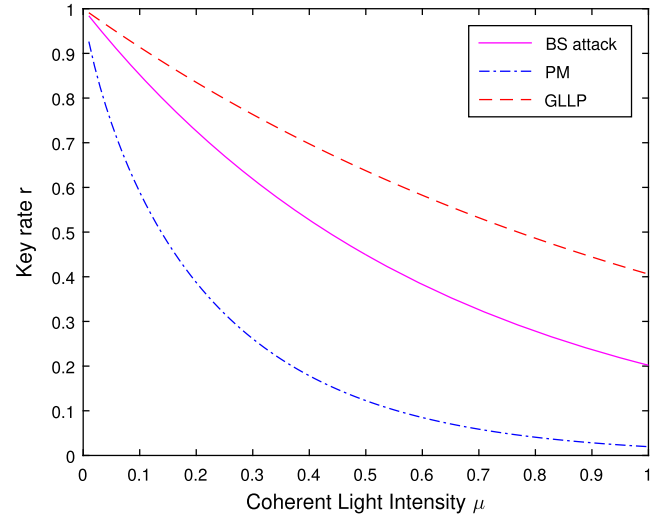Then Eqs. (C1), (A15), and (B27) can be simplified to

FIG. 9. Key-rate comparison with fixed transmittance $\eta = 0.2$. The GLLP tagging formula for the single-photon component cannot hold under the beam-splitting attack.

$$r_{GLLP} = q_1 = \eta\mu e^{-\mu},$$
$$r_{PM} = [1 - H(E^X)]$$
$$\geq [1 - H(1 - q_1 - q_3 - q_5)]. \qquad (C18)$$

We compare the key-rate formula r_{GLLP}, r_{PM} in Eq. (C18) with the key-rate upper bound by the beam-splitting attack r_{BS} in Eq. (C14). We set the total light intensity to be a typical value $\mu = 0.5$, and we adjust η to compare the key-rate performance. As shown in Fig. 8, the GLLP "tagging" formula for the "single-photon" component cannot hold under the beam-splitting attack for a transmittance $\eta < 0.6$. If we fix the transmittance $\eta = 0.2$ and adjust μ, Fig. 9 shows that the GLLP tagging formula cannot hold under the beam-splitting attack.

The beam-splitting attack results serve to invalidate the tagging method so that even the single-photon component cannot exist, since the announcement of phase ϕ_a, ϕ_b will leak more information of the key bits κ_a and κ_b.

Recently, Wang *et al.* proposed an eavesdropping strategy to the TF-QKD protocol [47]. The attack can also be performed against the PM-QKD protocol. Under such an attack, Eve can learn all the key bits. The key rate provided by the GLLP formula, Eq. (C1), is 0.5 (for all the clicked signals), while that given by our security proof is strictly 0. This also shows the invalidation of the GLLP key-rate formula, and our security proof is still valid under such an attack.

APPENDIX D: COMPARISON WITH OTHER PHASE-ENCODING MDI-QKD

Here, we compare three related phase-encoding MDI-QKD protocols, including the previous phase-encoding MDI-QKD (Scheme I in Ref. [17]), the recently proposed

TF-QKD [16], and our protocol (PM-QKD). For the simplicity of the statements, we assume that the phase reference of Alice and Bob is locked in all the protocols.

1. Phase-encoding MDI-QKD

In the phase encoding MDI-QKD (Scheme I in Ref. [17]), Alice generates two random bits κ_a, β_a as the key and the random choice of the X or Y basis, respectively, and then generates a coherent pulse $|\sqrt{\mu/2}e^{i(\pi\kappa_a+\pi\beta_a/2)}\rangle_A$. Similarly, Bob generates $|\sqrt{\mu/2}e^{i(\pi\kappa_b+\pi\beta_b/2)}\rangle_B$. They send their coherent pulses to Eve, who is supposed to perform an interference measurement and announce the detection results [Fig. 10(a)]. After Eve's announcement, Alice and Bob announce the basis information β_a, β_b and perform basis sifting.

Note that there is only single-photon detection in this protocol. Therefore, the number of clicked signals scales with $O(\sqrt{\eta})$, where η is the total transmittance between Alice and Bob. However, there is a considerable source flaw caused by using a coherent state as an approximation of an ideal single-photon state, resulting in a final key rate of $O(\eta)$.
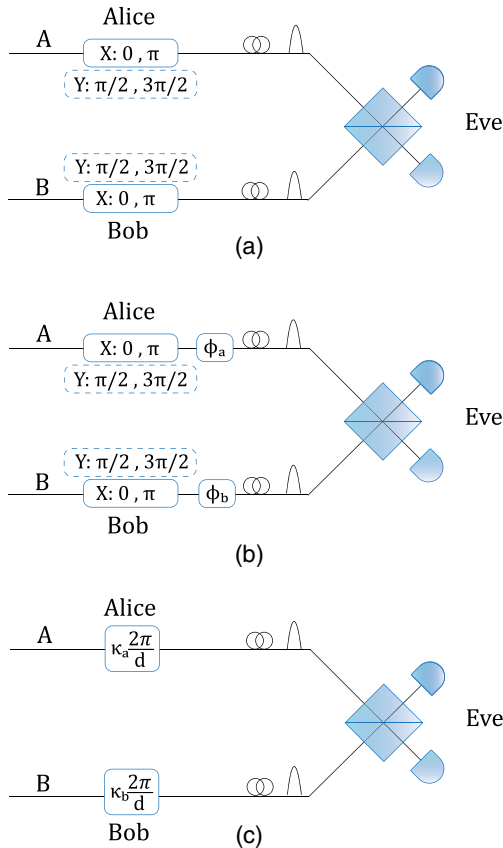

(a)

(b)

(c)

FIG. 10. (a) Schematic diagram of phase-encoding MDI-QKD (Scheme I in Ref. [17]). (b) Schematic diagram of TF-QKD, which is the decoy-state version of the scheme in (a). (c) Schematic diagram of d-phase PM-QKD.

2. TF-QKD

To avoid the performance deterioration caused by the source flaw in the phase-encoding MDI-QKD protocol above, a natural idea is to apply the decoy-state method [25], that is, to perform phase randomization, and to estimate the fraction of q_1 and the error rate e_1 of a single-photon component.

Recently, Lucamarini et al. modified the phase-encoding QKD protocol, namely, TF-QKD [16]. As shown in Fig. 10(b), Alice generates two random bits κ_a, β_a as the key, chooses randomly the X or Y basis, and modulates another random phase ϕ_a for the phase randomization in the decoy-state method. She generates a coherent pulse $|\sqrt{\mu/2}e^{i(\pi\kappa_a+\pi\beta_a/2+\phi_a)}\rangle_A$. Similarly, Bob generates a coherent pulse $|\sqrt{\mu/2}e^{i(\pi\kappa_b+\pi\beta_b/2+\phi_b)}\rangle_B$. They send their coherent pulses to Eve, who is supposed to perform the interference measurement and announce the detection results. After Eve's announcement, Alice and Bob announce β_a, β_b; ϕ_a, ϕ_b and perform basis sifting and phase sifting.

3. d-phase phase-matching QKD

In the d-phase PM-QKD, Alice first generates a random integer $\kappa_a \in \{0, 1, ..., d-1\}$ and then prepares a coherent pulse $|\sqrt{\mu/2}\exp[i\kappa_a(2\pi/d)]\rangle_A$. Similarly, Bob generates $\kappa_b \in \{0, 1, ..., d-1\}$ and prepares a similar state $|\sqrt{\mu/2}\exp[i\kappa_b(2\pi/d)]\rangle_B$. They send their coherent pulses to Eve, who is supposed to perform an interference measurement and announce the detection results. If Eve announces detector L/R clicks, Alice and Bob keep the numbers κ_a, κ_b and which detector clicks.

After many rounds of the steps above, Alice and Bob randomly select some of the data, announce them, and calculate the L/R detection probability for each case. By the estimated probabilities, they calculate the key rate and extract private keys.

As we can see, after Eve's announcement, Alice and Bob will share some mutual information. While Eve cannot fully learn the variable κ_a, the information-secure key can be generated between Alice and Bob.

The PM-QKD protocol in the main text and Appendix A corresponds to the case of $d = 2$, which is combined with a random phase announcement and the decoy-state method. In Appendix A, we completed the proof for the PM-QKD of $d = 2$ with a random phase announcement. The security proof for this generalized case is left for future work.

4. Comparison of different protocols

In all three protocols, phase-encoding MDI-QKD [17], TF-QKD [16], and PM-QKD, single-detection clicks on the untrusted node are used as successful measurement events, whose rate scales with $O(\sqrt{\eta})$. Technically, this is the reason why the key rate could have square-root scaling in

the first place [16]. Nevertheless, in the phase-encoding MDI scheme, without phase randomization, the single-photon source can be approximated by two weak coherent states, which decreases significantly the key rate of the protocol to $O(\eta)$. In TF-QKD, a single-qubit view is taken and a higher key rate is targeted. Unfortunately, the phase announcement invalidates the existence of the photon number channel model [19], and, hence, no enhancement can be claimed by directly applying the decoy-state method onto the phase-encoding MDI-QKD scheme.

Here, in the phase-matching QKD scheme, we switch from the qubit-based view to the optical-mode-based view. As shown above, our proposed phase-matching QKD follows the phase-encoding MDI-QKD scheme and the TF-QKD scheme, by modifying the encoding and basis choice. The name "phase-matching (MDI-)QKD" follows "phase-encoding MDI-QKD." We removed MDI (which is not the key point to our work) to make the name concise.

The PM-QKD protocol in the main text and Appendix A is the one with $d = 2$ and random phase announcement. Though the current practical implementations of phase-encoding MDI-QKD/TF-QKD and PM-QKD do resemble each other, the security scenarios are quite different. The TF-QKD can be taken as an extension of the BB84 protocol, which utilizes the single-photon source and is a discrete-variable QKD protocol. In the future, many discrete-variable QKD design techniques, such as a six-state protocol and reference-frame-independent protocol, can be employed in this framework. On the other hand, in PM-QKD, we focus more on the optical modes rather than single-photon states (qubits). It would be interesting to see whether the security proof techniques developed in continuous-variable QKD can be applied to PM-QKD.

5. Recent related works on TF-QKD

There are some recent works based on TF-QKD. Tamaki *et al.* provided a security proof of the TF-QKD protocol [48]. They modified the TF-QKD protocol by introducing a "test mode," where Alice and Bob do not announce the phase information and the photon-number-channel model holds. The original TF-QKD protocol is called "code mode." Following the original security proof of phase-encoding MDI-QKD [17], they estimated the phase error E_X by considering the imbalance of different bases. With a fair sampling argument on the test mode and the code mode, the basis imbalance in the code mode can be estimated by the one in the test mode. A square-root-scaling key rate has been derived, but it is significantly lower than ours. Note that there are still two bases in Tamaki *et al.*'s protocol and security proof, which follows the qubit-based view of BB84. The two-basis requirement in the security proof implies that it cannot be applied to our PM-QKD protocol directly, which also highlights the difference between the phase-encoding MDI-QKD/TF-QKD and PM-QKD.

Wang *et al.* proposed a "sending or not sending" TF-QKD protocol [49], which aims to utilize the Z-basis of single-photon for key generation, following the viewpoint of TF-QKD. However, the definition of the Z-basis encoding seems confusing. In the original TF-QKD protocol, the definitions of the X or Y bases refer to the ancillary bits rather than the real single photon. Also, the Z-basis encoding on the real photon does not correspond to a Z-basis encoding on the ancillary bits. This protocol needs further studies.

---

[1] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, 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, *Quantum Cryptography Based on Bell's Theorem*, Phys. Rev. Lett. **67**, 661 (1991).

[3] D. Mayers, *Unconditional Security in Quantum Cryptography*, J. Assoc. Comput. Mach. **48**, 351 (2001).

[4] H. K. Lo and H. F. Chau, *Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances*, Science **283**, 2050 (1999).

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

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptol. **5**, 3 (1992).

[7] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, *Satellite-to-Ground Quantum Key Distribution*, Nature (London) **549**, 43 (2017).

[8] In practice, single-photon sources are often replaced with weak coherent state sources or heralded single-photon sources. Nevertheless, only the single-photon components are used for secure key distribution.

[9] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Entanglement as a Precondition for Secure Quantum Key Distribution*, Phys. Rev. Lett. **92**, 217903 (2004).

[10] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental Rate-Loss Tradeoff for Optical Quantum Key Distribution*, Nat. Commun. **5**, 5235 (2014).

[11] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental Limits of Repeaterless Quantum Communications*, Nat. Commun. **8**, 15043 (2017).

[12] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *"Event-Ready-Detectors" Bell Experiment via Entanglement Swapping*, Phys. Rev. Lett. **71**, 4287 (1993).

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication*, Phys. Rev. Lett. **81**, 5932 (1998).

[14] K. Azuma, K. Tamaki, and H.-K. Lo, *All-Photonic Quantum Repeaters*, Nat. Commun. **6**, 6787 (2015).

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

[16] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters*, Nature (London) **557,** 400 (2018).

[17] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, *Phase Encoding Schemes for Measurement-Device-Independent Quantum Key Distribution with Basis-Dependent Flaw*, Phys. Rev. A **85,** 042307 (2012).

[18] X. Ma and M. Razavi, *Alternative Schemes for Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. A **86,** 062319 (2012).

[19] X. Ma, *Quantum Cryptography: From Theory to Practice*, Ph.D. thesis, University of Toronto, 2008.

[20] C. H. Bennett, *Quantum Cryptography Using Any Two Nonorthogonal States*, Phys. Rev. Lett. **68,** 3121 (1992).

[21] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, *Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution*, Phys. Rev. Lett. **114,** 180502 (2015).

[22] A. Ferenczi, *Security Proof Methods for Quantum Key Distribution Protocols* (UWSpace, Waterloo, 2013)

[23] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, *Security of Quantum Key Distribution with Imperfect Devices*, Quantum Inf. Comput. **4,** 325 (2004).

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

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

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

[27] C. C. W. Lim, B. Korzh, A. Martin, F. Bussieres, R. Thew, and H. Zbinden, *Detector-Device-Independent Quantum Key Distribution*, Appl. Phys. Lett. **105,** 221112 (2014).

[28] P. González, L. Rebón, T. F. da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, *Quantum Key Distribution with Untrusted Detectors*, Phys. Rev. A **92,** 022337 (2015).

[29] G. Santarelli, A. Clairon, S. N. Lea, and G. M. Tino, *Heterodyne Optical Phase-Locking of Extended-Cavity Semiconductor Lasers at 9 GHz*, Opt. Commun. **104,** 339 (1994).

[30] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, *Experimental Study on the Gaussian-Modulated Coherent-State Quantum Key Distribution over Standard Telecommunication Fibers*, Phys. Rev. A **76,** 052323 (2007).

[31] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, *Generating the Local Oscillator "Locally" in Continuous-Variable Quantum Key Distribution Based on Coherent Detection*, Phys. Rev. X **5,** 041009 (2015).

[32] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, *Self-Referenced Continuous-Variable Quantum Key Distribution Protocol*, Phys. Rev. X **5,** 041010 (2015).

[33] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, *Discrete-Phase-Randomized Coherent State Source and Its Application in Quantum Key Distribution*, New J. Phys. **17,** 053014 (2015).

[34] S. Droste, F. Ozimek, Th. Udem, K. Predehl, T. W. Hänsch, H. Schnatz, G. Grosche, and R. Holzwarth, *Optical-Frequency Transfer over a Single-Span 1840 km Fiber Link*, Phys. Rev. Lett. **111,** 110801 (2013).

[35] G. Carvacho, J. Cariñe, G. Saavedra, Á. Cuevas, J. Fuenzalida, F. Toledo, M. Figueroa, A. Cabello, J.-Å. Larsson, P. Mataloni, G. Lima, and G. B. Xavier, *Postselection-Loophole-Free Bell Test over an Installed Optical Fiber Network*, Phys. Rev. Lett. **115,** 030503 (2015).

[36] M. Lipka, M. Parniak, and W. Wasilewski, *Optical Frequency Locked Loop for Long-Term Stabilization of Broad-Line DFB Laser Frequency Difference*, Appl. Phys. B **123,** 238 (2017).

[37] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, *Measurement-Device-Independent Quantum Key Distribution over 200 km*, Phys. Rev. Lett. **113,** 190501 (2014).

[38] S. Pirandola, *Capacities of Repeater-Assisted Quantum Communications*, arXiv:1601.00966.

[39] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, *Mixed-State Entanglement and Quantum Error Correction*, Phys. Rev. A **54,** 3824 (1996).

[40] M. Ben-Or, D. W. Leung, D. Mayers, and J. Oppenheim, *The Universal Composable Security of Quantum Key Distribution*, in *International Conference on Theory of Cryptography* (Springer, Berlin, Heidelberg, 2005), pp. 386–406.

[41] R. Renner and R. König, *Universally Composable Privacy Amplification against Quantum Adversaries*, in *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10–12, 2005. Proceedings*, edited by Joe Kilian (Springer, Berlin, Heidelberg, 2005), pp. 407–425.

[42] A. R. Calderbank and P. W. Shor, *Good Quantum Error-Correcting Codes Exist*, Phys. Rev. A **54,** 1098 (1996).

[43] J. Minář, H. De Riedmatten, C. Simon, H. Zbinden, and N. Gisin, *Phase-Noise Measurements in Long-Fiber Interferometers for Quantum-Repeater Applications*, Phys. Rev. A **77,** 052325 (2008).

[44] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Practical Decoy State for Quantum Key Distribution*, Phys. Rev. A **72,** 012326 (2005).

[45] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, *Direct and Reverse Secret-Key Capacities of a Quantum Channel*, Phys. Rev. Lett. **102,** 050503 (2009).

[46] G. Jaeger and A. Shimony, *Optimal Distinction between Two Non-orthogonal Quantum States*, Phys. Lett. A **197,** 83 (1995).

[47] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, *Effective Eavesdropping to Twin-Field Quantum Key Distribution*, arXiv:1805.02272v1.

[48] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, *Information Theoretic Security of Quantum Key Distribution Overcoming the Repeaterless Secret Key Capacity Bound*, arXiv:1805.05511.

[49] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, *Sending or Not Sending: Twin-Field Quantum Key Distribution with Large Misalignment Error*, arXiv:1805.09222.