


# Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound Over a Noisy Channel

Pei Zeng<sup>1</sup>, Weijie Wu, and Xiongfeng Ma<sup>1\*</sup>

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

 (Received 25 September 2019; revised manuscript received 20 March 2020; accepted 28 April 2020; published 4 June 2020)

There are two main factors limiting the performance of quantum key distribution—channel transmission loss and noise. Previously, a linear bound was believed to put an upper limit on the rate-transmittance performance. Remarkably, the recently proposed twin-field and phase-matching quantum key distribution schemes have been proven to overcome the linear bound. In practice, due to the intractable phase fluctuation of optical signals in transmission, these schemes suffer from large error rates, which renders the experimental realization extremely challenging. Here, we close this gap by proving the security based on a different principle—encoding symmetry. With the symmetry-based security proof technique, we can decouple the privacy from the channel disturbance, and eventually remove the limitation of secure key distribution on bit error rates. As a direct application, we show that the phase-matching scheme can yield positive key rates even with high bit error rates up to 50%. In the simulation, with typical experimental parameters, the key rate is able to break the linear bound with an error rate of 13%. Meanwhile, we provide a simple finite-data size analysis for the phase-matching scheme under this symmetry-based analysis, which can break the bound with a reasonable data size of  $10^{12}$ . Encouraged by high loss and error tolerance, we expect the approach based on symmetry-protected privacy will provide a different insight into the security of quantum key distribution.

DOI: [10.1103/PhysRevApplied.13.064013](https://doi.org/10.1103/PhysRevApplied.13.064013)

## I. INTRODUCTION

Quantum key distribution (QKD) offers information theoretically secure means to distribute private keys between distant parties by harnessing the laws of quantum mechanics [1,2]. The commercialization and application of QKD raise requirements in both impregnable security and outstanding performance. For a review of the subject, see the recent review article [3] and references therein.

The security, as the cornerstone of QKD, has been proven theoretically at the end of the last century [4–6] on the protocol level, while rigorous definition [7,8] and strict finite-size analysis [9,10] have been provided later. The security of QKD is based on the idea that information gain means disturbance. That is, an eavesdropper's attempt of learning the keys would inevitably introduce disturbance to the quantum states. To characterize the information leakage, the disturbance in the channel is monitored in real time. In practice, the physical devices used in practical implementations often deviate from the assumed theoretical models [11], resulting in various loopholes and corresponding attacks [12,13]. In 2012, measurement-device-independent quantum key distribution (MDI QKD) has been presented [14], which removes the theoretical

assumptions on measurement devices in security analysis and hence closes all the detection loopholes.

The performance of QKD, on the other hand, characterized by the key generation rate with respect to the communication distance, reflects its value in commercial cryptographic tasks. Under the circumstances that quantum repeaters [15–17], as the ultimate solution to extend quantum communication against losses, are currently infeasible, the linear key-rate-transmittance bound [18] was widely believed to hold for all the point-to-point QKD schemes without repeaters. For the commonly used telecom fiber channel, the transmittance decreases exponentially with the transmission distance, which puts an upper limit on quantum transmission distance. Interestingly, a recent work named twin-field QKD shows the possibility of phase-encoding MDI QKD protocol to break the linear key-rate bound [19]. A follow-up work, named phase-matching quantum key distribution (PM QKD) has been proposed [20,21], which has been rigorously shown to be able to beat the linear bound even with statistical fluctuations [22]. The twin-field-like MDI QKD is currently a heated topic [23–26].

In PM QKD, only one basis is adopted for key generation and parameter estimation, which is distinct from the former BB84-type protocol while sharing some similarities with the Bennett-1992 protocol [27]. Essentially, the PM

\*xma@tsinghua.edu.cn

QKD protocol can be viewed as an MDI version of the Bennett-1992 protocol [28]. To understand the security of PM QKD, we would resort to the nonorthogonality of the encoded state with  $0/\pi$  encoding. However, the analysis based on nonorthogonality usually cannot tolerate high channel losses.

In this work, for a generic MDI QKD model, we establish a connection between the encoding symmetry and privacy, which serves as a perspective of QKD security different from the conventional basis complementarity [29]. In this symmetry-based security proof, we first define symmetric states given certain encoding operations, then explore the realistic construction of symmetric states, and finally propose efficient methods to estimate the ratio of detection caused by symmetric states. For this generalized MDI QKD framework, the symmetric state can promise perfect privacy, i.e., with no information leakage. As a result, the amount of information leakage only depends on the state produced by the source and is irrelevant to the channel condition. A similar phenomenon is also observed in the round-robin differential-phase-shifting protocol [30]. The symmetry-based security proof allows higher error tolerance compared with the original BB84 protocol. Furthermore, we complete the finite-size analysis with an improved decoy-state method [31–33].

## II. ENCODING SYMMETRY AND PERFECT PRIVACY

To show the close relationship between encoding symmetry and privacy, we introduce a generalized MDI QKD framework. As is shown in Fig. 1, during each run, Alice and Bob start with a preshared bipartite state  $\rho_{AB}$ , where the systems held by Alice and Bob are denoted as  $A$  and  $B$ , respectively. They generate random bits  $\kappa_a$  and  $\kappa_b$  independently and apply  $U[\kappa_{a(b)}] \equiv U^{\kappa_{a(b)}}$  to their subsystem  $A$  and  $B$  separately, where  $U^2 = I$ . Then, the modulated state, denoted as  $\rho'_{AB}(\kappa_a, \kappa_b)$ , is sent to an untrusted party

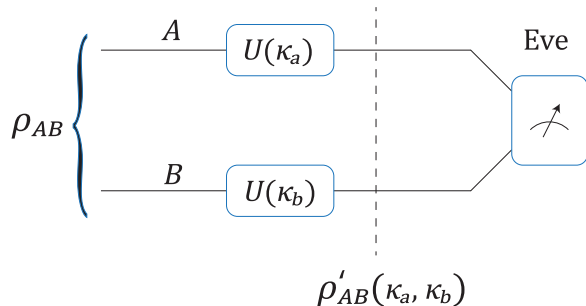


FIG. 1. Schematic diagram of a generalized discrete-variable MDI QKD framework. Here we make no assumption on Alice’s and Bob’s sources or their encoding unitary operations. The only assumption is the symmetric property of the encoding operation, i.e.,  $U^2 = I$ .

Eve, who measures the joint state, aiming to discriminate whether  $\kappa_a = \kappa_b$  or  $\kappa_a \neq \kappa_b$ , and announces the detection result. In each round, Alice and Bob encode two-bit information,  $\kappa_a, \kappa_b$ , into the state  $\rho_{AB}$ . The encoded state  $\rho'_{AB}(\kappa_a, \kappa_b)$  can be written as

$$\rho'_{AB}(\kappa_a, \kappa_b) = [U_A(\kappa_a) \otimes U_B(\kappa_b)]\rho_{AB}[U_A(\kappa_a) \otimes U_B(\kappa_b)]^\dagger. \quad (1)$$

After many rounds, Alice and Bob generate random bit strings  $K_a$  and  $K_b$ , respectively. With the assistance of Eve’s announcement and classical error correction, Bob reconciles his bit string  $K_b$  to  $K_a$ . They then perform privacy amplification on  $K_a$  to extract a private key.

Note that, we do not make any restriction on the dimension of the system  $A$  and  $B$  and the exact form of encoding operation  $U$ . The only reasonable assumption made on the source is that the encoding operation should be closed, i.e.,  $U^2 = I$ . We believe such a MDI QKD framework is able to cover a wide range of discrete-variable MDI QKD protocols.

Now, let us focus on a symmetric case, where the preshared state  $\rho_{AB}$  remains invariant under the transformation of encoding operation  $U_A \otimes U_B$ . That is, a pure state  $|\psi\rangle_{AB}$  is invariant under the encoding operation if

$$|\psi\rangle_{AB} = U_A \otimes U_B |\psi\rangle_{AB}. \quad (2)$$

Then,  $|\psi\rangle_{AB}$  is an eigenstate of  $U_A \otimes U_B$ . Since  $(U_A \otimes U_B)^2 = I$ , the eigenvalue of  $U_A \otimes U_B$  is either  $+1$  or  $-1$ . We name the eigenvalue  $+1$  subspace of  $U_A \otimes U_B$  as the even space  $\mathcal{H}^{\text{even}}$  and the eigenvalue  $-1$  subspace as the odd space  $\mathcal{H}^{\text{odd}}$ . The states lie in  $\mathcal{H}^{\text{even}}$  are called even states and the states lie in  $\mathcal{H}^{\text{odd}}$  are called odd states. Together they are called parity states. Obviously, a mixture of odd (even) states is still an odd (even) state.

For a generic mixture of pure parity states,  $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ , where all the components  $\{|\psi_i\rangle\}$  are parity states, it remains invariant under  $U_A \otimes U_B$ ,

$$\begin{aligned} \rho'_{AB}(0, 0) &= \rho'_{AB}(1, 1), \\ \rho'_{AB}(0, 1) &= \rho'_{AB}(1, 0). \end{aligned} \quad (3)$$

The raw key-bit information  $\kappa_a$  is “hidden” on the encoded state  $\rho'_{AB}(\kappa_a, \kappa_b)$ . However, when Eve holds the purification of  $\rho_{AB}$ , she may still learn  $\kappa_a$  from the encoded state. Without loss of generality, we consider a purification of  $\rho_{AB}$ ,  $|\Psi\rangle_{ABC} = \sum_i \sqrt{p_i} |\psi_i\rangle_{AB} |i\rangle_C$ , where system  $C$  is held by Eve. Under the encoding operation  $U_A \otimes U_B$ , all the odd and even state components of  $\{|\psi_i\rangle\}$  will gain a factor  $-1$  and  $1$ , respectively. If there are only odd or even components in  $\rho_{AB}$ , the purified state  $|\Psi\rangle_{ABC}$  will keep unchanged under the encoding operation. On the other hand, the coexistence of odd and even components in  $\rho_{AB}$  will lead to

a change of relative phase in  $|\Psi\rangle_{ABC}$ , allowing Eve to discriminate  $\rho'_{AB}(0,0)$  and  $\rho'_{AB}(1,1)$ .

To make the observations above rigorous, in Appendix A, we analyze the security of QKD with symmetric encoding by employing a standard phase-error-correction approach [5,6,29]. When the input state  $\rho_{AB}$  is an (even or odd) parity state, the symmetric encoding shown in Fig. 1, provides perfect privacy, which is reflected as a zero phase-error rate,  $E^{(\text{ph})} = 0$ . Note that a similar result has been derived in a coherent-state-based twin-field QKD work using a different approach [34].

**Theorem 1.** *In the protocol shown in Fig. 1, if Alice and Bob share an (even or odd) parity state  $\rho_{AB}$  at the beginning of each run, then Eve has no information on Alice's (or Bob's) encoded key bit  $\kappa_a$  (or  $\kappa_b$ ), i.e., perfect privacy.*

To generalize the discussion, when Alice and Bob's preshared state  $\rho_{AB}$  is a mixture of even and odd state,

$$\rho_{AB} = p_{\text{odd}}\rho_{\text{odd}} + p_{\text{even}}\rho_{\text{even}}, \quad (4)$$

then by applying Theorem 1, we can estimate the ratios of odd and even components causing effective detection,

$$\begin{aligned} q_{\text{odd}} &= p_{\text{odd}} \frac{Y_{\text{odd}}}{Q}, \\ q_{\text{even}} &= p_{\text{even}} \frac{Y_{\text{even}}}{Q}, \end{aligned} \quad (5)$$

where  $Y_{\text{odd}}$ ,  $Y_{\text{even}}$ , and  $Q$  are the successful detection probability of  $\rho_{\text{odd}}$ ,  $\rho_{\text{even}}$ , and  $\rho_{AB}$ , respectively. The phase-error rate is  $E^{(\text{ph})} = q_{\text{even}}$ . Therefore, the key rate is given by

$$r = 1 - H(E) - H(q_{\text{even}}), \quad (6)$$

where  $E$  is the quantum bit error rate. Here, we can see that as long as the final state postselected by successful detection is close to a parity state (either even or odd), the information leakage can be bounded.

### III. IMPROVED ANALYSIS OF PHASE-MATCHING QUANTUM KEY DISTRIBUTION

The problem for implementing symmetric encoding is that both the parity states  $\rho_{\text{odd}}$  and  $\rho_{\text{even}}$  are usually nonlocal. That is, they cannot be obtained by Alice and Bob via independent local state preparation. Thus, they will inevitably prepare a mixture of even and odd parity states in practice. The PM QKD protocol can be regarded as a special realization of symmetric encoding, where Alice and Bob construct the parity state-input  $\rho_{AB}$  using two optical modes based on independent laser sources. To construct parity state  $\rho_{AB}$  from experimentally accessible coherent

states, a natural way is to perform simultaneous  $0/\pi$  phase randomization on two coherent states  $|\sqrt{\mu_a}\rangle_A, |\sqrt{\mu_b}\rangle_B$  to decouple the odd and even photon components.

For the convenience of parameter estimation, we consider the PM QKD protocol where Alice and Bob randomize the phase  $\phi$  on  $|\sqrt{\mu_a}e^{i\phi}\rangle_A, |\sqrt{\mu_b}e^{i\phi}\rangle_B$  continuously so that the photon-number components  $\{|m, n\rangle\}_{m+n=k}$  are decoupled,

$$\rho_{AB} = \sum_{k=0}^{\infty} p_k \rho_k, \quad (7)$$

where  $\rho_k$  a pure parity state since it is a Fock state. The overall phase error of PM QKD is given by

$$q_{\text{even}} = 1 - \sum_k q_{2k+1}, \quad (8)$$

where  $q_k$  is the fraction of detection when Alice and Bob send out  $k$ -photon signals,

$$q_k = P_{\mu_t}(k) \frac{Y_k}{Q_{\mu_t}}. \quad (9)$$

Here  $\mu_t = \mu_a + \mu_b$ ;  $Y_k$  is the yield of  $k$ -photon component;  $Q_{\mu_t}$  is the overall gain, i.e., the successful detection probability when Alice and Bob send out coherent lights with intensities of  $\mu_a$  and  $\mu_b$ , respectively; and  $P_{\mu_t}(k) = e^{-2\mu} (2\mu)^k / (k!)$  is the Poisson distribution. In order to estimate the information leakage, we only need to estimate the fraction of odd-state detections.

The simultaneous phase randomization is also nonlocal. To achieve this in practice, Alice and Bob first randomize the phase independently, and then postselect the pulses with the same random phase by phase announcement and sifting [35]. The overall privacy, characterized by the overall phase-error rate, will not change after the random-phase announcement [20,22], which indicates that simultaneous phase randomization can be replaced by independent phase randomization and postselection.

In each turn, Alice and Bob each generate a random phase  $\phi_{a(b)}$  and a random key bit  $\kappa_{a(b)}$ . They then modulate their coherent pulse  $|\sqrt{\mu_{a(b)}}\rangle$  by a phase  $[\phi_{a(b)} + \pi\kappa_{a(b)}]$ . After Eve announces the detection result, they announce the random phases  $\phi_{a(b)}$  to group the signals with the same random-phase difference. From the detection result, they estimate the information leakage and extract the keys from the encoding bits. In practice, the continuous phase randomization can be replaced with discrete randomization [36]. The detailed analysis of PM QKD with phase postselection and discrete phase randomization is presented in Appendix B.

In discrete-phase encoding, Alice and Bob randomly pick up one of the  $D$  phases equally distributed in  $[0, 2\pi)$ . They announce the discrete random phase  $\phi_a =$

$(2\pi/D)j_a$  and  $\phi_b = (2\pi/D)j_b$  with the indexes  $j_{a(b)} = 0, 1, \dots, D-1$ . Based on the random-phase difference, they group the signals by  $j_s = (j_b - j_a) \bmod (D/2)$ . For example, when  $D = 16$ , the signals with  $j_b - j_a = 1$  and 9 are in the same group. After grouping, there is  $D/2$  groups with the label of  $j_s = 0, 1, \dots, D/2 - 1$ . In the ideal case, the signals with  $j_s = 0$  are the signals with matched phase. For the signals with  $j_s \neq 0$ , there is an intrinsic mismatched phase  $\phi_\delta$ . It is conservative to regard  $\phi_\delta$  being caused by Eve in security analysis. For each group of data, the information leakage can be bounded by  $q_{\text{even}}$  in Eq. (8), regardless of Eve's measurement setting or the bit error rates.

Thanks to this decoupled relationship between privacy and channel disturbance, we can improve the postprocessing step by utilizing the unaligned data with  $j_s \neq 0$ . Alice and Bob first reconcile their sifted raw key bits  $K_a$  and  $K_b$  for each group  $j_s$  separately. If the error rate in a group of data is too large, they can simply discard that group. Denote the group set  $J$  to be the set of remaining phase-group indexes  $\{j_s\}$ . That is, if  $j_s \in J$ , then the phase group  $j_s$  is kept for key generation. They then estimate the even photon fraction  $q_{\text{even}}$  for all the remaining data and perform privacy amplification. Note that  $q_{\text{even}}$  is the same for different data group  $j_s$ . The overall key rate of PM QKD, taking the phase sifting and loss into account, is given by

$$R = \frac{2Q_\mu}{D} \sum_{j_s \in J} [1 - H(q_{\text{even}}) - fH(E_{j_s})], \quad (10)$$

where  $f$  is the error-correction efficiency, and  $E_{j_s}$  is the bit error rate of phase group  $j_s$  with  $\mu_{i_a} = \mu_{i_b} = \mu/2$ . In the experiment, all the parameters in Eq. (10) can be directly obtained except for  $q_{\text{even}}$ , which needs to be bounded by the decoy-state method. It has been shown in the literature that with the infinite decoy-state method [32], all the parameters, including  $q_{\text{even}}$  can be estimated accurately [20,21].

#### IV. ROBUSTNESS TO LOSS AND NOISE

To test the capability to tolerate high noises, we simulate the performance of PM QKD in the asymptotic limit, under a different level of misalignment errors, with  $D = 16$  discrete phases. In the simulation model, there are three major error sources: the system misalignment error  $e_d$ , caused by phase fluctuation and system misalignment; the background error, caused by dark counts  $p_d$ ; and the mismatch error  $e_\Delta(j_s)$  caused by the intrinsic mismatch for different phase groups,

$$e_\Delta(j_s) = \begin{cases} \sin^2\left(\frac{\pi j_s}{D}\right), & 0 \leq j_s \leq \frac{D}{4}, \\ \sin^2\left(\frac{\pi}{2} - \frac{\pi j_s}{D}\right), & \frac{D}{4} < j_s \leq \frac{D}{2} - 1, \end{cases} \quad (11)$$

which is related to the index deviation  $0 \leq j_s \leq D/2 - 1$ . The overall bit error rate  $E_\mu^{(j_s)}$  is then given by

$$E_\mu^{(j_s)} = \min\left(\{p_d + \eta\mu[e_\Delta(j_s) + e_d]\} \frac{e^{-\eta\mu}}{Q_\mu}, 0.5\right), \quad (12)$$

where  $\eta$  is the transmittance.

In practice, the phase drift caused by lasers and fiber links will degrade the performance of PM QKD. To avoid the effect caused by phase drift, one demanding way is to introduce active feedback and phase locking. Another enhancement is to introduce the phase postcompensation method [20], where Alice and Bob can estimate the phase drift  $\phi_\delta$  by strong light pulses, record it, and take it into account in the sifting step. Suppose the phase drift is slow, then Alice and Bob are able to figure out the closest discrete phase  $\phi_j \equiv (2\pi/D)j$  to  $\phi_\delta$ . Denote the index of the closest discrete phase as  $j_\delta$ . During the sifting step, Alice and Bob modify the definition of  $j_s$  to  $j_s = j_a - j_b - j_\delta$ . In this sense, Alice and Bob “postcompensate” the effect caused by phase drift.

With the parameters given in Table I, we simulate the asymptotic key-rate performance under the setting of system misalignment error rates  $e_d$  of 1, 5, 9, and 13%. Note that the normal symmetric BB84 protocol cannot yield any positive key rate under the misalignment error  $e_d \geq 11\%$ . From Fig. 2, one can see, even if  $e_d = 13\%$ , the key rate of PM QKD is still able to surpasses the linear bound when  $l > 330$  km. This illustrates the robustness of PM QKD against both noisy and lossy channels. In an extreme case when the source-light intensity  $\mu \rightarrow 0$  and the dark count of the detector  $p_d = 0$ , the single photon fraction among all the detected signal  $q_1 \rightarrow 1$  according to Eq. (9), hence the phase-error rate  $E^{(\text{ph})} \rightarrow 0$ . In this case, the key rate of PM QKD is positive even when the bit error  $E_\mu^{(j_s)}$  is close to 50%. In Appendix D, we compare our analysis to the one in the literature [20] and demonstrate its advantage when  $e_d$  gets larger.

TABLE I. List of parameters for the simulations shown in Figs. 2 and 3. The failure probability  $\epsilon$  and sending rounds  $N$  is used for the finite data-size analysis in Fig. 3.

Parameters	Values
Dark count rate $p_d$	$1 \times 10^{-8}$
Error-correction efficiency $f$	1.1
Detector efficiency $\eta_d$	20%
Number of phase slices $D$	16
BB84 misalignment error $e_d^{(\text{BB84})}$	1.5%
Failure probability $\epsilon$	$1.7 \times 10^{-10}$
Sending rounds $N$	$1 \times 10^{12}$ or $1 \times 10^{13}$



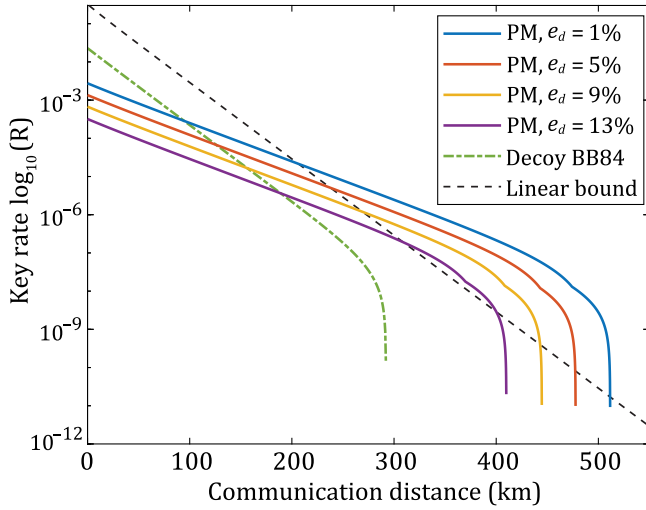


FIG. 2. Rate-distance performance of PM QKD under different system misalignment error rates  $e_d$ . For BB84,  $e_d = 1.5\%$ . The nonsmooth point indicates the places where the key contribution from unaligned groups with  $j_s \neq 0$  turns to 0.

## V. FINITE-SIZE PERFORMANCE

With the symmetry-based security proof of PM QKD, the finite-size analysis can be considerably simplified. In a complete finite-size analysis, we should take the cost and failure probability of channel authentication, error verification, privacy amplification, and parameter estimation into account. However, the cost of the first three steps is negligible comparing to the one in parameter estimation. When the final key length is much larger than 37 bits, we can ignore the corresponding failure probability with a constant secret-key cost [10]. For simplicity, we ignore these parts in our analysis. The phase-error estimation is at the core of the finite-size analysis. According to Eqs. (8) and (9), our task is to estimate the number of clicks caused by odd-photon fraction in the phase groups  $J$ , with signal intensity  $\mu_a = \mu_b = \mu/2$ . The Chernoff bound is applied to estimate the statistical fluctuation of decoy parameters [37]. We leave the details of the finite decoy-state analysis in Appendix C.

To demonstrate the practicality of PM QKD, we perform a simulation with finite data sizes, as shown in Fig. 3. The key rate beat the linear bound at 270 km under the condition where data size  $N = 1 \times 10^{12}$  and system misalignment error  $e_d = 3\%$ . When the system misalignment error is 6%, which can be easily realized in current experimental implementation, the linear bound is exceeded at a similar length of 270 km, where, as an expense, the data size should be enlarged into  $N = 1 \times 10^{13}$ . Note that in the decoy analysis, the rounds with mismatched phases are also used for parameter estimation, which is substantiated by the fact that the single-photon state is  $\rho^1 = \frac{1}{2}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|)$ , regardless of

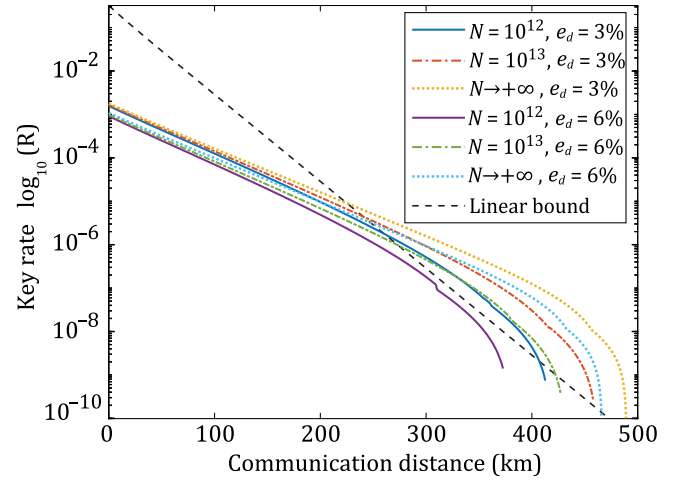


FIG. 3. Rate-distance performance of PM QKD under the data size  $N = 1 \times 10^{12}$ ,  $1 \times 10^{13}$  or infinitely large, and misaligned error  $e_d = 3$  or 6%.

the sending intensity and random-phase difference. With this observation, the size of available data for parameter estimation is enlarged, which marginally reduces the impact of statistical fluctuation and results in a higher key rate.

## VI. DISCUSSION

We analyze the security of a generalized MDI QKD framework, from which we provide a perspective where the QKD security originates from the encoding symmetry. As an example, we show that the parity symmetry in the encoded states provides the privacy of PM QKD. In the same manner, here we conjecture that the translation symmetry of encoded state in the round-robin differential-phase-shifting protocol may explain why the information leakage will not be affected by the channel noise, and leave it for future works.

The symmetry-protected quality not only makes PM QKD robust against channel disturbance but also simplifies the parameter estimation and finite-size analysis considerably. With improved decoy-state analysis, we demonstrate the capability of PM QKD to surpass the linear bound with data size  $N = 1 \times 10^{13}$ , currently accessible experimental devices, and a high noise level of 6%. Note that, the discrete phase randomization with  $\{\phi = 2\pi(j/D)\}_{j=0}^{D-1}$  and Alice and Bob's imbalanced signal intensity  $\mu_a, \mu_b$  will not destroy the parity-symmetry essentially. This implies a natural extension of PM QKD analysis to the cases with few discrete random phases and the imbalanced intensity arrangement of Alice and Bob.

Due to the universality of encoding symmetry and the existence of symmetric states, we expect this symmetry-based analysis will benefit the security proof of a large variety of QKD protocols. For example, the analysis of

encoding operation with parity symmetry  $U^2 = I$  in this work can be extended to the  $n$ -fold rotational symmetry case, i.e.,  $U^n = I$ , where  $n \geq 2$ . Note that, our analysis is irrelevant to the exact form of the source and measurement device. Therefore, this symmetry-based analysis can be extended to the case where the security proof is not obvious in a usual complementarity-based security view, for example, the continuous-variable QKD protocol, where the measurement is performed by homodyne detection on optical modes.

## ACKNOWLEDGMENTS

We acknowledge M. Koashi, N. Lütkenhaus, and H. Zhou for the insightful discussions. This work is supported by the National Natural Science Foundation of China Grants No. 11875173 and No. 11674193, the National Key R&D Program of China Grants No. 2017YFA0303900 and No. 2017YFA0304004, and the Zhongguancun Haihua Institute for Frontier Information Technology.

P.Z. and W.W. contribute equally to this work.

## APPENDIX A: PROOF OF SYMMETRY-PROTECTED PRIVACY

In this section, we provide security analysis of symmetric encoding QKD. We first review the security proof based on phase-error correction [5,6]. Then, we present a general entanglement-based symmetric encoding protocol by establishing the link between symmetric states and perfect privacy.

Denote  $\mathcal{D}(\mathcal{H}^A)$  as the space of density operators acting on  $\mathcal{H}^A$  and  $\mathcal{L}(\mathcal{H}^A)$  as the space of linear operators acting on  $\mathcal{H}^A$ . For a qubit system  $A'$ , the Hilbert space is denoted by  $\mathcal{H}^{A'}$ . The Pauli operators on  $\mathcal{H}^{A'}$  are  $X_{A'}$ ,  $Y_{A'}$ , and  $Z_{A'}$ . The eigenstates of  $X_{A'}$ ,  $Y_{A'}$ , and  $Z_{A'}$  are  $\{|\pm\rangle_{A'}\}$ ,  $\{|\pm i\rangle_{A'}\}$ , 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  $M_Z : \{|0\rangle_{A'}\langle 0|, |1\rangle_{A'}\langle 1|\}$ . The four Bell state are

$$\begin{aligned} |\Phi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \\ |\Psi_{\pm}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \end{aligned} \quad (\text{A1})$$

For a qubit  $A'$  and a qudit  $A$ , the controlled- $U$  operation is defined as

$$C_{A'A} = |0\rangle_{A'}\langle 0| \otimes I_A + |1\rangle_{A'}\langle 1| \otimes U_A. \quad (\text{A2})$$

### 1. Security definition

In QKD, the two communication parties, Alice and Bob, will finally obtain a pair of bit strings  $S_a$  and  $S_b$  with a

length of  $N_k$  (if the protocol succeeds), which can be correlated to a quantum state held by Eve. The joint state  $\rho_{ABE}$  is a classical-classical-quantum state,

$$\rho_{ABE} = \sum_{s_a, s_b} \Pr_{S_a, S_b}(s_a, s_b) |s_a\rangle_A \langle s_a| \otimes |s_b\rangle_B \langle s_b| \otimes \rho_E^{(s_a, s_b)}, \quad (\text{A3})$$

where  $S_a, S_b$  are random variables and  $s_a, s_b \in \{0, 1\}^{N_k}$  are the values. In particular, an ideal key state held by Alice and Bob is described by the private state,

$$\rho_{ABE}^{\text{ideal}} = (2^{N_k})^{-1} \sum_s |s\rangle_A \langle s| \otimes |s\rangle_B \langle s| \otimes \rho_E, \quad (\text{A4})$$

where  $s_a = s_b = s$  implies that Alice and Bob hold the same string, and  $\rho_E$  is independent of  $s$ , that is, Eve has no information on the key-string variable  $S$ .

A QKD protocol is defined to be  $\epsilon$  secure, if the final distilled state  $\rho_{ABE}$  is  $\epsilon$  closed to any private state  $\rho_{ABE}^{\text{ideal}}$  with a proper chosen  $\rho_E$

$$\min_{\rho_E} \frac{1}{2} \|\rho_{ABE} - \rho_{ABE}^{\text{ideal}}\|_1 \leq \epsilon, \quad (\text{A5})$$

where  $\|A\|_1 \equiv \text{Tr}[\sqrt{A^\dagger A}]$  is the trace norm.

Usually, we would like to decompose the secret definition to two parts, secrecy and correctness. A QKD protocol is defined to be  $\epsilon_{\text{cor}}$  correct, if the probability distribution  $\Pr_{S_a, S_b}(s_a, s_b)$  of the final state  $\rho_{ABE}$  in Eq. (A3) satisfies

$$\Pr_{S_a, S_b}(s_a \neq s_b) \leq \epsilon_{\text{cor}}. \quad (\text{A6})$$

A QKD protocol is defined to be  $\epsilon_{\text{sec}}$  secret, if the state  $\rho_{AE}$  is closed to the single-party private state  $\rho_{AE}^{\text{ideal}}$

$$\min_{\rho_E} \frac{1}{2} \|\rho_{AE} - \rho_{AE}^{\text{ideal}}\|_1 \leq \epsilon_{\text{sec}}, \quad (\text{A7})$$

where  $\rho_{AE}^{\text{ideal}} \equiv (2^{N_k})^{-1} \sum_s |s\rangle_A \langle s| \otimes \rho_E$ . If a QKD protocol is  $\epsilon_{\text{cor}}$  correct and  $\epsilon_{\text{sec}}$  secret, then it is  $(\epsilon_{\text{cor}} + \epsilon_{\text{sec}})$  secure [29].

### 2. Security proof based on phase-error correction

Here, we briefly review the main idea of phase-error-based security proof, which is first proposed by Lo and Chau [5], reduced to prepare-and-measure scheme later by Shor and Preskill [6], and improved by Koashi later [29].

In an entanglement-based QKD protocol, Alice and Bob will finally share a large bipartite state  $\rho_{AB}$ . Denote Alice and Bob's subspaces in a single run as  $\mathcal{H}_A$  and  $\mathcal{H}_B$ . Here, the encrypted error correction is used to decouple the error correction and privacy amplification. The protocol is presented as below.

### Actual protocol

(1) (State distribution) Alice and Bob share a bipartite state  $\rho_{AB}$  in the space  $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ , where  $n$  is the total number of runs.

(2) (Measurement) Alice and Bob measure their systems  $\mathcal{H}_A^{\otimes n}$  and  $\mathcal{H}_B^{\otimes n}$ , respectively. Suppose the measurement results can be described by  $n$ -bit strings  $\kappa_A$  and  $\kappa_B$ .

(3) (Error correction) They reconcile the key strings through an encrypted classical channel consuming  $l_{EC}$  bits of secret key. They agree on an  $n$ -bit raw key string  $\kappa_{rec}$  except for a small failure probability  $\epsilon_{EC}$ .

(4) (Privacy amplification) Alice randomly chooses  $n - m$  strings  $\{V_k\}_{k=1, \dots, n-m}$  of  $n$  bit, which are linearly independent, and announces the strings to Bob. The final key length is  $n - m$ , where the  $k$ th key bit is  $\kappa_{rec} \times V_k$ . Denote the final key as  $\kappa_{fin}$ .

Note that the error correction can be easily conducted just by classical information theory. The only remaining concern is to quantize the information leakage  $m$  on  $\kappa_{rec}$ . Note that, Eve's knowledge of  $\kappa_{rec}$  will not change after any operation on  $\mathcal{H}_A$  and  $\mathcal{H}_B$  that keeps Eve's state and the raw key bits  $\kappa_{rec}$ . Based on this argument, we construct the following virtual protocol.

### Virtual protocol

(1) (State distribution) Alice and Bob share a bipartite state  $\rho_{AB} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ .

(2) (Squashing) They apply operation  $\Lambda$  on  $\rho_{AB}$  and convert it to a key space  $\mathcal{K}^{\otimes n}$  and ancillary space  $\mathcal{H}_R$ , i.e.,  $\Lambda(\rho_{AB}) \in \mathcal{K}^{\otimes n} \otimes \mathcal{H}_R$ .

(3) (Measurement) They measure  $\mathcal{K}^{\otimes n}$  on the  $Z$  basis and obtain  $\kappa_{rec}$ . They then measure  $\mathcal{H}_R$  by  $M_R$ . Suppose the measurement result of  $M_R$  is  $\gamma$ .

(4) (Privacy amplification) They randomly choose  $n - m$  linearly independent  $n$ -bit strings  $\{V_k\}_{k=1, \dots, n-m}$  and announce them. The final key length is  $n - m$ , and the  $k$ th key bit is  $\kappa_{rec} \times V_k$ . Denote the final key as  $\kappa_{fin}$ .

The operation  $\Lambda$  and measurement  $M_R$  can be chosen freely, and are only subjected to the requirement that the  $Z$ -basis measurement statistics on  $\mathcal{K}^{\otimes n}$  is the same as  $\kappa_{rec}$  in the actual protocol. Therefore, Eve's knowledge of  $\kappa_{rec}$  in the virtual protocol is the same as in the actual protocol. The secrecy of  $\kappa_{rec}$  in the virtual protocol is the same as the one in the practical protocol.

The core observation in the security proof based on phase-error correction is that, with a proper choice of  $\Lambda$  and  $M_R$ , the security of  $Z$ -basis measurement result  $\kappa_{rec}$  can be reflected on the predictability of  $X$ -basis measurement result  $T_\gamma$ , given the measurement outcome  $\gamma$  on  $\mathcal{H}_R$ . Denote  $|T_\gamma|$  as the size of possible  $X$ -basis measurement outcomes.

**Lemma 1** (Koashi, 09 [29]). *If the chosen  $\Lambda$  and  $M_R$  in the above virtual protocol meets the requirements,*

(1) *the  $Z$ -basis measurement statistics on  $\mathcal{K}^{\otimes n}$  is the same as  $\kappa_{rec}$  in actual protocol;*

(2) *given each measurement outcome  $\gamma$  on  $\mathcal{H}_R$ , the size of  $X$ -basis measurement outcome on  $\mathcal{K}^{\otimes n}$  is bounded by  $|T_\gamma| \leq 2^{n\xi}$ , except for a small probability  $\epsilon_T$ ,*

*then the virtual protocol is  $\sqrt{\epsilon'_T}$  secret and  $\epsilon_{EC}$  correct, thus  $(\sqrt{\epsilon'_T} + \epsilon_{EC})$  secure, where  $\epsilon'_T = \epsilon_T + 2^{-n\zeta}$  and  $m = n(\xi + \zeta)$ .*

Here we collect all the related small failure probabilities,

(i)  $\epsilon_{EC}$  is the failure probability of error correction that affect the correctness of the protocol, which is determined by the method used in the error-correction step;

(ii)  $\epsilon_T$  is the failure probability of bounding  $|T_\gamma|$ . Usually this is the failure probability  $\epsilon_{pe}$  of estimating phase-error number  $n^{EX}$ . This amount is determined by the method used to estimate the phase error;

(iii)  $\zeta$  is the extra amount of privacy amplification to enhance the privacy of the protocol, which can be determined arbitrarily according to the need for privacy. Usually we denote  $\epsilon_{PA} = 2^{-n\zeta}$  as the failure probability of privacy amplification.

Usually, we introduce phase-error number  $n^{EX}$  to characterize the size of  $|T_\gamma|$ . Suppose that, in an ideal case, the  $X$ -basis measurement outcome  $\mathcal{K}^{\otimes n}$  for a given  $\gamma$  is deterministic  $T_\gamma^{(0)}$ . Then we can calculate the number of phase error  $n^{EX}$  of given measurement result  $T_\gamma$  from  $T_\gamma^{(0)}$ , defined as  $n^{EX}(T_\gamma) \equiv \text{wt}(T_\gamma \oplus T_\gamma^{(0)})$ , where  $\text{wt}(A)$  is the weight, i.e., number of nonzero elements in string  $A$ , and  $\oplus$  is the modulo-2 addition. Denote  $n^{EX}$  as the maximum value of  $n^{EX}(T_\gamma)$  for a given set  $\{T_\gamma\}$ . Then the size of  $\{T_\gamma\}$  is bounded by

$$|T_\gamma| = \sum_{k=0}^{n^{EX}} \binom{n}{k} < \binom{n}{n^{EX} + 1} < 2^{nH[(n^{EX} + 1)/n]}, \quad (\text{A8})$$

where the first inequality holds when  $(n^{EX} + 1 < n/3)$  [10]. The proof of the second inequality can be found in Ref. [38]. From a phase-error correction point of view, this is essentially the typical space argument used in Shannon's theory.

Denote the average phase-error number as  $\bar{n}^{EX}$ . The phase-error rate is defined to be  $E^X \equiv \bar{n}^{EX}/n$ . Note that the final key length is  $n - m$ , where  $m = n\xi \geq nH[(n^{EX} + 1)/n] = nH(E^X)$ , we conclude that an approximate proportion  $H(E^X)$  of raw key bits is sacrificed

in privacy amplification. Taken the reconciliation case  $l_{\text{EC}}$  into account, the net key-generation length is

$$K = n - m - l_{\text{EC}} \geq n[1 - H(E^X)] - l_{\text{EC}}. \quad (\text{A9})$$

One should note that, in Koashi's security proof, there is a *degree of freedom on choosing the definition of phase error  $E^X$* , based on the operation  $\Lambda$  and the ancillary measurement  $M_R$ , as long as Lemma 1 holds. This endows a large flexibility when we analyze the security of QKD.

### 3. Perfect privacy induced by encoding symmetry

We prove the symmetric encoding QKD based on the aforementioned security proof, which essentially generalizes the one employed in the security proof of PM QKD [20]. First, we introduce a general entanglement-based symmetric encoding QKD protocol, as shown in Fig. 4. Here, Alice and Bob share a two-qudit state  $\sigma_{AB}$  on system  $A$  and  $B$ , at the beginning of each run. Alice holds an extra qubit  $A'$  on state  $|+\rangle$  initially, and she creates entanglement between  $A$  and  $A'$  by applying the following control- $U$  operation

$$C_{A'A}(U) = |0\rangle_{A'} \langle 0| \otimes I_A + |1\rangle_{A'} \langle 1| \otimes U_A. \quad (\text{A10})$$

She then sends qudit  $A$  out to Eve. Similarly, Bob holds  $B'$ , performs  $C_{B'B}(U)$  on  $B$  and  $B'$ , and sends  $B$  to Eve. Eve performs joint measurement on system  $A$  and  $B$  to create entanglement on qubit system  $A'$  and  $B'$ . Here, the encoding unitary  $U_A$  in  $C_{A'A}(U)$  meets the requirement of symmetric encoding,

$$U^2 = U^\dagger U = I. \quad (\text{A11})$$

In that case, the eigenvalue of  $U_A$  will be either 1 or  $-1$ . Denote the subspaces spanned by the eigenvectors with

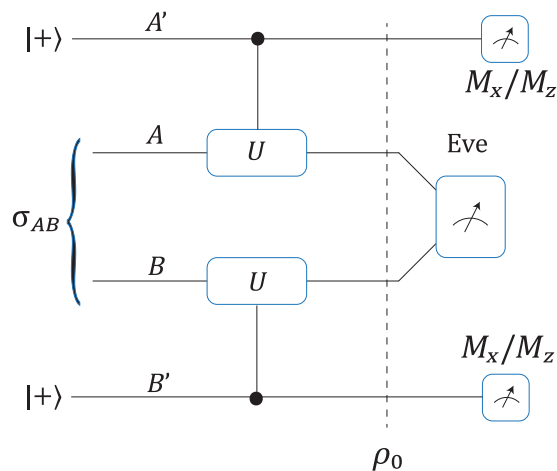


FIG. 4. Schematic diagram for a general entanglement-based version of symmetric encoding protocol. When  $\sigma_{AB}$  is a parity state, then the protocol is perfectly private without any information leakage.

eigenvalue 1 and  $-1$  to be the even space  $\mathcal{H}_A^{\text{even}}$  and the odd space  $\mathcal{H}_A^{\text{odd}}$ . For a joint unitary  $U_A \otimes U_B$ , the eigenvalue will also be 1 or  $-1$ . The even space and the odd space of the joint  $A, B$  Hilbert space is

$$\begin{aligned} \mathcal{H}_{AB}^{\text{odd}} &= (\mathcal{H}_A^{\text{odd}} \otimes \mathcal{H}_B^{\text{even}}) \oplus (\mathcal{H}_A^{\text{even}} \otimes \mathcal{H}_B^{\text{odd}}), \\ \mathcal{H}_{AB}^{\text{even}} &= (\mathcal{H}_A^{\text{odd}} \otimes \mathcal{H}_B^{\text{odd}}) \oplus (\mathcal{H}_A^{\text{even}} \otimes \mathcal{H}_B^{\text{even}}). \end{aligned} \quad (\text{A12})$$

**Definition 1.** A state  $\rho$  on two qudits  $A, B$  is an odd state with respect to  $U_A \otimes U_B$  iff  $\rho \in \mathcal{H}_{AB}^{\text{odd}}$  and an even state with respect to  $U_A \otimes U_B$  iff  $\rho \in \mathcal{H}_{AB}^{\text{even}}$ . Both odd states and even states are called parity states.

**Corollary 1.** A state  $\rho$  remains invariant under the transformation of  $U_A \otimes U_B$ , i.e.,  $\rho = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$ , iff  $\rho$  is a mixture of parity states.

*Proof:* Obviously, the mixture of parity states satisfies the encoding symmetry  $\rho = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$ . Here we prove all the states  $\rho$  with encoding symmetry are mixture of parity states.

Since  $(U_A \otimes U_B)^2 = I$ , the eigenvalue of it should be either  $-1$  or 1. Denote the eigenbasis of  $U_A \otimes U_B$  as  $\{|p, i\rangle\}$  with eigenvalues  $\{(-1)^p\}$ , where  $p = 0, 1$  denotes the even subspace  $\mathcal{H}_{AB}^{\text{even}}$  or odd subspace  $\mathcal{H}_{AB}^{\text{odd}}$ , while  $i$  denotes the inner degeneracy in the even or odd subspace.

We expand  $\rho$  in the eigenbasis of  $U_A \otimes U_B$ ,

$$\rho = \sum_{p,q,i,j} c_{p,q,i,j} |p, i\rangle \langle q, j|. \quad (\text{A13})$$

Therefore,

$$U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger = \sum_{p,q,i,j} (-1)^{p-q} c_{p,q,i,j} |p, i\rangle \langle q, j|, \quad (\text{A14})$$

and  $\rho = U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$  implies that

$$c_{p,q,i,j} = 0 \quad \text{if } p \neq q, \quad (\text{A15})$$

that is, the off-diagonal space between odd and even states is a null space.

Moreover, due to the degeneracy of odd and even subspace, it is always possible to find an eigenbasis of  $U_A \otimes U_B$  as  $\{|p, i\rangle\}$  to diagonalize the parity states. ■

We first consider the following entanglement-based QKD protocol, and analyze how the symmetry of the state will preserve QKD privacy.

#### Protocol I

(1) State preparation: Alice and Bob share a known state  $\sigma_{A,B}$  on two qudits  $A, B$ , at the beginning of each run.



They initialize their qubits  $A', B'$  in  $|+\rangle$ . Alice applies the control gate  $C_{A'A}(U)$  to  $A'$  and  $A$ . Similarly, Bob applies  $C_{B'B}(U)$  to  $B'$  and  $B$ .

(2) Measurement: Alice and Bob send the two optical pulses  $A$  and  $B$  to an untrusted party, Eve, who is supposed to perform joint measurement and announce the detection results. The ideal measurement is to discriminate whether the state is  $\sigma_{AB}$  or  $(U_A \otimes I)\sigma_{AB}(U_A \otimes I)^\dagger$ .

(3) Announcement: Eve announces the detection result for each round. Based on Eve's announcement, Bob decides whether or not to apply  $X$  operation on his qubit  $B'$ .

(4) Sifting: Given a specific announcement of Eve, Alice and Bob keep the qubits of systems  $A'$  and  $B'$ .

Alice and Bob perform the above steps for many rounds and end up with a joint  $2n$ -qubit state  $\rho_{A'B'} \in (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})^{\otimes n}$ .

(5) Key generation: Alice and Bob perform local  $Z$  measurements on  $\rho_{A'B'}$  to generate raw data string  $\kappa_A$  and  $\kappa_B$ . They reconcile the key string to  $\kappa_{\text{rec}}$  by an encrypted classical channel, with the consummation of  $l_{\text{EC}}$ -bit keys. Here we set Alice's key as the final reconciled key  $\kappa_A = \kappa_{\text{rec}}$ .

Denote the whole  $2n$  state Alice and Bob share after the quantum step as  $\rho_{A'B'}$ , and the partial-traced state of the  $m$ th round as  $\rho_{A'B'}^{(m)}$ .

**Lemma 2.** *In protocol I, if the optical state  $\sigma$  Alice and Bob share during the  $m$ th run is an odd state, then the two-qubit state Alice and Bob finally obtain,  $\rho_{A'B'}^{(m)}$ , is in the subspace spanned by  $\{\Phi^-, \Psi^-\}$ ; and if  $\sigma$  is an even state, then  $\rho_{A'B'}^{(m)}$  is in the subspace spanned by  $\{\Phi^+, \Psi^+\}$ . Here  $m \in \{1, 2, \dots, n\}$ .*

*Proof:* First consider the pure state  $\sigma = |\psi\rangle\langle\psi|$ . The joint state on system  $A', B', A, B$  before the  $C(\pi)$  operations is

$$|++\rangle_{A'B'} |\psi\rangle_{AB} = \frac{1}{2} [(|00\rangle + |11\rangle) + (|01\rangle + |10\rangle)]_{A'B'} |\psi\rangle_{AB}. \quad (\text{A16})$$

Note that for odd state  $|\psi_o\rangle_{AB}$ ,

$$\begin{aligned} U_A \otimes U_B |\psi_o\rangle_{AB} &= -|\psi_o\rangle_{AB}, \\ U_A \otimes I_B |\psi_o\rangle_{AB} &= -I_A \otimes U_B |\psi_o\rangle_{AB}, \end{aligned} \quad (\text{A17})$$

and for even state  $|\psi_e\rangle_{AB}$ ,

$$\begin{aligned} U_A \otimes U_B |\psi_e\rangle_{AB} &= |\psi_e\rangle_{AB}, \\ U_A \otimes I_B |\psi_e\rangle_{AB} &= I_A \otimes U_B |\psi_e\rangle_{AB}, \end{aligned} \quad (\text{A18})$$

Therefore, for odd pure state  $|\psi_o\rangle$  input, the state after the  $C_{A'A}(U) \otimes C_{B'B}(U)$  operations is

$$\begin{aligned} |\Psi_o\rangle &= C_{A'A}(U) \otimes C_{B'B}(U) \left( \frac{1}{2} [(|00\rangle + |11\rangle) + (|01\rangle + |10\rangle)]_{A'B'} |\psi_o\rangle_{AB} \right) \\ &= \frac{1}{2} \{ [|00\rangle_{A'B'} + |11\rangle_{A'B'} (U_A \otimes U_B)] + [|01\rangle_{A'B'} (U_A \otimes I_B) + |10\rangle_{A'B'} (I_A \otimes U_B(\pi))] \} |\psi_o\rangle_{AB} \\ &= \frac{1}{2} [(|00\rangle - |11\rangle)_{A'B'} |\psi_o\rangle_{AB} + (|01\rangle - |10\rangle)_{A'B'} (U_A \otimes I_B) |\psi_o\rangle_{AB}], \end{aligned} \quad (\text{A19})$$

and for even pure state  $|\psi_e\rangle$  input, the state after the  $C_{A'A}(U) \otimes C_{B'B}(U)$  operations is

$$\begin{aligned} |\Psi_e\rangle &= C_{A'A}(U) \otimes C_{B'B}(U) \left( \frac{1}{2} [(|00\rangle + |11\rangle) + (|01\rangle + |10\rangle)]_{A'B'} |\psi_e\rangle_{AB} \right) \\ &= \frac{1}{2} \{ [|00\rangle_{A'B'} + |11\rangle_{A'B'} (U_A \otimes U_B)] + [|01\rangle_{A'B'} (U_A \otimes I_B) + |10\rangle_{A'B'} (I_A \otimes U_B(\pi))] \} |\psi_e\rangle_{AB} \\ &= \frac{1}{2} [(|00\rangle + |11\rangle)_{A'B'} |\psi_e\rangle_{AB} + (|01\rangle + |10\rangle)_{A'B'} (U_A \otimes I_B) |\psi_e\rangle_{AB}]. \end{aligned} \quad (\text{A20})$$

For the odd-state case, if we partially trace out system  $A, B$  in  $|\Psi_o\rangle$ , the state  $\rho_{A'B'}^{(m)}$  is in the subspace of  $\{\Phi^-, \Psi^-\}$ . Whatever Eve's announcement afterward is, the possible operation on  $\rho_{A'B'}^{(m)}$  is either  $I_{A'} \otimes I_{B'}$  or  $I_{A'} \otimes X_{B'}$ .

Note that  $(I_{A'} \otimes X_{B'}) |\Phi^-\rangle = |\Psi^-\rangle$ , hence the state  $\rho_{A'B'}^{(m)}$  is still in the subspace of  $\{\Phi^-, \Psi^-\}$ . Similarly, for the even-state case, the state  $\rho_{A'B'}^{(m)}$  is in the subspace of  $\{\Phi^+, \Psi^+\}$ .

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

$$\begin{aligned}\sigma_{\text{odd}} &= \sum_i p_i |\psi_o^{(i)}\rangle \langle \psi_o^{(i)}|, \\ \sigma_{\text{even}} &= \sum_i p_i |\psi_e^{(i)}\rangle \langle \psi_e^{(i)}|.\end{aligned}\quad (\text{A21})$$

This is equivalent to Charlie sending out  $|\psi_{o(e)}^{(i)}\rangle$  with probability  $p_i$ . For each odd pure-state component, the left qubit state  $\rho_{A'B'}^{(m)}$  is in the subspace of  $\{\Phi^-, \Psi^-\}$ , therefore their mixtures are still in this subspace. Similar arguments hold for the even-parity states. ■

Note that

$$\begin{aligned}(X_{A'} \otimes X_{B'}) |\Phi^+\rangle &= (X_{A'} \otimes X_{B'}) |\Psi^+\rangle = 1, \\ (X_{A'} \otimes X_{B'}) |\Phi^-\rangle &= (X_{A'} \otimes X_{B'}) |\Psi^-\rangle = -1.\end{aligned}\quad (\text{A22})$$

Therefore, if the state  $\rho_{A'B'}^{(m)}$  is in the subspace of  $\{\Phi^-, \Psi^-\}$ , then the measurement outcome of  $X \otimes X$  is always  $-1$ ; in contrast, if the state is in the subspace of  $\{\Phi^+, \Psi^+\}$ , then the measurement outcome of  $X \otimes X$  is always  $1$ .

**Definition 2.** In protocol I, define the observed value  $\frac{1}{2}(1 - \langle X_{A'} \otimes X_{B'} \rangle)$  to be the odd phase-error rate  $E_o^X$ , and  $\frac{1}{2}(1 + \langle X_{A'} \otimes X_{B'} \rangle)$  to be the even phase-error rate  $E_e^X$ .

Note that  $E_e^X = 1 - E_o^X$ . From Lemma 2, we have the following Theorem.

**Theorem 2.** In protocol I, for an odd (even) state input  $\sigma$ , the odd (even) phase-error rate is always 0. That is, if Alice measures system  $A'$  on  $X$  basis instead of  $Z$  basis, then the measurement result is certain, given Bob's measurement outcome  $\gamma_{B'}$  on system  $B'$ . In this case, Eve has no information on Alice's  $Z$ -basis measurement result  $\kappa_{\text{rec}}$ , i.e., perfect privacy.

In the phase-error-based proof, the definition of phase error  $E^X$  is adaptive as long as the requirements in Lemma 1 hold. Both the odd states and even states  $\sigma$  yield certain  $X_{A'} \otimes X_{B'}$  results, hence they are the perfect source for protocol I, which yield keys with perfect privacy.

Now we consider the case when Alice and Bob hold a mixture of odd and even states. The overall phase-error rate cannot be zero, regardless of whether odd or even phase-error definition is applied.

We write the state  $\sigma_{AB}$  shared by Alice and Bob as

$$\sigma_{AB} = \sum_i p_o^{(i)} |\psi_o^{(i)}\rangle_{AB} \langle \psi_o^{(i)}| + \sum_j p_e^{(j)} |\psi_e^{(j)}\rangle_{AB} \langle \psi_e^{(j)}|, \quad (\text{A23})$$

with  $\sum_i p_o^{(i)} + \sum_j p_e^{(j)} = 1$ . Introduce the purification of  $\sigma$ ,

$$\begin{aligned}|\Psi\rangle_{PAB} &= \sum_i \sqrt{p_o^{(i)}} |o, i\rangle_P |\psi_o^{(i)}\rangle_{AB} \\ &+ \sum_j \sqrt{p_e^{(j)}} |e, j\rangle_P |\psi_e^{(j)}\rangle_{AB},\end{aligned}\quad (\text{A24})$$

where system  $P$  is a register to store the parity information. Suppose  $\{|p, i\rangle_P\}$  is an orthogonal basis such that  $\langle p, i | q, j \rangle = \delta_{pq} \delta_{ij}$ , with  $p = o, e$  denotes the parity of the according state, and  $i$  denotes the index of odd and even pure states. Such a basis is defined as the  $Z$  basis of system  $P$ .

Here we consider two cases, where Eve's knowledge of  $\sigma_{AB}$  is different. First, we consider the case when Eve's state is decoupled from  $\sigma_{AB}$  at the beginning, that is,  $\rho_{ABE} = \sigma_{AB} \otimes \rho_E$ . That is to say, Eve does not hold the purified system  $P$ , and we can virtually imagine that system  $P$  is held by Alice and Bob. In Fig. 5 we draw the whole protocol Ia with the ancillary  $P$  presents. In phase-error-based proof, when we characterize Eve's knowledge of Alice's final  $Z$ -basis measurement results on  $A'$   $\kappa_{\text{rec}}$ , we transform the problem to how Alice can predict the  $X$ -basis measurement result  $\gamma$  in the presence of system  $B'$  and  $P$ . In this case, Alice can learn the parity information of each single round from the measurement result of  $P$ , where Alice can flip her  $X$ -basis measurement result on  $\mathcal{K}$  to match  $\gamma$  if the parity is not in accordance with the definition choice of phase error. Therefore, by Theorem 2 above, Alice can perfectly predict the  $X$ -basis measurement result. Applying Lemma 1, we prove the perfect privacy of parity states.

**Corollary 2.** In protocol I, if Alice and Bob share a mixture of odd and even states  $\sigma_{AB}$  at the beginning of each run, and Eve's state  $\rho_E$  is decoupled from  $\sigma_{AB}$ , i.e.,  $\rho_{ABE} = \sigma_{AB} \otimes \rho_E$ , then Eve has no information on Alice's  $Z$ -basis measurement result  $\kappa_{\text{rec}}$ , i.e., perfect privacy.

Now we consider the case when Eve holds the purification of  $\sigma_{AB}$ . We consider the following protocol.

### Protocol Ia

(1) In the same manner, Alice and Bob perform steps (1)–(4) in protocol I for many rounds and end up with a

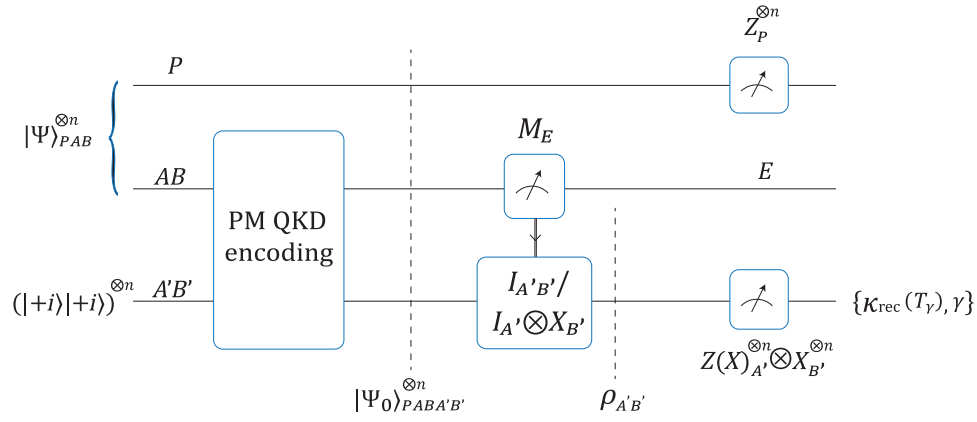


FIG. 5. Schematic diagram for the whole protocol I/Ia when the input state is a general mixed parity state  $\sigma_{AB}$ . Here we postselect the rounds when Eve announces effective clicks. Alice and Bob prepare  $n$  rounds of state  $|\Psi\rangle_{PAB}$  in Eq. (A24). They perform the PM QKD encoding by applying  $C(U)$  gates on system  $A', A$  and  $B', B$ , as illustrated in Fig. 4. After that, they send system  $A, B$  to Eve, and perform  $I_{A'B'}$  or  $I_{A'} \otimes X_{B'}$  operation on each round of system  $A', B'$ . They measure them by  $Z_{A'} \otimes X_{B'}$  to get strings  $\kappa_{\text{rec}}, \gamma$ . In protocol Ia, after Eve's announcement, they send system  $P$  to Eve. In phase-error-based proof, Eve's knowledge of  $\kappa_{\text{rec}}$  can be characterized by Alice's knowledge of her  $X$ -basis measurement result  $T_\gamma$  on  $A'$ .

joint  $2n$ -qubit state  $\rho_{A'B'}$ . After that, Alice and Bob send the purified system  $P$  of each run to Eve.

(2) Key generation: Bob performs local  $X$  measurements on system  $B'$  with measurement outcome  $\gamma_{B'}$ , and Alice performs local  $Z$  measurements to obtain the final key  $\kappa_{\text{rec}}$ .

In protocol Ia, a weaker version of protocol I, Alice and Bob no longer hold the system  $P$ , which makes them unable to discriminate the parity information, and their ability to predict  $T_\gamma$  is weakened. However, an important observation is that, due to system  $P$  being sent to Eve after her announcement, the announcement result must be independent of system  $P$ , in which case, for Eve's fixed measurement strategy, the state  $\rho_{A'B'}$  in protocols Ia and Ib will be the same.

In another aspect, without the assistance of parity information in  $P$ , Alice and Bob cannot deal with the odd and even rounds separately, and there is no longer perfect privacy. Alice's knowledge of  $T_\gamma$  given  $\gamma$  is characterized by the overall odd or even phase error. For the clicked  $n$  rounds, if we measure the system  $P$  on  $Z$  basis, and there are  $n_{\text{even}}$  rounds with even-parity measurement results. Then the overall odd phase-error rate is

$$E_o^X = \frac{n_{\text{even}}}{n}. \quad (\text{A25})$$

**Corollary 3.** In protocol I/Ia, if Alice and Bob share a mixture of odd and even states  $\sigma_{AB}$  at the beginning of each run and Eve holds the purification of  $\sigma_{AB}$ , then the final odd phase error  $E_o^X$ , which characterizes the information leakage of  $\kappa_{\text{rec}}$  to Eve, is given by

$$E_o^X = \frac{n_{\text{even}}}{n}, \quad (\text{A26})$$

where  $n$  is the round number with effective signals, and  $n_{\text{even}}$  is the estimated rounds with even state as the source.

From now on, we define the phase error  $E^{\text{ph}}$  as the odd phase-error rate  $E_o^X$ . As an expense to realize parity states by independent phase randomization with phase announcement, we cannot discriminate even and odd components any more, and should use a unified phase-error definition, while Eve's announcement strategy is unchanged, and the local state  $\rho_{A'B'}$  also remains unchanged, which indicates that protocol Ia and protocol Ib are the same except in parity discrimination.

## APPENDIX B: SECURITY PROOF OF PM QKD

Here we present security proof of PM QKD, by reducing it to the symmetric encoding QKD mentioned above. In particular, we use the decoy method to monitor the phase-error number  $n^{EX}$  in real experimental setting to determine what proportion of raw keys should be sacrificed to enhance the total privacy. First, we introduce the notation used in the proof.

The qudit system  $A$  considered in Appendix A is on an optical mode, whose creation operator is  $a^\dagger$  and Hilbert space is denoted as  $\mathcal{H}^A$ . A  $k$ -photon Fock state  $|k\rangle_A$  is defined as

$$|k\rangle_A \equiv \frac{(a^\dagger)^k}{\sqrt{k!}} |0\rangle_A, \quad (\text{B1})$$

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

$$|\alpha\rangle_A \equiv e^{-(1/2)|\alpha|^2} \sum_{k=0}^{\infty} \frac{\alpha^k}{\sqrt{k!}} |k\rangle_A \quad (\text{B2})$$

The photon number of  $|\alpha\rangle_A$  follows a Poisson distribution  $P_\mu(k) = e^{-\mu} \mu^k / k!$ , where  $\mu = |\alpha|^2$  is the mean photon number, also the light intensity. In the following proof, we specifically select

$$U = U_A = U_B = e^{i\pi a^\dagger a}, \quad (\text{B3})$$

which satisfies the condition  $U^2 = I$ . When applied on a Fock state  $|n\rangle$ , this operation adds an additional phase  $(-1)^n$ , which has no effect on even-photon Fock states, while changing the phase of odd-photon Fock states. As a result, we have the following corollary.

**Corollary 4.** *A state  $\rho$  on two modes  $A, B$  is an odd (even) state with respect to  $U_A \otimes U_B$  iff  $\hat{\Pi}_o \rho \hat{\Pi}_o = \rho$  ( $\hat{\Pi}_e \rho \hat{\Pi}_e = \rho$ ).  $\hat{\Pi}_o$  and  $\hat{\Pi}_e$  are the projectors of the odd and even subspaces respectively, which are defined as*

$$\begin{aligned} \hat{\Pi}_o &= \sum_{m+n:\text{odd}} |m, n\rangle_{AB} \langle m, n|, \\ \hat{\Pi}_e &= \sum_{m+n:\text{even}} |m, n\rangle_{AB} \langle m, n|, \end{aligned} \quad (\text{B4})$$

where  $\{|m, n\rangle_{A,B}\}_{m,n}$  are the Fock basis on optical modes  $A$  and  $B$ .

### 1. Phase randomization and parity state

To generate a mixture of parity states, we introduce the “twirling” operation,

$$\mathcal{E}(\sigma_{AB}) = \frac{1}{2}\sigma_{AB} + \frac{1}{2}(U_A \otimes U_B)\sigma_{AB}(U_A \otimes U_B)^\dagger. \quad (\text{B5})$$

Note that  $\mathcal{E}(\sigma_{AB})$  remains invariant under the transformation  $U_A \otimes U_B$ , and therefore is a mixture of parity state for any state  $\sigma_{AB}$  on two optical modes  $A$  and  $B$  according to Corollary 1. To implement  $\mathcal{E}$  in PM QKD, Alice and Bob can first randomize their systems  $A, B$  with random phase  $\phi_a$  and  $\phi_b$  independently, announce the random phase, and postselect the runs with the same random phase *after Eve's detection announcements*. PM QKD with independent randomization is summarized as protocol II below, as shown in Fig. 6.

#### Protocol II

(1) State preparation: Alice and Bob share a known state  $\sigma_{AB}$  on two optical modes  $A, B$ , at the beginning of each run. They initialize their qubits  $A', B'$  in  $|+\rangle$ . Alice applies the control gate  $C_{A'A}(U)$  to qubit  $A'$  and optical pulse  $A$ , and adds an extra random  $0$  or  $\pi$  phase  $\phi_a$  on  $A$ . Similarly, Bob applies  $C_{B'B}(U)$ ,  $\phi_b$  to  $B'$  and  $B$ .

(2) Measurement: Alice and Bob send the two optical pulses  $A$  and  $B$  to an untrusted party, Eve, who is supposed

to perform joint measurement and obtain the detection results  $L$  or  $R$ , which is expected to be projective measurement on the basis  $\mathcal{E}(\sigma_{AB})$  and  $(U_A \otimes I)\mathcal{E}(\sigma_{AB})(U_A \otimes I)^\dagger$ . However, this is not an assumption or requirement of the measurement of Eve, as an untrusted party.

(3) Announcement: Eve announces the detection result or no successful detection for each round. After that, Alice and Bob announce their random phases  $\phi_a$  and  $\phi_b$ .

(4) Sifting: When Eve announces an  $L$  or  $R$  click, Alice and Bob keep the qubits of systems  $A'$  and  $B'$ . In addition, Bob applies a Pauli  $X$  gate to his qubit  $B'$  if Eve's announcement is  $R$  click. If  $|\phi_a - \phi_b| = \pi$ , Bob applies another Pauli  $X$  gate on  $B'$ .

Alice and Bob perform the above steps for many rounds and end up with a joint  $2n$ -qubit state  $\rho_{A'B'} \in (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})^{\otimes n}$ .

(5) Parameter estimation: Alice and Bob estimate the click ratios caused by even-state fractions.

(6) Key generation: Alice and Bob perform local  $Z$  measurements on  $\rho_{A'B'}$  to generate raw data strings  $\kappa_A$  and  $\kappa_B$ . They reconcile the key string to  $\kappa_A$  by an encrypted classical channel, with the consummation of  $t_{EC}$ -bit keys. After that, they perform privacy amplification according to the even-state ratio to generate keys.

In protocol II, the signals with  $|\phi_a - \phi_b| = \pi$  can also be used if Bob performs extra  $Y_{B'}$  gate on system  $B'$  before the key-generation step [20]. Besides the independent randomization, protocol II is the same as protocol I, which indicates that the security of protocol II can be reduced to protocol I, and the information leakage in protocol II can be bounded by the phase-error rate,  $E_o^X$ , which is introduced in protocol Ia, a weaker form of protocol I. The problem of independent randomization is analyzed in the following text.

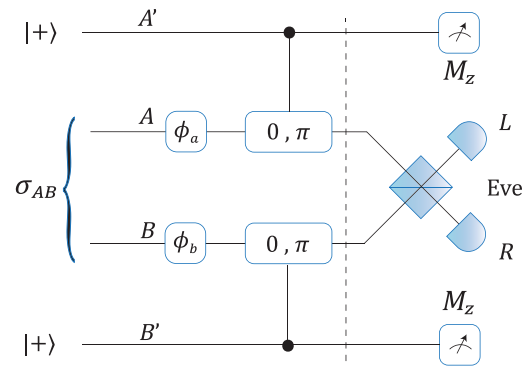


FIG. 6. Realistic PM QKD protocol with extra  $0/\pi$ -phase randomization.  $\sigma_{AB}$  is a generic state on optical modes  $A$  and  $B$ .  $\phi_a, \phi_b$  are two random phases, which are either  $0$  or  $\pi$ . In practice, the phase can be absorbed into the controlled- $U(\pi)$  operations afterwards.



In the protocol, Alice and Bob have to announce  $\phi_a, \phi_b$  publicly to postselect the runs with the same random phase  $\phi_a = \phi_b$ . As is analyzed in Ref. [20], the random phase  $\phi_a, \phi_b$  is correlated to the key information, which can be utilized by Eve. To model the information leakage caused by random-phase announcement, consider the case where Alice and Bob share a pure state  $|\psi\rangle_{AB}$ . In a purified scenario, suppose a qubit register  $P$  is initialized in the state  $|+\rangle$ , then Alice and Bob realize  $\mathcal{E}$  with

$$\begin{aligned} |\Psi\rangle_{PAB} &= U(|+\rangle_P |\psi\rangle_{AB}), \\ &= \frac{1}{\sqrt{2}}\{|+\rangle_P |\psi\rangle_{AB} + |-\rangle_P [U_A(\pi) \otimes U_B(\pi)] |\psi\rangle_{AB}\}, \\ &= |0\rangle_P |\bar{\psi}_e\rangle_{AB} + |1\rangle_P |\bar{\psi}_o\rangle_{AB}, \\ &= \sqrt{p_e} |0\rangle_P |\psi_e\rangle_{AB} + \sqrt{p_o} |1\rangle_P |\psi_o\rangle_{AB}, \end{aligned} \quad (\text{B6})$$

where

$$\begin{aligned} |\bar{\psi}_e\rangle_{AB} &= \frac{1}{2} [|\psi\rangle_{AB} + (U_A \otimes U_B) |\psi\rangle_{AB}], \\ |\bar{\psi}_o\rangle_{AB} &= \frac{1}{2} [|\psi\rangle_{AB} - (U_A \otimes U_B) |\psi\rangle_{AB}]. \end{aligned} \quad (\text{B7})$$

Here  $|\bar{\psi}_e\rangle_{AB}, |\bar{\psi}_o\rangle_{AB}$  are unnormalized even and odd states, where  $p_e = \langle \bar{\psi}_e | \bar{\psi}_e \rangle$  and  $p_o = \langle \bar{\psi}_o | \bar{\psi}_o \rangle$ .

Therefore, the register  $P$  records whether  $\pi$  modulation is applied by  $X$ -basis state  $|\pm\rangle$ , while the parity information of the state is kept in the  $Z$ -basis state  $|0\rangle$  or  $|1\rangle$  of the register, as shown in the equation given above.

In this scenario, phase announcement can be interpreted as the following process: Alice and Bob prepare  $|\Psi\rangle_{PAB}$ , as a purification of  $\mathcal{E}(\sigma_{AB})$ , and measure system  $P$  on  $X$  basis, followed by announcing the result to Eve after the detection announcement. In a worse case, we can reduce the protocol to protocol Ib, where Eve holds the system  $P$  after her detection announcement.

To conclude, the PM QKD protocol can be realized by any initial state  $\sigma_{AB}$  with the assistance of a phase randomization, at the expense of losing the capability of distinguishing parity components.

## 2. PM QKD based on coherent state

So far, we do not make any assumption on the structure of initial state  $\sigma_{AB}$ . Here, we focus on one specific implementation. Due to the fact that coherent states are easy to implement in experiments, we set  $\sigma_{AB}$  as  $|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}e^{i\delta}\rangle_B$ . After the twirling phase randomization, the

state becomes

$$\begin{aligned} \rho &= \frac{1}{2} (|\sqrt{\mu_a}\rangle_A \langle\sqrt{\mu_a}| \otimes |\sqrt{\mu_b}e^{i\delta}\rangle_B \langle\sqrt{\mu_b}e^{i\delta}| \\ &\quad + |-\sqrt{\mu_a}\rangle_A \langle-\sqrt{\mu_a}| \otimes |-\sqrt{\mu_b}e^{i\delta}\rangle_B \langle-\sqrt{\mu_b}e^{i\delta}|) \\ &= p_{\text{even}} |\psi_e^\delta(\mu_a, \mu_b)\rangle_{AB} \langle\psi_e^\delta(\mu_a, \mu_b)| \\ &\quad + p_{\text{odd}} |\psi_o^\delta(\mu_a, \mu_b)\rangle_{AB} \langle\psi_o^\delta(\mu_a, \mu_b)|, \end{aligned} \quad (\text{B8})$$

where

$$\begin{aligned} |\psi_e^\delta(\mu_a, \mu_b)\rangle_{AB} &= \frac{1}{\sqrt{p_{\text{even}}}} (|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}e^{i\delta}\rangle_B \\ &\quad + |-\sqrt{\mu_a}\rangle_A \otimes |-\sqrt{\mu_b}e^{i\delta}\rangle_B), \\ |\psi_o^\delta(\mu_a, \mu_b)\rangle_{AB} &= \frac{1}{\sqrt{p_{\text{odd}}}} (|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}e^{i\delta}\rangle_B \\ &\quad - |-\sqrt{\mu_a}\rangle_A \otimes |-\sqrt{\mu_b}e^{i\delta}\rangle_B). \end{aligned} \quad (\text{B9})$$

Here the probabilities  $p_{\text{even}}, p_{\text{odd}}$  are the normalization factors. In the case where  $\delta = 0$ , the initial state is an unbiased mixing of  $|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}\rangle_B$  and  $|-\sqrt{\mu_a}\rangle_A \otimes |-\sqrt{\mu_b}\rangle_B$ , in which case the even and odd components are

$$\begin{aligned} \rho_e(\mu_a, \mu_b) &= \frac{1}{2} [|\psi_e^0(\mu_a, \mu_b)\rangle_{AB} \langle\psi_e^0(\mu_a, \mu_b)| \\ &\quad + |\psi_e^\pi(\mu_a, \mu_b)\rangle_{AB} \langle\psi_e^\pi(\mu_a, \mu_b)|], \\ \rho_o(\mu_a, \mu_b) &= \frac{1}{2} [|\psi_o^0(\mu_a, \mu_b)\rangle_{AB} \langle\psi_o^0(\mu_a, \mu_b)| \\ &\quad + |\psi_o^\pi(\mu_a, \mu_b)\rangle_{AB} \langle\psi_o^\pi(\mu_a, \mu_b)|]. \end{aligned} \quad (\text{B10})$$

Note that  $\rho_e(\mu_a, \mu_b)$  [ $\rho_o(\mu_a, \mu_b)$ ] is only comprised of even (odd)-photon Fock states, and therefore in even (odd) subspace.

In the final key distillation steps, we deal with the runs with  $\phi_a = \phi_b$  and  $|\phi_a - \phi_b| = \pi$  together, and the overall phase-error rate  $E^{\text{ph}}$  is given by the fraction of clicks caused by even components  $\rho_e(\mu_a, \mu_b)$ . To estimate the even clicks, we only need to estimate the yield  $Y_{\text{even}}$ , i.e., the detection probability when Alice and Bob send the state  $\rho_e(\mu_a, \mu_b)$ . The phase-error rate  $E^{\text{ph}}$  is

$$E^{\text{ph}} = \frac{p_{\text{even}} Y_{\text{even}}}{Q_{\mu_a, \mu_b}}. \quad (\text{B11})$$

Here, the only task remaining is to estimate  $Y_{\text{even}}$ , as  $Q_{\mu_a, \mu_b}$  given experiment parameters and data.  $p_{\text{even}}$  describes the proportion of even photon rounds, which relates to the intensities  $\mu_a, \mu_b$ .

### 3. Phase-error estimation and continuous randomization

As a common technique, the decoy-state method [31–33] can be applied to estimate the value of  $Y_{\text{even}}$ . The core of the decoy-state method is to use a set of testing states to learn Eve's behavior on specific components in the signal states. The decoy is based on the observation that, if the same components appear in both the (mixed) signal states and the (mixed) testing states, Eve cannot attack on them with different manners, in principle. In this section, we consider the asymptotic case with  $n \rightarrow \infty$ , so that there is no statistical fluctuation. The finite-size analysis is in Appendix C.

For the simplicity of discussion, we assume that  $\mu_a = \mu_b = \mu/2$ . The following argument can be easily generalized to the case when  $\mu_a \neq \mu_b$ . Denote the fraction of odd- and even-labeled clicked rounds as

$$q_{\text{odd}} = \frac{n_{\text{odd}}}{n}; q_{\text{even}} = \frac{n_{\text{even}}}{n}. \quad (\text{B12})$$

According to Eq. (B10), the signal source is combined by  $|\psi_e\rangle$  and  $|\psi_o\rangle$  with probability of  $p_{\text{even}}$  and  $p_{\text{odd}}$ ,

$$\rho = p_{\text{odd}}^\mu \rho_o \left( \frac{\mu}{2}, \frac{\mu}{2} \right) + p_{\text{even}}^\mu \rho_e \left( \frac{\mu}{2}, \frac{\mu}{2} \right), \quad (\text{B13})$$

Here we add superscript  $\mu$  to the probabilities and states, since they are the functions of  $\mu$ . The core is to estimate the detection probability of  $\rho_e(\mu/2, \mu/2)$ , namely, the yield  $Y_{\text{even}}^\mu$ .

The fraction of odd- and even-parity states in the final detected signal is given by

$$\begin{aligned} q_{\text{odd}}^\mu &= p_{\text{odd}}^\mu \frac{Y_{\text{odd}}^\mu}{Q_\mu}, \\ q_{\text{even}}^\mu &= p_{\text{even}}^\mu \frac{Y_{\text{even}}^\mu}{Q_\mu}, \end{aligned} \quad (\text{B14})$$

where  $Q_\mu$  is the total gain of the signals. For signals with intensity  $\mu$ , we have

$$Q^\mu = p_{\text{odd}}^\mu Y_{\text{odd}}^\mu + p_{\text{even}}^\mu Y_{\text{even}}^\mu. \quad (\text{B15})$$

To efficiently estimate  $q_{\text{odd}}$  and  $q_{\text{even}}$ , Alice and Bob adjust the intensity  $\mu$  of their prepared coherent lights. With constraints from different intensities,

$$\begin{aligned} Q^\mu &= p_{\text{odd}}^\mu Y_{\text{odd}}^\mu + p_{\text{even}}^\mu Y_{\text{even}}^\mu, \\ Q^\nu &= p_{\text{odd}}^\nu Y_{\text{odd}}^\nu + p_{\text{even}}^\nu Y_{\text{even}}^\nu, \end{aligned} \quad (\text{B16})$$

we have better estimation of  $Y_{\text{odd}}^\mu$  and  $Y_{\text{even}}^\mu$ . Note that  $Y_{\text{odd}}^\mu, Y_{\text{even}}^\mu$  is dependent on the intensity  $\mu$ . For different

signal intensities  $\mu, \nu$ , the difference of yield  $Y_{\text{odd}}^\mu, Y_{\text{even}}^\mu$  is bounded by

$$|Y_{\text{odd}}^\mu - Y_{\text{odd}}^\nu| \leq \sqrt{1 - F_{\mu\nu}^2}, \quad (\text{B17})$$

where  $F_{\mu\nu}$  is the fidelity between the odd state  $|\psi_o\rangle$  with intensities  $\mu$  and  $\nu$ , respectively,

$$F_{\mu\nu} = \text{Tr} \left[ \sqrt{\sqrt{\rho_{\text{odd}}^\mu} \rho_{\text{odd}}^\nu \sqrt{\rho_{\text{odd}}^\mu}} \right]. \quad (\text{B18})$$

In order to obtain a tighter bound on the estimation of  $Y_{\text{even}}^\mu$ , we can introduce extra phases other than  $\{0, \pi\}$  for coherent states  $|\sqrt{\mu/2}\rangle_A \otimes |\sqrt{\mu/2}\rangle_B$ . As an extreme case, one choice is to randomize the phase continuously from 0 to  $2\pi$ , i.e., continuous randomization. Note that, for a coherent state,

$$\frac{1}{2\pi} \int_0^{2\pi} d\phi |\sqrt{\mu} e^{i\phi}\rangle \langle \sqrt{\mu} e^{i\phi}| = \sum_{k=0}^{\infty} P_\mu(k) |k\rangle \langle k|, \quad (\text{B19})$$

where  $P_\mu(k) = e^{-\mu} (\mu^k / k!)$  is the proportion of Fock state  $|k\rangle$  in the mixed states.

If we randomize the phase of two coherent pulses simultaneously, for states with  $|\phi_a - \phi_b| = \delta$ , we have

$$\begin{aligned} \frac{1}{2\pi} \int_0^{2\pi} d\phi |\sqrt{\mu/2} e^{i\phi}\rangle_A \langle \sqrt{\mu/2} e^{i\phi}| \otimes |\sqrt{\mu/2} e^{i(\phi+\delta)}\rangle_B \\ \times \langle \sqrt{\mu/2} e^{i(\phi+\delta)}| = \sum_{k=0}^{\infty} P_\mu(k) |\bar{k}^\delta\rangle_{AB} \langle \bar{k}^\delta|, \end{aligned} \quad (\text{B20})$$

the  $k$ -photon state  $|\bar{k}^\delta\rangle_{AB}$  is

$$|\bar{k}^\delta\rangle_{AB} = \frac{(a^\dagger + e^{i\delta} b^\dagger)^k}{\sqrt{2^k k!}} |00\rangle_{AB}. \quad (\text{B21})$$

Consider the simultaneous randomization and the key-encoding process, the total phase difference of Alice and Bob's coherent state can be  $\phi_a = \phi_b$  or  $|\phi_a - \phi_b| = \pi$ , which indicates the mixed  $k$ -photon state, which is sent to Eve, is

$$\rho_k = \frac{1}{2} (|\bar{k}^0\rangle_{AB} \langle \bar{k}^0| + |\bar{k}^\pi\rangle_{AB} \langle \bar{k}^\pi|), \quad (\text{B22})$$

which is independent of the intensity  $\mu$ . In this case, the state Alice and Bob send out can be regarded as a probabilistic mixture of mixed  $k$ -photon state  $\rho_k$ . By directly

applying Lemma 2, we can estimate the phase error by

$$E^{\text{ph}} = \sum_{k=0}^{\infty} q_{2k}, \quad (\text{B23})$$

where  $q_k$  is the proportion of detection event caused by state  $\rho_{AB}$ , especially  $q_0$  corresponds to the vacuum signal detection, i.e., dark counts.

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

$$q_k^\mu = P^\mu(k) \frac{Y_k}{Q_\mu}. \quad (\text{B24})$$

The overall gain is given by

$$Q_\mu = \sum_{k=0}^{\infty} P^\mu(k) Y_k. \quad (\text{B25})$$

Similarly, we use the decoy-state method in the continuous randomization case, and there is a set of Eq. (B25) with different signal intensities  $\mu$  and corresponding proportion  $P^\mu(k)$ , which can be used to bound  $\{Y_k\}$ , therefore we can estimate  $E^{\text{ph}}$  efficiently.

The continuous phase-randomized protocol, named protocol III, is as follows.

### Protocol III

(1) State preparation: Alice and Bob prepare coherent states  $|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}\rangle_B$  on two optical modes  $A, B$ , at the beginning of each run. They initialize their qubits  $A', B'$  in  $|+\rangle$ . Alice applies the control gate  $C_{A'A}(U)$  to qubit  $A'$  and optical pulse  $A$ , and adds an extra random  $0 \sim 2\pi$  phase  $\phi_a$  on  $A$ . Similarly, Bob applies  $C_{B'B}(U)$ ,  $\phi_b$  to  $B'$  and  $B$ .

(2) Measurement: Alice and Bob send the two optical pulses  $A$  and  $B$  to an untrusted party, Eve, who is supposed to perform joint measurement and obtain the detection results  $L$  or  $R$ .

(3) Announcement: Eve announces the detection result or no successful detection for each round. After that, Alice and Bob announce their random phases and intensity settings  $\{\phi_a, \mu_a\}$  and  $\{\phi_b, \mu_b\}$  and keep the signals with  $|\phi_a - \phi_b| = 0$  or  $\pi$  and  $\mu_a = \mu_b$ .

(4) Sifting: When Eve announces an  $L$  or  $R$  click, Alice and Bob keep the qubits of systems  $A'$  and  $B'$ . In addition, Bob applies a Pauli  $X$ -gate to his qubit  $B'$  if Eve's announcement is  $R$  click. If  $|\phi_a - \phi_b| = \pi$ , Bob applies another Pauli  $X$  gate on  $B'$ .

Alice and Bob perform the above steps for many rounds and end up with a joint  $2n$ -qubit state  $\rho_{A'B'} \in (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})^{\otimes n}$ .

(5) Parameter estimation: Alice and Bob estimate the click ratio caused by even-state fractions by decoy-state methods.

(6) Key generation: For the signals with intensity  $\mu_a = \mu_b = \mu/2$ , Alice and Bob perform local  $Z$  measurements on  $\rho_{A'B'}$  to generate raw data strings  $\kappa_A$  and  $\kappa_B$ . They reconcile the key string to  $\kappa_A$  by an encrypted classical channel, with the consumption of  $l_{\text{EC}}$ -bit keys. After that, they perform privacy amplification according to the even-state ratio to generate keys.

## 4. Practical issues in PM QKD

In practice, to bound the phase error, we only need to bound the yield of single-photon components  $\rho_1$ ,

$$\rho_1 = \frac{1}{2}(|01\rangle_{AB} \langle 01| + |10\rangle_{AB} \langle 10|), \quad (\text{B26})$$

and the overall odd phase-error rate is bounded by

$$E^{\text{ph}} \leq 1 - q_1, \quad (\text{B27})$$

where  $q_1 = P_\mu(1)Y_1/Q_\mu$ .

To make the above protocol III practical, we now consider the following issues.

(1) From continuous phase randomization to discrete phase randomization. A continuous phase randomization and phase postselection is practically intractable. However, in practice, randomizing the phases of coherent pulses discretely is enough. For a coherent state  $|\sqrt{\mu}\rangle$ , if we randomize its phase discretely with  $\{\phi_j = (2\pi/D)j\}_{j=0}^{D-1}$ , the state can be expanded by a group of ‘‘pseudo’’ Fock states [36],

$$\frac{1}{D} \sum_{j=0}^{D-1} |\sqrt{\mu}e^{i\phi_j}\rangle_C \langle \sqrt{\mu}e^{i\phi_j}| = \sum_{k=0}^{D-1} P_D^\mu(k) |\lambda_k\rangle_C \langle \lambda_k|, \quad (\text{B28})$$

where

$$|\lambda_k\rangle_C = \frac{e^{-\mu/2}}{\sqrt{P^\mu(k)}} \sum_{l=0}^{\infty} \frac{(\sqrt{\mu})^{lD+k}}{\sqrt{(lD+k)!}} |lD+k\rangle_C, \quad (\text{B29})$$

$$P_D^\mu(k) = \sum_{l=0}^{\infty} \frac{\mu^{lD+k} e^{-\mu}}{(lD+k)!},$$

as we can see, when  $D$  becomes large,  $|\lambda_0\rangle$  and  $|\lambda_1\rangle$  will get close to the Fock state  $|0\rangle$  and  $|1\rangle$ .

Now we calculate the deviation of  $q_1$  caused by discrete phase randomization. Without loss of generality, we set  $|\phi_a - \phi_b| = \delta$ . After the discrete phase randomization,

the state is

$$\frac{1}{D} \sum_{j=0}^{D-1} \left| \sqrt{\frac{\mu}{2}} e^{i\phi_j} \right\rangle_A \left\langle \sqrt{\frac{\mu}{2}} e^{i\phi_j} \right| \otimes \left| \sqrt{\frac{\mu}{2}} e^{i(\phi_j+\delta)} \right\rangle_B \times \left\langle \sqrt{\frac{\mu}{2}} e^{i(\phi_j+\delta)} \right| = \sum_{k=0}^{\infty} P_D^\mu(k) |\bar{\lambda}_k^\delta\rangle_{AB} \langle \bar{\lambda}_k^\delta|, \quad (\text{B30})$$

the  $k$ -photon state  $|\bar{\lambda}_k^\delta\rangle_{AB}$  is

$$|\bar{\lambda}_k^\delta\rangle_{AB} = \frac{e^{-\mu/2}}{\sqrt{P_D^\mu(k)}} \sum_{l=0}^{\infty} \frac{(\sqrt{\mu})^{lD+k}}{\sqrt{(lD+k)!}} |\bar{l}D+k\rangle_{AB}, \quad (\text{B31})$$

where  $|\bar{l}D+k\rangle_{AB}$  is defined in Eq. (B21).

We compare the fidelity between  $|\bar{l}D+k\rangle_{AB}$  and  $|\bar{\lambda}_1^\delta\rangle_{AB}$ ,

$$\begin{aligned} |\langle \bar{l}D+k | \bar{\lambda}_1^\delta \rangle|^2 &= \frac{e^{-\mu}}{P_D^\mu(1)} \left| \sum_{l=0}^{\infty} \frac{(\sqrt{\mu})^{lD+1}}{(lD+1)!} \langle \bar{l}D+k | \bar{l}D+1 \rangle^\delta \right|^2, \\ &= \frac{e^{-\mu}}{P_D^\mu(1)} \mu, \\ &= \frac{e^{-\mu} \mu}{e^{-\mu} \left( \mu + \frac{\mu^{(D+1)}}{(D+1)!} + \frac{\mu^{(2D+1)}}{(2D+1)!} + \dots \right)}, \\ &= \frac{1}{1 + \frac{\mu^D}{(D+1)!} + \frac{\mu^{2D}}{(2D+1)!} + \dots}, \\ &\geq 1 - \frac{\mu^D}{(D+1)!}, \end{aligned} \quad (\text{B32})$$

the final inequality holds because  $[(n+1)D+1]! \geq (nD+1)!(D+1)!$  for  $n \geq 1$ . Note that the fidelity is independent of the phase difference  $\delta$ .

Therefore, according to Eq. (B17), the yield difference of  $|\bar{l}D+k\rangle_{AB}$  and  $|\bar{\lambda}_1^\delta\rangle_{AB}$  is bounded by

$$|Y_1 - Y_{\lambda_1}^\mu| \leq \sqrt{1 - |\langle \bar{l}D+k | \bar{\lambda}_1^\delta \rangle|^2} \leq \sqrt{\frac{\mu^D}{(D+1)!}}, \quad (\text{B33})$$

then the difference between estimated  $|\bar{\lambda}_1^\delta\rangle_{AB}$  fraction, denoted by  $q_1$  and  $q_{\lambda_1}^\mu$ , is bounded by

$$\begin{aligned} |q_1 - q_{\lambda_1}^\mu| &\leq P_D^\mu(1) \frac{|Y_1 - Y_{\lambda_1}^\mu|}{Q_\mu} \leq \frac{P_D^\mu(1)}{Q_\mu} \sqrt{\frac{\mu^D}{(D+1)!}} \\ &= \frac{\xi_D(\mu)}{Q_\mu}, \end{aligned} \quad (\text{B34})$$

note that  $\xi_D(\mu) \equiv P_D^\mu(1) \sqrt{\mu^D/(D+1)!} \approx (\mu^{D/2+1} e^{-\mu}) / \sqrt{(D+1)!}$ , which is only correlated to the signal intensity

$\mu$  and discrete phase number  $D$ . Therefore, we can compare the ratio  $\xi_D(\mu)/Q_\mu$ , which illustrates the deviation of the estimated  $q_1$  from the real  $q_{\lambda_1}^\mu$ .

If we set  $D = 16$ , then  $\xi_D(\mu) \approx \mu^9 e^{-\mu} / \sqrt{17!}$ , which is a tiny value when  $\mu < 1$ , compared to the gain  $Q_\mu \approx \eta\mu$ , where  $\eta$  is the channel transmittance from Alice or Bob to the middle point Eve. Therefore, we can safely ignore the effect caused by discrete phase randomization and borrow the former decoy-state method based on continuous phase randomization [32,39].

(2) Key generation and parameter estimation with signals where the phases are not aligned.

In protocol III, only the states with aligned phases  $|\phi_a - \phi_b| = 0, \pi$  and the same intensity  $\mu_a = \mu_b$  are post-selected to estimate the detections caused by single-photon components and generate keys. This will cause a huge waste on sifting in a practical finite-size case. We now discuss how to use these signals for key generation and parameter estimation.

First, we notice that for signals with  $\mu_a = \mu_b = \mu/2$  and  $|\phi_a - \phi_b| = \delta, \delta + \pi$ , we can regard it as a specific case of protocol III, where Alice and Bob originally share a state  $|\sqrt{\mu_a}\rangle_A \otimes |\sqrt{\mu_b}e^{i\delta}\rangle_B$ . According to Eq. (B21), the mixed  $k$ -photon state when  $|\phi_a - \phi_b| = \delta, \delta + \pi$  is

$$\rho_k^\delta = \frac{1}{2} (|\bar{k}^\delta\rangle_{AB} \langle \bar{k}^\delta| + |\bar{k}^{\delta+\pi}\rangle_{AB} \langle \bar{k}^{\delta+\pi}|). \quad (\text{B35})$$

In general, the  $k$ -photon state is correlated with the misaligned phase  $\delta$ , which implies that states with different mismatched phases have different mixed  $k$ -photon states. However, this state is not true for  $k = 1$ , where the single-photon state,

$$\rho_1^\delta = \frac{1}{2} (|01\rangle_{AB} \langle 01| + |10\rangle_{AB} \langle 10|), \quad (\text{B36})$$

is independent of the misaligned phase. Therefore, states with different unaligned phases have the same single-photon component, which indicates that we can use all of the states to estimate the yield of the single-photon component, regardless of the misaligned phase  $\delta$ . The phase error can be bounded by

$$E^{\text{ph}} \leq 1 - q_1. \quad (\text{B37})$$

Based on this observation, during the postprocessing, Alice and Bob first reconcile their sifted raw key bits  $K_a$  and  $K_b$  for each group  $j_s = j_a - j_b$  separately. If the error rate in a group of data is too large, they can simply discard that group. Denote the group set  $J$  to be the set of remaining phase-group indexes  $\{j_s\}$ . That is, if  $j_s \in J$ , then the phase group  $j_s$  is kept for key generation. They then estimate the even-photon fraction  $q_{\text{even}}$  for all the remaining data in  $J$  and perform privacy amplification.



In a more general scenario, Alice and Bob can estimate the yield of states  $|01\rangle_{AB}$  and  $|10\rangle_{AB}$ , denoted as  $Y_{01}$  and  $Y_{10}$ , respectively. The overall yield  $Y_1$  can be calculated by

$$Y_1 = \frac{1}{2}(Y_{01} + Y_{10}). \quad (\text{B38})$$

Similar to the traditional MDI QKD [14,40,41], Alice and Bob can use signals with different intensities to achieve a better estimation on  $Y_1$ . However, in this paper, to simplify the discussion, we focus on the signals with  $\mu_a = \mu_b$ , and leave the better estimation for future works.

(3) From infinite decoy-state analysis to the finite decoy-state setting.

In practice, with finite data size, we can use only finite rounds for testing. To accurately bound the even-state components, we have to use the testing states with finite intensity settings.

We explicitly analyze this problem in Appendix C. As a result, we show that Alice and Bob can use only vacuum + weak decoy state, similar to the BB84 decoy-state analysis [39].

With all the factors taken into consideration, the practical version of protocol III, named protocol IV, is presented as below.

#### **Protocol IV**

(1) State preparation: Alice prepares coherent state  $|\sqrt{\mu_a}e^{i\phi_{ja}}\rangle_A$  on optical mode  $A$ , with  $\mu_a \in \{0, \nu/2, \mu/2\}$ , and  $\phi_{ja} \in \{(2\pi/D)j_a\}_{j_a=0}^{D-1}$ . She initializes her qubit  $A'$  in  $|+i\rangle$ . She applies the control gate  $C_{A'A}(U)$  to qubit  $A'$  and optical pulse  $A$ . Similarly, Bob prepares  $|\sqrt{\mu_b}e^{i\phi_{jb}}\rangle_B$  on optical mode  $B$ . He initializes his qubit  $B'$  in  $|+\rangle$ . He applies the control gate  $C_{B'B}(U)$  to qubit  $B'$  and optical pulse  $B$ .

(2) 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.

(3) Announcement: Eve announces the detection result or no successful detection for each round. After that, Alice and Bob announce their random phases and intensity settings  $\{j_a, \mu_a\}$  and  $\{j_b, \mu_b\}$  and keep the signals with  $\mu_a = \mu_b$ .

(4) Sifting: When Eve announces an  $L$  or  $R$  click, Alice and Bob keep the qubits of systems  $A'$  and  $B'$ . In addition, Bob applies a Pauli  $X$  gate to his qubit  $B'$  if Eve's announcement is  $R$  click. If  $3D/4 > [(j_a - j_b) \bmod D] \geq D/4$ , Bob applies another Pauli  $X$  gate on  $B'$ .

Alice and Bob perform the above steps for many rounds and end up with a joint  $2n$ -qubit state  $\rho_{A'B'} \in (\mathcal{H}_{A'} \otimes \mathcal{H}_{B'})^{\otimes n}$ .

(5) Parameter estimation: For all the raw data that they have retained, Alice and Bob record the detect number  $M_{i_a, i_b}^{(j_s)}$  of different intensity combinations  $\{\mu_{i_a}, \mu_{i_b}\}$  and phase groups  $j_s$ . They then estimate the information leakage  $E_\mu^{\text{ph}}$  using Eq. (B27).

(6) Key generation: For the signals with intensity  $\mu_a = \mu_b = \mu/2$ , Alice and Bob perform local  $Z$  measurements on  $\rho_{A'B'}$  to generate raw data strings  $\kappa_A$  and  $\kappa_B$ . They first group the signals by  $j_s = \min[(j_a - j_b) \bmod D, (j_b - j_a) \bmod D]$ . After that, they keep the signals with  $j_s$  in a set  $J$ . They reconcile the corresponding key string to  $\kappa_A$  by an encrypted classical channel, with the consumption of  $l_{\text{EC}}^s$ -bit keys according to  $j_s$ . After that, they perform privacy amplification according to the estimated single-photon ratio  $q_1$  to generate keys.

The key rate of this protocol is

$$r = \frac{2}{D} \sum_{j_s \in J} \left[ 1 - H(E^{\text{ph}}) - l_{\text{EC}}^s \right]. \quad (\text{B39})$$

Typically,  $l_{\text{EC}}^s$  can be replaced by  $fH(E^{j_s})$ , where  $f$  is error-correction efficiency and  $E^{j_s}$  is bit error rate for each phase group  $j_s$  that is in  $J$ .  $E^{\text{ph}}$  is the phase-error rate bounded by Eq. (B37).

Following Shor and Preskill [6], we can move the measurement before the sifting step, in which case  $C - \pi$  rotation is replaced by the bit flip operation. Then protocol IV reduces to PM QKD protocol in the paper.

#### **PM QKD**

(1) State preparation: Alice randomly generates a key bit  $\kappa_a$ , and picks a random phase  $\phi_{ja}$  from the set  $\{j_a \frac{2\pi}{D}\}_{j_a=0}^{D-1}$ , and the intensity  $\mu_{i_a}$  from  $\{0, \nu/2, \mu/2\}$ . She then prepares the coherent state  $|\sqrt{\mu_{i_a}}e^{i(\phi_{ja} + \pi\kappa_a)}\rangle_A$ . Similarly, Bob generates  $\kappa_b$ ,  $\phi_{jb}$ ,  $\mu_{i_b}$  and then prepares  $|\sqrt{\mu_{i_b}}e^{i(\phi_{jb} + \pi\kappa_b)}\rangle_B$ .

(2) 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.

(3) Announcement: Eve announces the detection result for each round. After that, Alice and Bob announce their random phases and intensity settings  $\{j_a, \mu_a\}$  and  $\{j_b, \mu_b\}$  and keep the signals with  $\mu_a = \mu_b$ .

(4) Sifting: When Eve announces a successful detection, (a click from exactly one of the detectors  $L$  or  $R$ ), Alice and Bob keep  $\kappa_a$  and  $\kappa_b$ . Bob flips his key bit  $\kappa_b$  if Eve's announcement is an  $R$  click. Then, Alice and Bob group the signals by  $j_s = (j_a - j_b) \bmod D$ . If  $j_s \in [D/4, 3D/4)$ , Bob flips his key bit  $\kappa_b$ . After that, Alice and Bob merge the data with  $j_s$  and  $j_s + D/2$ , with  $j_s = 0, 1, \dots, D/2 - 1$ .

(5) Parameter estimation: For all the raw data that they have retained, Alice and Bob record the detect number  $M_{i_a, i_b}^{(j_s)}$  of different intensity combinations  $\{\mu_{i_a}, \mu_{i_b}\}$  and phase groups  $j_s$ . They then estimate the information leakage  $E_\mu^{\text{ph}}$  using Eq. (B27).

(6) Key generation: For the signals with  $\mu_{i_a} = \mu_{i_b} = \mu/2$ , Alice and Bob group them by the phase index  $j_s = \min[(j_a - j_b) \bmod D, (j_b - j_a) \bmod D]$ . After that, they keep the signals with  $j_s$  in a set  $J$ . They reconcile the corresponding key string to  $\kappa_A$  by an encrypted classical channel, with the consummation of  $l_{\text{EC}}^s$ -bit keys according to  $j_s$ . After that, they perform privacy amplification according to the estimated single-photon ratio  $q_1$  to generate keys.

### APPENDIX C: FINITE DATA-SIZE ANALYSIS

In this section, we analyze the finite-size effect of the PM QKD protocol introduced in the main text. Here we ignore the effect caused by discrete phase randomization. Recall that during the postprocessing in PM QKD, Alice and Bob first reconcile their sifted raw key bits  $K_a$  and  $K_b$  for each phase group  $j_s = j_a - j_b$  separately. They keep some of the phase groups  $j_s \in J$  for key generation. They then estimate the single-photon fraction  $q_1^j$  for all the remaining data in  $J$  and perform privacy amplification.

As mentioned in the main text, in QKD finite-size analysis, one should take the cost and failure probability of channel authentication, error verification, privacy amplification, and parameter estimation into account. However, the cost of the first three steps is negligible in comparison to the one in parameter estimation. When the final key length is much larger than 37 bits, one can ignore the corresponding failure probability with a constant secret-key cost [10]. For simplicity, we ignore these parts in our analysis. The finite-size key length  $N_k$  is then

$$N_k = \sum_{j \in J} M_{\text{si}}^j [1 - H(E^{\text{ph}}) - fH(E^j)], \quad (\text{C1})$$

with the failure probability of  $\epsilon_{\text{eph}}$ . Here  $M_{\text{si}}^j$  is the sifted raw key length of phase group  $j$  before error verification and privacy amplification,  $f$  is the error-correction efficiency,  $E^j$  is the quantum bit error rate of group  $j$ ,  $E^{\text{ph}}$  is the estimated upper bound of phase-error rate bounded by

$$E^{\text{ph}} < 1 - q_1^j = 1 - \frac{M_1^{\mu J}}{M^{\mu J}}, \quad (\text{C2})$$

with a failure probability of  $\epsilon_{\text{eph}}$ . Here  $M^{\mu J}$  is the click round number with  $\mu_a = \mu_b = \mu/2$  and phase group  $j_s \in J$ , and  $M_1^{\mu J}$  is the estimated single-photon component in it.

The core of parameter estimation of  $E^{\text{ph}}$  is to estimate the clicked rounds caused by the single-photon component  $M_1^{\mu J}$ , for all the clicked rounds with  $\mu_a = \mu_b = \mu/2$  and

all the left phase group  $J$ . Here, we follow Ref. [37] for a tight decoy-state analysis in the finite-data regime.

As stated in Appendix 4, since the single-photon state  $\rho_1$  is the same whatever  $\phi_a$  and  $\phi_b$  is, we can first estimate the single-photon clicks  $M_1^\mu$  caused by all the phase groups with different  $j_d$  all together, and then estimate  $M_1^{\mu J}$  for the left groups  $J$  afterwards.

Without matching the random phase  $\phi_a, \phi_b$  by  $j_s$ , the state on optical modes  $A, B$  sent out to Eve when  $\mu_a = \mu_b = \mu/2$  is

$$\rho_{AB} = \sum_k P^\mu(k) \rho_k^{\text{tot}}, \quad (\text{C3})$$

where

$$\rho_k^{\text{tot}} = \int_0^\pi d\delta \rho_k^\delta = \sum_{k_a, k_b} B\left(k_a; k, \frac{1}{2}\right) |k_a, k_b\rangle \langle k_a, k_b|, \quad (\text{C4})$$

and  $B(k; n, p) = \binom{n}{k} p^k (1-p)^{(n-k)}$  is the binomial distribution.  $\rho_k^\delta$  is given by Eq. (B35). Note that  $\rho_1^{\text{tot}} = \rho_1$ . For different intensities  $\{0, \nu, \mu\}$ , the  $k$ -photon component  $\rho_k^{\text{tot}}$  are the same, following Poisson distribution with different parameters. Therefore, the former finite-size decoy-state analysis on the BB84 protocol can be directly applied to PM QKD.

For each intensity  $\{0, \nu, \mu\}$ , suppose Alice and Bob send out  $N^{\text{vac}}, N^w, N^s$  rounds of pulses, with  $M^{\text{vac}}, M^w, M^s$  rounds of effective clicks, respectively. We have

$$\begin{aligned} N^{\text{vac}} &\approx (r^{\text{vac}})^2 N, \\ N^w &\approx (r^w)^2 N, \\ N^s &\approx (r^s)^2 N. \end{aligned} \quad (\text{C5})$$

A unified notation is  $\{N^a, M^a\}$ , with  $a \in \{\text{vac}, w, s\}$  indicating the intensity setting of vacuum, weak, and signal. Denote the normalized rate of each intensity setting  $a$  in the final clicked signals as

$$q^a = N^a / N, \quad (\text{C6})$$

note that,  $q^a$  is a fixed number after Alice and Bob send out all the signals.

For a specific intensity setting  $a \in \{\text{vac}, w, s\}$ , denote the rounds of sending out  $k$ -photon pulses  $\rho_k^{\text{tot}}$  and clicks caused by it as  $\{N_k^a, M_k^a\}$ . Define

$$N_k \equiv \sum_a N_k^a, \quad (\text{C7})$$

to be the overall rounds to send  $k$ -photon signals. Denote the conditional probability that Alice and Bob choose the

intensity setting  $a$  when sending out the  $k$ -photon signal as

$$p(a|k) = \lim_{N_k \rightarrow \infty} \frac{N_k^a}{N_k} \quad (\text{C8})$$

$$= \frac{q^a P^a(k)}{q^{\text{vac}} P^0(k) + q^w P^w(k) + q^s P^s(k)},$$

where we slightly abuse the notation  $P^a(k)$  to denote the Poisson distribution with intensity setting  $a$ .

Therefore, we have

$$N^a = \sum_k N_k^a \approx \sum_k p(a|k) N_k, \quad (\text{C9})$$

$$M^a = \sum_k M_k^a \approx \sum_k p(a|k) M_k,$$

where  $p(\text{vac}|k) = 0$  for all  $k \neq 0$ .

In the whole QKD process, the values  $\{N^a\}_a$  and  $\{M^a\}_a$  are known by Alice and Bob. The values  $\{N_k^a\}_{a,k}$  are available to Alice and Bob, in principle, and cannot be controlled by Eve. The values  $\{M_k\}_k$  are, however, controlled by Eve and unknown to Alice and Bob.

The core observations to perform finite-size analysis in this case are as follows.

(1) When Alice and Bob send out  $k$ -photon signals, the choosing of a different intensity setting  $a$  is independent and identically distributed (i.i.d.), given by the probability distribution  $p(a|k)$ .

(2) Eve's attack on  $k$ -photon signals cannot depend on the intensity setting  $a$ .

Therefore, Eve's attack can be described by a random sampling from the set of  $N_k$ . She randomly chooses  $M_k$  rounds from it and announces them as effective clicks. Among them,  $\{M_k^a\}_a$ , i.e., the clicks caused by different intensity settings, are randomly distributed.

To clarify the random-sampling model, we can then rewrite  $M_k^a$  as

$$\bar{M}_k^a = \sum_{i=1}^{M_k} (\bar{\chi}_k^a)_i, \quad (\text{C10})$$

where

$$(\bar{\chi}_k^a)_i = \begin{cases} 1 & \text{with probability } p_k^a, \\ 0 & \text{with probability } 1 - p_k^a, \end{cases} \quad (\text{C11})$$

(with  $i = 1, \dots, M_k$ ) are i.i.d. indicator random variables.

Group these random variables and define

$$\bar{M}^a = \sum_k \bar{M}_k^a = \sum_k \sum_{i=1}^{M_k} (\bar{\chi}_k^a)_i, \quad (\text{C12})$$

as the variable indicating the overall clicks caused by intensity setting  $a$ . The bar on  $M_k^a$  is used to indicate that it is a variable.

The decoy-state problem can be modeled as *for the unknown*  $\{M_k\}_k$  *and the known*  $\{p_k^a\}_{a,k}$ , *to evaluate the value of the variable*  $\bar{M}_1^s$ , *given the observed constraints that*  $\{\bar{M}^a = M^a\}_a$ .

We first observe that,

$$\mathbb{E}(\bar{M}_k^a) = p(a|k) M_k, \quad (\text{C13})$$

and hence

$$\mathbb{E}(\bar{M}^a) = \sum_k \mathbb{E}(\bar{M}_k^a) = \sum_k p(a|k) M_k. \quad (\text{C14})$$

Note that, *the expectation values are taken with respect to the i.i.d. variables*  $\{(\bar{\chi}_i^a)_j\}_{a,i,j}$ . Therefore, we can bound the expected values  $\mathbb{E}(\bar{M}^a)$  by applying an inversed form of the Chernoff bound on Eq. (C12) and with the observed  $\{M^a\}_a$ . From Eq. (C14), we have

$$\mathbb{E}^U(\bar{M}^a) \geq \sum_k p(a|k) M_k \geq \mathbb{E}^L(\bar{M}^a), \quad (\text{C15})$$

where we use superscripts  $U$  and  $L$  to denote upper and lower bounds, respectively.

To estimate  $M_1^s$ , we first estimate  $M_1$  from Eq. (C15), and then estimate  $M_1^s$  by direct use of the Chernoff bound on Eq. (C10). We briefly summarize the results of the Chernoff bound in Appendix 1.

The decoy method discussed above is based on Eq. (C14) and the correlation between variables  $\{\bar{M}^a, M_k\}$ . To unify it with the former decoy-state formulas with  $\{Q^a, Y_k\}$ , we further define the gain and yield variable as

$$\bar{Q}^a := \frac{\bar{M}^a}{N^a}, \quad (\text{C16})$$

$$Y_k^* := \frac{M_k}{N_k^\infty},$$

where

$$N_k^\infty = \sum_a P^a(k) N^a = \sum_a P^a(k) (r^a)^2 N, \quad (\text{C17})$$

is the expectation value of  $N_k$ .

From Eq. (C14) and the definition of  $\bar{Q}^a, \bar{Y}_k^*$  in Eq. (C16), we can recover the decoy-state formula expressed by  $\bar{Q}^a$  and  $\bar{Y}_k^*$ ,

$$\begin{aligned}\mathbb{E}[\bar{Q}^a] &= \frac{\mathbb{E}[\bar{M}^a]}{N^a} = \frac{\sum_k P(a|k)M_k}{N^a} \\ &= \sum_k \frac{q^a P^a(k)}{q^{\text{vac}}P^0(k) + q^w P^w(k) + q^s P^s(k)} \frac{M_k}{q^a N} \\ &= \sum_k P^a(k) \frac{M_k}{N [q^{\text{vac}}P^0(k) + q^w P^w(k) + q^s P^s(k)]}, \\ &= \sum_k P^a(k) \frac{M_k}{N^{\infty}}, \\ &= \sum_k P^a(k) Y_k^*.\end{aligned}\quad (\text{C18})$$

Now, with the observed value  $M^a$ , we can calculate  $\bar{Q}^a$ , and apply the decoy-state formulas,

$$\mathbb{E}^U[\bar{Q}^a] \geq \sum_k P^a(k) Y_k^* \geq \mathbb{E}^L[\bar{Q}^a]. \quad (\text{C19})$$

With Eq. (C19), we can estimate  $Y_1^*$  by Ref. [37]

$$\begin{aligned}Y_1^* \geq (Y_1^*)^L &= \frac{\mu}{\mu\nu - \nu^2} \left( \mathbb{E}^L[Q^w]e^\nu - \mathbb{E}^U[Q^s]e^\mu \frac{\nu^2}{\mu^2} \right. \\ &\quad \left. - \frac{\mu^2 - \nu^2}{\mu^2} \mathbb{E}^U[Q^{\text{vac}}] \right).\end{aligned}\quad (\text{C20})$$

Note that the whole process can be divided into two steps. Step I is to estimate  $(Y_1^*)^L$  and  $(M_1)^L$  for all of the phase groups. Step II is to estimate  $(M_1^{s,J})^L$  for phase-group set  $J$  from  $(M_1)^L$  in all phase groups. To summarize, the whole phase-error estimation process is as follows.

(1) (Data recording) To record  $\{N^s, N^w, N^{\text{vac}}\}$  and record the number of clicked rounds  $\{M^s, M^w, M^{\text{vac}}\}$ .

(2) (Chernoff estimation I) Based on an inversed usage of the Chernoff bound, to calculate  $\{\mathbb{E}^U(\bar{M}^a), \mathbb{E}^L(\bar{M}^a)\}_a$ , given  $M^a$  and estimate the failure probability  $\epsilon_1$ . Calculate the  $\{\mathbb{E}^U(\bar{Q}^a), \mathbb{E}^L(\bar{Q}^a)\}_a$  by Eq. (C16).

(3) (Decoy estimation) Calculate the lower bound  $(Y_1^*)^L$  based on  $\{\mathbb{E}^U(\bar{Q}^a), \mathbb{E}^L(\bar{Q}^a)\}_a$  by Eq. (C20). Calculate  $(M_1)^L$  by Eq. (C16).

(4) (Chernoff estimation II) Based on a direct usage of the Chernoff bound, to calculate  $(M_1^{s,J})^L$  for phase-group set  $J$  and estimate the failure probability  $\epsilon_2$ . To calculate  $E^{\text{ph}}$  based on Eq. (C2). The overall failure probability is  $\epsilon_{\text{eph}} = \epsilon_1 + \epsilon_2$ .

## 1. Chernoff bound

Here we present the methods to evaluate  $\mathbb{E}(\bar{M}^a)$  from  $M^a$  and evaluate  $M_1^s$  from  $M_1$  using Chernoff bounds.

To evaluate  $\mathbb{E}(\bar{M}^a)$  from  $M^a$ , we inversely use the Chernoff bounds based on Bernoulli variables. We briefly summarize the results in Ref. [37]. For the observed value  $\chi$ , we set the lower and upper bound of estimated  $\mathbb{E}(\chi)$  as  $\{\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)\}$ . Denote

$$\begin{aligned}\mathbb{E}^L(\chi) &= \frac{\chi}{1 + \delta^L}, \\ \mathbb{E}^U(\chi) &= \frac{\chi}{1 - \delta^U}.\end{aligned}\quad (\text{C21})$$

The failure probability of the estimation  $\mathbb{E}(\chi) \in [\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)]$ , given by the Chernoff bound, is

$$\epsilon = e^{-\chi g_2(\delta^L)} + e^{-\chi g_2(\delta^U)}, \quad (\text{C22})$$

where  $g_2(x) = \ln(1+x) - x/(1+x)$ .

To evaluate  $M_1^s$  from  $M_1$ , we directly apply the Chernoff bounds. Suppose the direct sampling expectation value of  $M_1^s$  is given by  $\mathbb{E}(M_1^s) = p_1^s M_1$ . For the expected value  $\mathbb{E}(\chi)$ , we set the lower and upper bound of the estimated  $\chi$  as  $\{\chi^L, \chi^U\}$ . Denote

$$\begin{aligned}\chi^L &= (1 - \delta^L)\mathbb{E}(\chi), \\ \chi^U &= (1 + \delta^U)\mathbb{E}(\chi).\end{aligned}\quad (\text{C23})$$

The failure probability of the estimation  $\chi \in [\chi^L, \chi^U]$ , given by the Chernoff bound, is

$$\epsilon = e^{-(\delta^L)^2 \mathbb{E}(\chi)/(2+\delta^L)} + e^{-(\delta^U)^2 \mathbb{E}(\chi)/(2+\delta^U)}. \quad (\text{C24})$$

In practice, we can preset the lower bound and upper bound  $\{\mathbb{E}^L(\chi), \mathbb{E}^U(\chi)\}$  or  $\{\chi^L, \chi^U\}$  by assuming a Gaussian distribution on  $\chi$  first,

$$\begin{aligned}\mathbb{E}^L(\chi) &= \chi - n_\alpha \sqrt{\chi}, & \mathbb{E}^U(\chi) &= \chi + n_\alpha \sqrt{\chi}, \\ \chi^L &= \chi - n_\alpha \sqrt{\mathbb{E}(\chi)}, & \chi^U &= \chi + n_\alpha \sqrt{\mathbb{E}(\chi)},\end{aligned}\quad (\text{C25})$$

where  $n_\alpha$  is a preset parameter to determine the estimation precision. After that, we calculate the failure probabilities by Eqs. (C22) and (C24).

## APPENDIX D: SIMULATION FORMULA AND RESULTS

Here we list the formulas used to simulate the key-rate performance of PM QKD and MDI QKD in Fig. 2 in the main text. The channel is modeled to be a pure loss one and symmetric for Alice and Bob with transmittance  $\eta$  (with the detector efficiency  $\eta_d$  taken into account).



### 1. Gain, yield, and error rate of PM QKD

In PM QKD, suppose Alice and Bob emit the  $k$ -photon light  $\rho_k^\delta$  in Eq. (B35), the yield (i.e., effective detection probability)  $Y_k$  is given by [cf. Eq. (B13) in Ref. [20]],

$$Y_k \approx 1 - (1 - 2p_d)(1 - \eta)^k, \quad (\text{D1})$$

suppose Alice and Bob emit the coherent states  $\rho$  in Eq. (B8) with  $\mu_a = \mu_b = \mu/2$ , the gain (i.e., effective detection probability)  $Q_\mu$  is [cf. Eq. (B14) in Ref. [20]]

$$Q_\mu \approx 1 - (1 - 2p_d)e^{-\eta\mu}. \quad (\text{D2})$$

As stated in the main text, the quantum bit error rate  $E^{js}$  is mainly composed of three components. The first one is the intrinsic error  $e_\Delta(j_s)$  caused by phase mismatch when  $j_s \neq 0$ ,

$$e_\Delta(j_s) = \begin{cases} \sin^2\left(\frac{\pi j_s}{D}\right), & j_s \leq \frac{D}{2}, \\ \sin^2\left(\frac{\pi}{2} - \frac{\pi j_s}{D}\right), & j_s > \frac{D}{2}, \end{cases} \quad (\text{D3})$$

which is related to the index deviation  $j_s$ . The second one is the extra misalignment error  $e_0$ , caused by phase fluctuation. Here we regard  $e_0$  and  $e_\Delta(j_s)$  as being caused by independent factors, and the overall misalignment error is  $e_d(j_s) = e_0 + e_\Delta(j_s)$ . Also, the dark-count effect will contribute to the bit error. The overall bit error rate  $E_\mu^{(j_s)}$  is then

given by [cf. Eq. (B22) in Ref. [20]]

$$E_\mu^{(j_s)} = [p_d + \eta\mu(e_\Delta(j_s) + e_0)] \frac{e^{-\eta\mu}}{Q_\mu}, \quad (\text{D4})$$

where  $p_d$  is the dark-count rate.

Similarly, the overall bit error rate for the  $k$ -photon light can be estimated by [cf. Eq. (B20) in Ref. [20]]

$$e_k^{(j_s)} = \frac{p_d(1 - \eta)^k + [e_\Delta(j_s) + e_0][1 - (1 - \eta)^k]}{Y_k} \quad (\text{D5})$$

when the phase deviation  $\delta$  belongs to group  $j_s$ .

The key-rate formula is listed in Eq. (10) of the main text. In the original PM QKD analysis, the phase-error rate  $E^X$  is bounded by [cf. Eq. (C3) in Ref. [20]]

$$E_\mu^X \leq q_0 e_0^Z + (q_1 e_1^Z + q_3 e_3^Z + q_5 e_5^Z) + (1 - q_0 - q_1 - q_3 - q_5). \quad (\text{D6})$$

### 2. Simulation formulas for MDI QKD protocols

The key rate of MDI QKD is [14]

$$R_{\text{MDI}} = \frac{1}{2} \{ Q_{11} [1 - H(e_{11})] - f Q_{\text{rect}} H(E_{\text{rect}}) \}, \quad (\text{D7})$$

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. [35]. In simulation, the gain and error rates are

$$Y_{11} = (1 - p_d)^2 \left[ \frac{\eta_a \eta_b}{2} + (2\eta_a + 2\eta_b - 3\eta_a \eta_b) p_d + 4(1 - \eta_a)(1 - \eta_b) p_d^2 \right],$$

$$e_{11} = e_0 Y_{11} - (e_0 - e_d)(1 - p_d^2) \frac{\eta_a \eta_b}{2},$$

$$Q_{\text{rect}} = Q_{\text{rect}}^{(C)} + Q_{\text{rect}}^{(E)}, \quad (\text{D8})$$

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

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

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

where  $\mu'$  denotes the average number of photons reaching Eve's beam splitter,  $\mu_a = \mu_b = \mu/2$ ,  $\eta_a = \eta_b = \eta$ , and

$$\begin{aligned} \mu' &= \eta_a \mu_a + \eta_b \mu_b, \\ x &= \frac{1}{2} \sqrt{\eta_a \mu_a \eta_b \mu_b}. \end{aligned} \quad (\text{D9})$$

We take these formulas from Eqs. (A9), (A11), (B7), and (B28)–(B31) in Ref. [35].

The linear key-rate bound of repeaterless point-to-point QKD protocol used in the main text is [18]

$$R_{\text{PLOB}} = -\log_2(1 - \eta). \quad (\text{D10})$$

### 3. Comparison of PM QKD key rates

Here, we compare PM QKD performance in our analysis with the previous analysis [20] in the asymptotic case. The channel and detector parameters are listed in the main

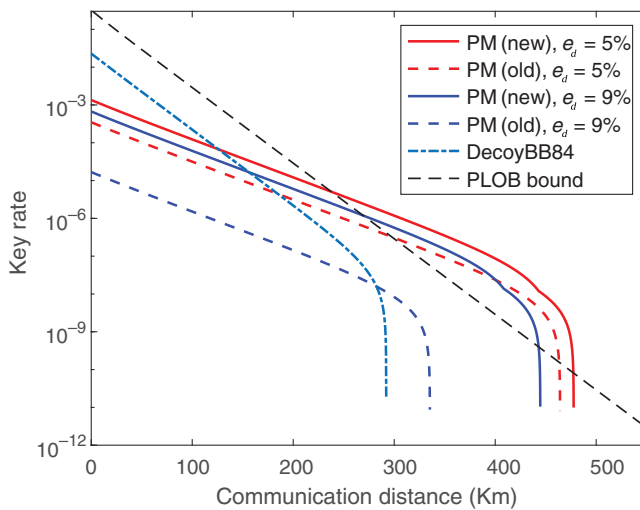


FIG. 7. Comparison of PM QKD performance with the previous analysis [20] and our results. We set the typical intrinsic misalignment error rates to be 5 and 9%.

text. In Fig. 7, we show the comparison results when the misalignment error  $e_d(0)$  is 5 and 9%. Clearly, our analysis makes PM QKD more robust against the noise.

- [1] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, NY, 1984), p. 175.
- [2] Artur K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [4] D. Mayers, Unconditional security in quantum cryptography, *J. ACM (JACM)* **48**, 351 (2001).
- [5] H. K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
- [6] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [7] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim, in *Theory of Cryptography*, edited by Joe Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), p. 386.
- [8] Renato Renner and Robert König, in *Theory of Cryptography: Second Theory of Cryptography Conference*, edited by Joe Kilian (Springer Berlin Heidelberg, Berlin, Heidelberg, 2005), p. 407.
- [9] Renato Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **6**, 1 (2008).
- [10] Chi-Hang Fred Fung, Xiongfeng Ma, and H. F. Chau, Practical issues in quantum-key-distribution postprocessing, *Phys. Rev. A* **81**, 012318 (2010).
- [11] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, Security of quantum key distribution with imperfect devices, *Quantum Inf. Comput.* **4**, 325 (2004).
- [12] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* **73**, 022320 (2006).
- [13] Bing Qi, Chi-Hang Fred Fung, Hoi Kwong Lo, and Xiongfeng Ma, Time-shift attack in practical quantum cryptosystems, *Quantum Inf. Comput.* **7**, 73 (2007).
- [14] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-Device-Independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [15] 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).
- [16] L.-M. Duan, M. D. Lukin, J. Ignacio Cirac, and Peter Zoller, Long-distance quantum communication with atomic ensembles and linear optics, *Nature* **414**, 413 (2001).
- [17] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo, All-photon quantum repeaters, *Nat. Commun.* **6**, 6787 (2015).
- [18] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [19] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [20] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou, Phase-Matching Quantum Key Distribution, *Phys. Rev. X* **8**, 031043 (2018).
- [21] Jie Lin and Norbert Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [22] Kento Maeda, Toshihiko Sasaki, and Masato Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, *Nat. Commun.* **10**, 3140 (2019).
- [23] Kiyoshi Tamaki, Hoi-Kwong Lo, Wenyuan Wang, and Marco Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, arXiv:1805.05511 (2018).
- [24] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu, Sending or not sending: Twin-field quantum key distribution with large misalignment error, arXiv: 1805.09222 (2018).
- [25] Chaohan Cui, Zhen-Qiang Yin, Rong Wang, Wei Chen, Shuang Wang, Guang-Can Guo, and Zheng-Fu Han, Twin-Field Quantum Key Distribution Without Phase Postselection, *Phys. Rev. Appl.* **11**, 034053 (2019).
- [26] Marcos Curty, Koji Azuma, and Hoi-Kwong Lo, Simple security proof of twin-field type quantum key distribution protocol, *npj Quantum Inf.* **5**, 1 (2019).
- [27] Charles H. Bennett, Quantum Cryptography Using any Two Nonorthogonal States, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [28] Agnes Ferenczi, Security proof methods for quantum key distribution protocols, Ph.D. thesis (2013).
- [29] M. Koashi, Simple security proof of quantum key distribution based on complementarity, *New J. Phys.* **11**, 045018 (2009).
- [30] Toshihiko Sasaki, Yoshihisa Yamamoto, and Masato Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* **509**, 475 (2014).

- [31] Won-Young Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [32] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [33] Xiang-Bin Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [34] Hua-Lei Yin and Zeng-Bing Chen, Coherent-state-based twin-field quantum key distribution, *Sci. Rep.* **9**, 1 (2019).
- [35] Xiongfeng Ma and Mohsen Razavi, Alternative schemes for measurement-device-independent quantum key distribution, *Phys. Rev. A* **86**, 062319 (2012).
- [36] Zhu Cao, Zhen Zhang, Hoi-Kwong Lo, and Xiongfeng Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, *New J. Phys.* **17**, 053014 (2015).
- [37] Zhen Zhang, Qi Zhao, Mohsen Razavi, and Xiongfeng Ma, Improved key-rate bounds for practical decoy-state quantum-key-distribution systems, *Phys. Rev. A* **95**, 012333 (2017).
- [38] Thomas M. Cover and Joy A. Thomas, *Elements of Information Theory* (John Wiley & Sons, Hoboken, New Jersey, 2012).
- [39] Xiongfeng Maa, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, Practical decoy state for quantum key distribution, *Phys. Rev. A* **72**, 012326 (2005).
- [40] Xiongfeng Ma, Chi-Hang Fred Fung, and Mohsen Razavi, Statistical fluctuation analysis for measurement-device-independent quantum key distribution, *Phys. Rev. A* **86**, 052305 (2012).
- [41] Marcos Curty, Feihu Xu, Wei Cui, Charles Ci Wen Lim, Kiyoshi Tamaki, and Hoi-Kwong Lo, Finite-key analysis for measurement-device-independent quantum key distribution, *Nat. Commun.* **5**, 3732 (2014).