Phase-matching quantum key distribution

Xiongfei Ma, Pei Zeng, and Hongyi Zhou
Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China
(Dated:)

Abstract—Quantum key distribution (QKD) is the most successful application in the quantum information science, whose security was proved in the end of the last century [3–5]. Since then, there has been a tremendous interest in developing this quantum technology for real-life applications, starting from the first 32-cm demonstration in the early 1990s [6] to the recent satellite QKD over 1200 km [7].

Introduction: The bottleneck throttling its real-life applications lies in the limited communication distance and key generation speed, due to the fact that the information carrier can be easily lost in the channel. For all the current implementations, the key rate is bounded by the channel transmission probability, $\eta$. Rather surprisingly, by matching the phases of two coherent states and encoding the key information into the common phase, this linear key-rate constraint can be overcome — the secure key rate scales with the square root of the transmission probability, $O(\sqrt{\eta})$. To achieve this, we develop an optical-mode-based security proof that is different from the conventional qubit-based security proofs. Furthermore, the proposed scheme is measurement-device-independent, i.e., it is immune to all possible detection attacks. The simulation result shows that the key rate can even exceed the transmission probability $\eta$ between two communication parties. In addition, we apply phase post-compensation to devise a practical version of the scheme without phase-locking, which makes the proposed scheme feasible with the current technology. This means that quantum key distribution can enjoy both sides of the world — practicality and security.

I. INTRODUCTION

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

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

The following two approaches to overcome this rate limit have been considered, quantum repeaters [12–14] and trusted relays. Unfortunately, using quantum repeater schemes with current technology is infeasible because they require high-quality quantum memory and complicated local entanglement distillation operations. The trusted-relay approach, however, relies on the assumption that the quantum relays between two users are trustworthy, which is difficult to ensure or verify practically; this severely undermines the primary goal of QKD, i.e., security. In 2012, the measurement-device-independent quantum key distribution (MDI-QKD) scheme is proposed to close all the detection loopholes [15], which enhances the security of a practical QKD system. Nevertheless, the key rate of MDI-QKD scheme is still bounded by $O(\eta)$. Therefore, the linear key rate bound [10, 11] was widely believed to hold for practical QKD systems without relays.

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

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

II. PM-QKD PROTOCOL

In PM-QKD, the two communication parties, Alice and Bob, both send a phase-randomized coherent pulse to an untrusted Eve, who is expected to perform interference detection. Eve obtains a successful detection when one and only one of the two detectors clicks, denoted by $L$-click and $R$-click, thus revealing that the relative phase of the coherent pulses $A$ and $B$ is either 0 or $\pi$. Then, Alice and Bob match the phases of pulses by post-selection. In a way, the key information is encoded in the “global phase” of the two coherent pulses, which is expected to be secret to Eve. The PM-QKD scheme is detailed below and shown in Fig. [1].

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

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

Announcement: Eve announces her detection results. Then, Alice and Bob announce the random phases $\phi_a$ and $\phi_b$, respectively.

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

Parameter estimation: For all the raw data that they have retained, Alice and Bob analyze the gains $Q_\mu$ and quantum bit error rates $E_\mu^X$. They then estimate $E_\mu^X$ using Eq. (2).

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

Notations: denote a coherent state in mode $A$ to be $|\sqrt{\mu}e^{i\phi}\rangle_A$, where $\mu$ is the intensity and $\phi$ is the phase; $\mu_a = \mu_b = \mu/2$; Alice’s (Bob’s) key bit $\kappa_a(b) \in \{0, 1\}$; total gain $Q_\mu$; phase error rate $E_\mu^X$; and bit error rate $E_\mu^Z$.

The above implementation of our PM-QKD protocol clearly resembles the phase-encoding MDI-QKD protocol [17, 18], where the key bits are encoded in the relative phase of two coherent pulses (the reference and signal pulses). However, in the PM-QKD protocol, the reference pulse can be regarded as being shared by Alice and Bob. Therefore, they no longer need to send the reference pulse, and the key becomes the global phase of the coherent signal pulses. Another significant difference between PM-QKD and the former phase encoding MDI-QKD scheme is that no basis switching is required. In this respect, it resembles the Bennett-1992 [20], and passive DPS [21] QKD protocols.

III. SECURITY OF PM-QKD

To provide an intuitive understanding of the manner in which PM-QKD works, we demonstrate its security by considering an equivalent scenario shown in Fig. [1(b)]. Here, a trusted party (Charlie) prepares a pure state $|\Psi\rangle_C$, splits it using a 50–50 beam splitter, and sends to Alice and Bob separately. Alice and Bob encode their key information, $\kappa_a$ and $\kappa_b$, into systems $A$ and $B$ by modulating the phases, and then send these to Eve who is supposed to tell whether $|\kappa_a - \kappa_b| = 0$ or 1. Thus, the four possible output states that could be sent to Eve can be expressed as $|\Psi_{0,0}\rangle$, $|\Psi_{0,\pi}\rangle$, $|\Psi_{1,0}\rangle$, and $|\Psi_{1,\pi}\rangle$.

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

In our PM-QKD protocol, both Alice and Bob transmit weak coherent pulses, $|\sqrt{\mu_a}e^{i(\phi_a + \pi\kappa_a)}\rangle_A$ and $|\sqrt{\mu_b}e^{i(\phi_b + \pi\kappa_b)}\rangle_B$, to Eve. The phase-matching condition $\phi_a = \phi_b = \phi$ is equivalent to imagining that Charlie employs a source state of $|\Psi\rangle_C = |\sqrt{\mu}e^{i\phi}\rangle_C$ in Fig. [1(b)]. For
a phase-randomized state \( |\sqrt{p} e^{i\phi} \rangle_C \), it is equivalent for Charlie to prepare a Fock state \( |\Psi\rangle_C = |k\rangle_C \) with a probability of \( P(k) = e^{-\mu_Q^Z} k! \). Thus, the PM-QKD protocol is secure if Eve cannot learn the phase \( \phi \). However, in the real PM-QKD protocol, the phase \( \phi \) will eventually be announced during the sifting process. When this happens, Charlie’s source \( |\Psi\rangle_C \) can no longer be regarded as combinations of different photon-number states \( |k\rangle_C \). The key challenge of the security proof of PM-QKD lies in the fact that the quantum source cannot be regarded as a mixture of photon number states, after Alice and Bob announce the phases, \( \phi_a \) and \( \phi_b \). That is, the photon number channel model \[19\] and the “tagging” method used in the GLLP security proof \[22\] cannot be applied here any more. In Appendix C, a beam-splitting attack is proposed to show that the GLLP formula is incorrect after the phase announcement. Therefore, one cannot simply reduce a randomized-phase coherent state protocol to a single-photon-based protocol.

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

\[
r_{PM} \geq 1 - H(E^Z_\mu) - H(E^X_\mu),
\]

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

\[
E^X_\mu \leq e^Z_0 q_0 + \sum_{k=0}^{\infty} e^Z_{k+1} q_{2k+1} + (1-q_0 - \sum_{k=0}^{\infty} q_{2k+1}).
\]

Here, \( q_k \) is the estimated ratio of the “k-photon signal” to the full detected signal:

\[
q_k = \frac{(e^{-\mu_Q^Z} k!/k!) Y_k}{Q_\mu},
\]

where \( Q_\mu \) is the total gain of the pulses, and \( Y_k \) and \( e^Z_\mu \) are the yield and bit error rate, respectively, if Charlie’s light source is a \( k \)-photon number state. Alice and Bob can estimate the yield and bit error rate via the decoy-state method \[23\]-\[25\]. Note that the parameters \( Y_k \) and \( e^Z_\mu \) can still be used to characterize Eve’s behaviour even though the source is not actually a combination of photon-number states.

Unlike the existing security analysis of discrete-variable QKD, our analysis is not single-qubit-based. For a long time, the sources in QKD implementations, such as weak coherent sources and spontaneous parametric down-conversion sources, have been fabricated as an approximation of single qubit, following the BB84 protocol \[1\]. Here, we show the security of PM-QKD with a coherent light source by directly applying the Lo-Chau entanglement distillation argument \[4\] on analyzing the
IV. PRACTICAL IMPLEMENTATION

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

To address these practical issues, we employ a phase post-compensation method [15], where Alice and Bob first divide the phase interval $[0, 2\pi)$ into $M$ slices $\{\Delta_j\}$ for $0 \leq j \leq M-1$, where $\Delta_j = [2\pi j/M, 2\pi (j+1)/M)$. Instead of comparing the exact phases, Alice and Bob only compare the slice indexes. This makes the phase sifting step practical, but introduces an intrinsic misalignment error. Besides, Alice and Bob do not perform the phase sifting immediately in each round, and instead, they do it in data postprocessing. In the parameter estimation step, they perform the following procedures, as shown in Fig. 2.

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

2. (Phase post-compensation method) Given an offset compensation $j_d \in \{0, 1, \ldots, M/2 - 1\}$, Bob sifts the sampled bits with the phase matching condition $|j_b + j_d - j_a| \mod M = 0$ or $M/2$. For the case of $M/2$, Bob flips the key bit $\kappa_b$. After sifting, Bob calculates the QBER $E_\mu$ with Alice’s sampling key bits. Bob tries all possible $j_d \in \{0, 1, \ldots, M-1\}$, and figures out the proper $j_d$ to minimize the sampling QBER. Using the phase matching condition with the proper $j_d$, Bob sifts (and flips if needed) the unsampled bits and announces the locations to Alice. Alice sifts her key bits accordingly.

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

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

An alternative method to phase post-compensation is that, Alice and Bob can generate strong pulses independent of quantum signals for phase calibration. The two pulses are interfered at the measurement site so that Alice and Bob can identify the phase fluctuations between two channels. Note that the strong pulses can be set in an optical mode slightly deviated from the quantum signals to reduce cross-talks. According to the phase difference measured from the strong calibration pulses, Alice and Bob can estimate the offset $j_d$ accurately. This is a feasible way to replace the phase post-compensation method.

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

- Alice and Bob first generate strong laser pulses with (unknown) randomized phases, either by turning on/off the lasers or active phase randomization. They then split the pulses and apply homodyne detection on one beam to measure the phase \( \phi_a, \phi_b \) accurately enough to determine the slice indexes \( j_a, j_b \). They use the rest beam for further quantum encoding.
- Alice and Bob first generate pulses with stable phases. Then, they actively randomize the phase using phase modulators. Alice and Bob can record the corresponding random numbers as for slice indexes \( j_a, j_b \). Note that the phase randomization can be discrete, which has been proven to be secure and efficient with a few discrete phases [28].

With such methods, the final key rate formula can be expressed as:

\[
R_{PM} \geq 2 \frac{2}{M} Q_\mu [-f H(E^Z_\mu) + 1 - H(E^X_\mu)],
\]

where the phase error rate \( E^X_\mu \) is given by Eq. (2), \( 2/M \) is the sifting factor and \( f \) is the error correction efficiency.

V. SIMULATION RESULTS

We simulate the performance of PM-QKD with the parameters given in Fig. 3(b), assuming a lossy channel that is symmetrical for Alice and Bob. The dark count rate \( p_d \) is from the work [29], and the other parameters are set to be typical values. The simulation formulas for \( Q_\mu, E^Z_\mu \) and \( E^X_\mu \) of PM-QKD are given in Eq. (B14), (B22), and (B27) in Appendix B2, respectively. The simulation formulas for BB84 and MDI-QKD are listed in Appendix B3.

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

Several QKD schemes are compared in Fig. 3(c). The comparison shows that the PM-QKD scheme outperforms the existing protocols in the following aspects. First, the PM-QKD scheme has a quadratic improvement of key rate, \( O(\sqrt{\eta}) \). In security aspect, PM-QKD enjoys the measurement-device-independent nature that is immune to all detection attacks. In practical aspect, it removes the requirement of basis switch, which can simplify the experiment apparatus and reduce the randomness consumption.

Note that the security of recently proposed twin-field QKD protocol [10] can be reduced to the security of PM-QKD protocol if the two bases \( X,Y \) information is ignored in twin-field QKD. It remains an open problem whether we can reach a higher key rate by taking advantage of the basis information together.

VI. OUTLOOK

To enhance the performance of PM-QKD, there are a few interesting directions. First, there may be a room for improvement on security analysis. In above discussions, PM-QKD is treated as a single-basis scheme with phase randomization. In a dual viewpoint, we can regard the different global phases \( \phi_a, \phi_b \) as different bases, and naturally the phase matching step as basis sifting. This is interesting, since it shows the advantage of QKD using multi-nonorthogonal bases. Moreover, this multi-bases view may help us to generalize the phase-matching scheme to, for example, a polarization-based one.

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

Third, we bound the total phase error \( E^X_\mu \) by pessimistically considering the phase errors \( e^X_\mu \) for even photon number components to be 1 in Eq. (A33), as shown in Appendix A3. There may be a scope to improve the bound of total phase error \( E^X_\mu \). For example, the twophoton error \( e^Z_2 \) and \( e^Z_2 \) can be better estimated with more decoy states, which leads to tighter bounds of \( E^X_\mu \).

Finally, since we can overcome the key rate linear bound, it is interesting to investigate a repeater-less secret key capacity bound for QKD; for example, whether it is possible to push the key rate to \( R = O(\eta^{1/3}) \) or \( O(\eta^{1/4}) \) without repeaters.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China Grant No. 11674193 and the National Key R&D Program of China (2017YFA0303900, 2017YFA0304004). We thank T. Chen, M. Lucamarini, and F. Xu for enlightening discussion, especially T. Chen for providing the alternative methods for compensating the phase reference difference.
Appendix A: Security Proof of PM-QKD

In this section, we provide a security proof for the PM-QKD protocol via entanglement distillation [30]. Note that the existing security proofs of discrete-variable QKD assume qubit (or qudit) states transmitted through the channel. Here, we develop a new security proof by exploring continuous optical modes directly.

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

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

$$|k\rangle_A \equiv \frac{(a^\dagger)^k}{\sqrt{k!}} |0\rangle_A,$$  \hspace{2cm} (A1)

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

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

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

$$P(k) = e^{-\mu} \frac{\mu^k}{k!},$$  \hspace{2cm} (A3)

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

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

\begin{table}[h]
\begin{tabular}{|c|c|c|c|c|c|}
\hline
Protocol & PM & TF & MDI & passive DPS & B92 \\
\hline
Key rate & $O(\sqrt{\eta})$ & $O(\sqrt{\eta})^*$ & $O(\eta)$ & $O(\eta^2)$ & \ \\
Detection loophole & No & No* & No & Yes & Yes \\
Qubit based & No & Yes & Yes & Yes & Yes \\
Basis switch & No & Yes & Yes & No & No \\
Phase locking & No & Yes & No & No & No \\
\hline
\end{tabular}
\end{table}

FIG. 3. (a) Simulation of our PM-QKD protocol. For the considered simulation parameters, the key rate of PM-QKD surpasses that of the conventional BB84 protocol when $l > 120$ km and it exceeds the SKC bound [17] when $l > 250$ km. In addition, our protocol is also able to achieve a long transmission distance of $l = 450$ km. (b) Parameters used for simulation. (c) Comparison of different QKD protocols: phase-matching (PM) QKD; twin-field (TF) QKD [16]; measurement-device-independent (MDI) QKD [15]; passive differential phase-shift (DPS) QKD [21]; Bennett-1992 (B92) QKD [20]. Key rate: dependence of the key rate on the channel transmittance $\eta$. Detection loophole: whether the protocol is immune to all detection loopholes; Qubit based: whether the security analysis is based on the single-qubit case; Basis switch: whether the source (measurement device) must prepare (measure) states in complementary bases; Phase locking: whether the protocol requires a fixed phase reference frame for the two users. *The security and performance of twin-field QKD can be reduced to our phase-matching scenario if the basis information $X, Y$ is ignored.
\[ |\alpha_{\text{odd}}\rangle_A = \frac{1}{2\sqrt{c_{\text{odd}}}} (|\alpha\rangle_A - |-\alpha\rangle_A) \]
\[ = \frac{1}{\sqrt{c_{\text{odd}}}} e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha)^{2k+1}}{(2k+1)!} |2k+1\rangle_A, \]
\[ |\alpha_{\text{even}}\rangle_A = \frac{1}{2\sqrt{c_{\text{even}}}} (|\alpha\rangle_A + |-\alpha\rangle_A) \]
\[ = \frac{1}{\sqrt{c_{\text{even}}}} e^{-\frac{1}{2}|\alpha|^2} \sum_{k=0}^{\infty} \frac{(\alpha)^{2k}}{(2k)!} |2k\rangle_A, \]

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

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

Denote the photon number measurement \( \{M_k\}_k \) as
\[ M_k \equiv |k\rangle_A \langle k| . \]

Denote the parity measurement \( \{M_{\text{odd}}, M_{\text{even}}\} \) as
\[ M_{\text{odd}} = \sum_{k=0}^{\infty} |2k+1\rangle_A \langle 2k+1| , \]
\[ M_{\text{even}} = \sum_{k=0}^{\infty} |2k\rangle_A \langle 2k|. \]

For a beam splitter (BS), we express the input optical modes as A, B with creation operators \( a^\dagger, b^\dagger \), respectively, and the output optical modes as C, D, with creation operators \( c^\dagger, d^\dagger \), respectively. The BS transforms modes A and B to C and D according to
\[ \begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix} . \]

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

A control-phase gate, \( C_{\pi} \), from a qubit \( A' \) to an optical mode A, is defined as
\[ C_{\pi} \equiv |0\rangle_{A'} \langle 0| \otimes U_A(0) + |1\rangle_{A'} \langle 1| \otimes U_A(\pi), \]

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

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

1. The quantum states transmitted in the channel are the same.
2. All announced classical information is the same.
3. Alice and Bob perform the same measurement on the same quantum states to obtain the raw key bits.
4. Alice and Bob use the same postprocessing to extract secure key bits.

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

**1. Security proof via entanglement distillation**

Here, we briefly review the security proof based on entanglement distillation [1] [2]. Suppose that in QKD, Alice generates an \( l \)-bit key string \( S \), and Bob generates an estimate of the key string \( S' \). Denote the space of \( S \) as \( S \), whose dimension is \( 2^l \). An adversary, Eve, attempts to learn about \( S \) from the information leakage.

After QKD, Alice and Bob should share the same key privately. A key \( S \) is called correct, if \( S' = S \) for any strategy of Eve, and is called \( \epsilon_{\text{cor}} \)-correct, if
\[ Pr[S' \neq S] \leq \epsilon_{\text{cor}}. \]

To define a private key, consider the quantum state \( \rho_{AE} \) that describes the correlation between Alice’s classical key \( S \) and Eve’s system \( E \) (for any attacks). A key \( S \) is called \( \epsilon_{\text{sec}} \)-private from \( E \) if [31] [32]
\[ \min_{\sigma_E} \frac{1}{2} ||\rho_{AE} - \omega_A \otimes \sigma_E||_1 \leq \epsilon_{\text{sec}}. \]

where \( \omega_A = (|S\rangle \langle S|)_A \sum_{S'=0}^{2^{l}-1} |S'\rangle \langle S'| = \) the equally mixed key state over all possible keys in space \( S \) and \( || \cdot ||_1 \) is the trace norm. A QKD protocol is called secure if the generated key is both correct and private. It is called \( \epsilon \)-secure if the generated key is \( \epsilon_{\text{cor}} \)-correct and \( \epsilon_{\text{sec}} \)-private with \( \epsilon = \epsilon_{\text{cor}} + \epsilon_{\text{sec}} \).

Here, we consider the case where Alice and Bob share an \( m \)-pair-of-qubits gigantic state \( \rho_{AB}^{(m)} \). If we can show that
\[ F((\rho_{AB}^{(m)}), |\Phi_{AB}^{(m)}\rangle) \geq \sqrt{1 - \epsilon_l^2} \]
where \( |\Phi_{AB}^{(m)}\rangle \) is the state of \( m \) perfect EPR pairs \( |\Phi^{+}\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \), and \( 0 \leq \epsilon_l \leq 1 \). Then it can be shown that it is \( \epsilon_l \)-private and \( \epsilon_l \)-correct, then it is \( 2\epsilon_l \)-secure. That is, to show the security of a QKD protocol, we only need to show that the state for key extraction \( \rho_{AB}^{(m)} \), is close to the perfect EPR pairs \( |\Phi_{AB}^{(m)}\rangle \). Here is the intuition of the Lo-Chau security proof [4]. Suppose Alice and Bob share an \( n \)-pair-of-qubit gigantic
state, $\rho_{(n)}^{A'B'}$, at the beginning. If they perform an efficient entanglement distillation protocol (EDP) to distill $m$ EPR pairs, then they will be able to share nearly $m$ bit correct and private keys. Now the task becomes how to find the right EDP.

Bennett, DiVincenzo, Smolin, and Wootters (BDSW) show that [30], if an $n$-pair-of-qubit state $\rho_{(n)}^{A'B'}$ can be written as a classical mixture of Bell state products,

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

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

(A13)

where $|\Phi_{b_i}^{(i)}\rangle$ is one of the four Bell states labeled by $b_i \in \{0,1,2,3\}$ on the $i$-th qubit, then one can distill entanglement by employing EDPs. In the one-way hashing method [30], a specific type of one-way EDP, Alice measures a series of commuting operators based on some random-hashing matrix on her $n$ qubits, and sends the results to Bob. Bob measures the same operators on his $n$ qubits and infers the locations and types of the errors from the difference in the measurement results. After that, Alice and Bob correct the errors and obtain $m$ ($m \leq n$, almost perfect) EPR pairs.

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

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

$$W = \sum_{b_1,b_2,...,b_n} |b_1,b_2,...,b_n\rangle \langle b_1,b_2,...,b_n| .$$

(A14)

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

In the Shor-Preskill security proof [5], the one-way EDP protocol is reduced to a “prepare-and-measure” QKD protocol, by employing the CSS code [38]. Later, other techniques of decoupling $X$-error correction and $Z$-error correction are introduced for this reduction. For a one-way EDP protocol based on the CSS code, the distillation rate of EPR pairs, $r \equiv \lim_{n \to \infty} m/n$, is given by,

$$r = 1 - H(E_Z) - H(E_X),$$

(A15)

where $E_Z$ and $E_X$ are the $Z$-error rate and $X$-error rate, respectively, and $H(x) = -x \log_2 x - (1 - x) \log_2 (1 - x)$ is the binary Shannon entropy function. The error rates can be defined as measurement results on $\rho_{(n)}^{A'B'}$:

$$E_Z \equiv Tr \left( \sum_{j=1}^{n} \frac{1}{2} (1 - Z_{A'}^{(j)} \otimes Z_{B'}^{(j)} \rho_{(n)}^{A'B'}) \right) ,$$

$$E_X \equiv Tr \left( \sum_{j=1}^{n} \frac{1}{2} (1 - X_{A'}^{(j)} \otimes X_{B'}^{(j)} \rho_{(n)}^{A'B'}) \right) ,$$

(A16)

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

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

2. Entanglement-based PM-QKD protocol

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

Protocol I

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

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

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

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

5. Parameter estimation: after many rounds of the above steps, Alice and Bob end up with a joint $2n$-qubit state, denoted by $\rho_{(n)}^{A'B'}$. They then perform random sampling on the remaining $\rho_{(n)}^{A'B'}$ to estimate $E_Z$ and infer $E_X$ by Eq. (A15).
by Charlie is a parity state, namely, $\rho$ is realized by a Hadamard gate followed by the $Z$-basis measurement. Here, we denote the $Z$-basis measurements on $A$ or $B$ as $\rho_{A}$ or $\rho_{B}$, respectively.

In Protocol I, for $\rho \in D(\mathcal{H}^{C}_{\text{odd}})$ or $\rho \in D(\mathcal{H}^{C}_{\text{even}})$, then the $X$-error rate and $Z$-error rate are given by $e_{odd}$ and $e_{even}$, respectively, and similarly, denote for an even state $\rho_{even}$ as $e_{even}$.\n
**Lemma 1.** In Protocol I, for $\rho \in D(\mathcal{H}^{C}_{\text{odd}})$, $e_{odd} = e_{odd}$; and for $\rho \in D(\mathcal{H}^{C}_{\text{even}})$, $e_{even} = 1 - e_{even}$.

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

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

The joint state on system $A', B', A, B$ before the $C_{\pi}$ operations is

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

After the $C_{\pi}$ operations, this state becomes,

$$|\Psi_{0}^{(k)}\rangle = \begin{cases} \frac{1}{2\sqrt{2^{k}k!}}(|00\rangle + |11\rangle)_{A'B'}(a^\dagger + b^\dagger)^k |00\rangle_{AB} + i(|01\rangle - |10\rangle)_{A'B'}(a^\dagger - b^\dagger)^k |00\rangle_{AB}, & \text{if } k \text{ is odd,} \\ \frac{1}{2\sqrt{2^{k}k!}}(|00\rangle - |11\rangle)_{A'B'}(a^\dagger + b^\dagger)^k |00\rangle_{AB} + i(|01\rangle + |10\rangle)_{A'B'}(a^\dagger - b^\dagger)^k |00\rangle_{AB}, & \text{if } k \text{ is even.} \end{cases} \hfill (A19)$$

As shown in Fig. 4(b), the $X$-basis measurement on $A'$ or $B'$ is realized by a Hadamard gate followed by the $Z$-basis measurement. Denote the state after local Hadamard gates as $|\Psi_{HH}^{(k)}\rangle \equiv (H_{A'} \otimes H_{B'}) |\Psi_{0}^{(k)}\rangle$, then,
In other words, the $X$-error rate, $e^X_k$, can be understood as the error rate by performing the $Z$-basis measurement on the state of $|\Psi^{(k)}_{HH}\rangle$. The relation between the $X$- and $Z$-error rates can be obtained by comparing Eqs. (A19) and (A20). For the odd-photon-number case, since $|\Psi^{(2k+1)}_{HH}\rangle = |\Psi^{(2k+1)}_{HH}\rangle$, we have $e^X_{2k+1} = e^Z_{2k+1}$. For the even-photon-number case, since $|\Psi^{(2k)}_{HH}\rangle = I^X \otimes Y^{B'} |\psi^{(2k)}\rangle$, we have $e^X_{2k} = 1 - e^Z_{2k}$.

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

$$|\Psi^{(\text{odd})}_0\rangle = \sum_k c_{2k+1} |\psi^{(2k+1)}_0\rangle,$$

(A21)

After local Hadamard gates, the state becomes $|\Psi^{(\text{odd})}_{HH}\rangle = (H^A \otimes H^{B'}) |\psi^{(\text{odd})}_{HH}\rangle$. From Eq. (A19), (A20) and (A22), we can see that $|\Psi^{(\text{odd})}_{HH}\rangle = |\psi^{(\text{odd})}_{HH}\rangle$, and hence $e^Z_{\text{odd}} = e^Z_{\text{odd}}$. With the same argument, we have $e^Z_{\text{even}} = 1 - e^Z_{\text{even}}$.

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

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

$$\rho_{\text{even}} = \sum_i p_i |\psi^{(i)}_{\text{even}}\rangle \langle \psi^{(i)}_{\text{even}}|,$$

(A22)

This is equivalent that Charlie sends out $|\psi^{(i)}_{\text{odd(even)}}\rangle$ with probability $p_i$. For each pure state component, we have $e^Z_{\text{odd(i)}} = e^Z_{\text{odd(i)}}$ and $e^X_{\text{even(i)}} = 1 - e^Z_{\text{even(i)}}$. Thus the relations hold for all (mixed) parity states.

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

$$\rho = p_{\text{odd}} \rho_{\text{odd}} + p_{\text{even}} \rho_{\text{even}},$$

(A23)

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

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

$$E^X = q_{\text{odd}} e^X_{\text{odd}} + q_{\text{even}} e^X_{\text{even}} = q_{\text{odd}} e^Z_{\text{odd}} + q_{\text{even}} (1 - e^Z_{\text{even}}).$$

(A24)

Here, the parameters $q_{\text{odd}}, q_{\text{even}}, e^Z_{\text{odd}}$, and $e^Z_{\text{even}}$ can be evaluated according to Charlie’s parity announcement. When the parity information is missing, Alice and Bob need to estimate these parameters, which will be described later in Section A.5

3. Coherent state protocol and equivalent process

From Protocol I to the PM-QKD protocol, there are a few practical issues need to be addressed. First, the trusted party Charlie and the BS should be removed. In order to do this, we consider a special case where Charlie prepares a coherent state $|\sqrt{\mu}\rangle_C$, as the photon source. In addition, Charlie adds a random phase $\phi \in \{0, \pi\}$ with equal probabilities to the coherent state, the density matrix can be written as,

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

$$= c_{\text{odd}} |\alpha_{\text{odd}}\rangle \langle \alpha_{\text{odd}}| + c_{\text{even}} |\alpha_{\text{even}}\rangle \langle \alpha_{\text{even}}|,$$

(A25)

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

Now, Alice and Bob want to prepare the state given in Eq. (A25) without Charlie’s assistance. They first locally prepare two coherent states, $|\sqrt{\mu/2}\rangle_{A(B)}$, and add a same random phase $\phi \in \{0, \pi\}$ to their states, as shown in Fig. 5(b). Then, the state becomes,
Appropriately, $\rho_{AB}(\sqrt{\mu}, -\sqrt{\mu})$ is the state after $\rho(\alpha, -\alpha)$ defined in Eq. (A25) going through the BS. Thus, this new protocol (Protocol II) is equivalent to Protocol I with the input state $\rho(\sqrt{\mu}, -\sqrt{\mu})$.

**Protocol II** runs as follows, as shown in Fig. 5(b).

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

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

3. **Announcement**: Eve announces the detection result, $L/R$-click or failure, for each round.

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

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

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

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

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

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

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

We shall remove the simultaneous phase randomisation requirement in Section A4 bound $q_{odd}, q_{even}, e^Z_{odd}$ and $e^Z_{even}$ in Section A3 and remove the phase-locking requirement in Section A6.

---

**FIG. 5.** (a) A specific realization of Protocol I, where Charlie prepares $|\sqrt{\mu}\rangle$ and $|-\sqrt{\mu}\rangle$ with equal probabilities. (b) Schematic diagram of Protocol II, where Alice and Bob prepare $|\sqrt{\mu/2}\rangle$ and add a same random phase $\phi \in \{0, \pi\}$.

$$\rho_{AB}(\sqrt{\mu}, -\sqrt{\mu}) = \frac{1}{2}(\sqrt{\mu/2})_A \langle \sqrt{\mu/2}| \otimes |\sqrt{\mu/2}\rangle_B \langle \sqrt{\mu/2}| + |\sqrt{-\mu/2}\rangle_A \langle \sqrt{-\mu/2}| \otimes |\sqrt{-\mu/2}\rangle_B \langle \sqrt{-\mu/2}|)$$. (A26)
4. Security with phase announcement

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

We deal with the phase announcement of \(\phi_a, \phi_b\) first. Consider Protocol IIa, as shown in Fig. 6, where Alice and Bob announce the random phase \(\phi\) in Protocol II during post-processing.

**Protocol IIa**

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

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

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

\[
M_{\text{odd}}^t = \sum_{k_1 + k_2 \text{ odd}} \frac{\ket{k_1 k_2}_{AB}}{\sqrt{2}} \bra{k_1 k_2}, \quad M_{\text{even}}^t = \sum_{k_1 + k_2 \text{ even}} \frac{\ket{k_1 k_2}_{AB}}{\sqrt{2}}. \tag{27}
\]

Here, \(\ket{k_1 k_2}_{AB}\) are the Fock states on mode \(A, B\), with \(k_1\) photons on \(A\) and \(k_2\) photons on \(B\). That is, in Protocol II, the photon source can be regarded as a mixture of odd states and even states. The parity state channel model is similar to the photon number channel used in the security proof of the decoy-state method [19, 24].

In Protocol IIa, as shown in Fig. 6, on the other hand, no such parity measurement is allowed because it does not commute with the phase announcement. That is, Eve can distinguish whether or not Alice and Bob perform \(\{M_{\text{odd}}^t, M_{\text{even}}^t\}\) after the announcement of phases \(\phi_a\) and \(\phi_b\). In other words, the quantum signals sent by Alice and Bob can no longer be regarded as a mixture of \(\rho_{\text{odd}}\) and \(\rho_{\text{even}}\) in Protocol IIa. To analyze the security of Protocol IIa, we notice the following observation.

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

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

**Corollary 1.** Both the X- and Z-error patterns of the joint states \(\rho_{A'B'}^{(n)}\) in Protocol II and IIa are the same. Then, the X-error rate \(E_X\) of Protocols II and IIa are the same, as given by Eq. (A24).

Now, we deal with the post-selection of \(\phi_a = \phi_b\). Regardless the values of \(\phi_a, \phi_b\), due to control-phase gates \(C_{\pi}\), the state \(\rho_{AB}\) sent to Eve is

\[
\rho_{AB} = \rho_A(\sqrt{\mu/2}, -\sqrt{\mu/2}) \otimes \rho_B(\sqrt{\mu/2}, -\sqrt{\mu/2}), \tag{28}
\]

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

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

Therefore, if Alice and Bob randomize their phases \(\phi_a, \phi_b \in \{0, \pi\}\) independently and perform phase post-selection operations after Eve’s announcement, shown in Fig. 6, it is equivalent to Protocol IIa. We call this protocol as Protocol III.

**Protocol III** runs as follows, as shown in Fig. 6. Here \(\mu_a = \mu_b = \mu = \mu/2\).

1. State preparation: Alice and Bob prepare coherent states \(|\sqrt{\mu_a}\rangle\) and \(|\sqrt{\mu_b}\rangle\) on optical modes \(A, B\), separately. They initial their qubits \(A', B'\) in \(|+i\rangle\).

They independently add random phases \(\phi_a, \phi_b \in \{0, \pi\}\) on optical modes \(A, B\). Alice applies the control gate \(C_{\pi}\), defined in Eq. (A9), to qubit \(A'\) and optical pulse \(A\). Similarly, Bob applies \(C_{\pi}\) to \(B'\) and \(B\).
2. Measurement: the two optical pulses, $A$ and $B$, are sent to an untrusted party, Eve, who is supposed to perform interference measurement and record which detector ($L$ or $R$) clicks.

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

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

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

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

5. Decoy-state method and phase randomization

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

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

\[ q^\mu_{odd} = p^\mu_{odd} Y^\mu_{odd}, \]
\[ q^\mu_{even} = p^\mu_{even} Y^\mu_{even}, \]

where \( Q^\mu \) is the total gain of the signals. For signals with intensity \( \mu \), we have

\[ Q^\mu = p^\mu_{odd} Y^\mu_{odd} + p^\mu_{even} Y^\mu_{even}, \]
\[ E^Z \mu Q^\mu = e^Z_\mu p^\mu_{odd} Y^\mu_{odd} + e^Z_\mu p^\mu_{even} Y^\mu_{even}, \]

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

If we directly estimate \( q^\mu_{odd}, q^\mu_{even}, e^Z_{odd} \) and \( e^Z_{even} \) from Eq. (A29), Eq. (A30) and the constraint that

\[ q^\mu_{odd}, q^\mu_{even}, e^Z_{odd}, e^Z_{even}, Y^\mu_{odd}, Y^\mu_{even} \in [0, 1], \]

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

Now, we introduce a more efficient method to estimate \( q^\mu_{odd}, q^\mu_{even}, e^Z_{odd} \) and \( e^Z_{even} \). Essentially, we employ the idea of the decoy-state method \[24\]. That is, in Protocol I, Charlie adjusts the intensity, \( \mu \), of his prepared coherent light. After Eve’s announcement, Charlie announces the value of \( \mu \). Furthermore, Charlie randomizes the phase \( \phi \) on state \( |\sqrt{\mu}e^{i\phi}\rangle \) continuously from \([-\pi, \pi]\). In this case, the state prepared by Charlie can be written as

\[ \frac{1}{2\pi} \int_{0}^{2\pi} d\phi |\sqrt{\mu}e^{i\phi}\rangle \langle \sqrt{\mu}e^{i\phi}| = \sum_{k=0}^{\infty} P(k) |k\rangle \langle k|. \] (A32)

That is, in Protocol I, if Charlie prepares \( |\sqrt{\mu}e^{i\phi}\rangle \) with random phase \( \phi \), this is equivalent to preparing the Fock states \( \{|k\}\} \) with probability \( P(k) \). Obviously, Fock states \( \{|k\}\} \) are parity states. Then, by directly applying Lemma 3 we can estimate the X-error by

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

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

The source components are Fock states \( \{|k\}\} \), whose yields \( Y_k \) and Z-error rates \( e_k^Z \) are independent of \( \mu \). The fractions \( q^\mu_k \) of “\( k \)-photon component” in the final detected signals are given by

\[ q^\mu_k = P^\mu(k) \frac{Y_k}{Q^\mu}. \] (A34)

The overall gain and QBER are given by

\[ Q^\mu = \sum_{k=0}^{\infty} P^\mu(k) Y_k, \] (A35)
\[ E^Z \mu Q^\mu = \sum_{k=0}^{\infty} e^Z_k P^\mu(k) Y_k. \]

The main idea of the decoy-state method is that Alice and Bob can obtain a set of linear equations in the form of Eq. (A35) and (A36) by using a few values of \( \mu \). When an infinite amount of decoy states are used, Alice and Bob can estimate all the parameters \( Y_k \) and \( e_k^Z \) accurately. Then, they can estimate \( q^\mu_k \) and \( e_k^Z \) accurately, and then upper bound the X-error by Eq. (A33).

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

First, we want to argue that the random-phase post-selection of \(|\phi_a - \phi_b| = 0 \text{ or } \pi \) would not affect the security. In fact, any phase post-selection would not be affected by Eve’s announcement. Note that the random phases \( \phi_a, \phi_b \) are determined by Alice and Bob locally. Thus, the sifted qubit pairs, \( \rho^{x,y}_{a,b} \), would be the same in the two cases: 1) Alice and Bob independently randomize the phases, \( \phi_a, \phi_b \), and employ this phase post-selection \(|\phi_a - \phi_b| = 0 \text{ or } \pi \); 2) Charlie randomizes the same phases, \( \phi_a = \phi_b \), to \( A \) and \( B \).

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

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

Now, we can modify Protocol III with continuous phase randomization \( \phi_a, \phi_b \) and the decoy-state method, namely Protocol IV, as shown in Fig. 4(a).

**Protocol IV**

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

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

3. Announcement: Eve announces the detection result, $L/R$-click for failure, for each round.

4. Sifting: when Eve announces an $L/R$-click, Alice and Bob keep the qubits of systems $A'$ and $B'$. Bob applies a Pauli $Y$-gate to his qubit if Eve’s announcement is $R$-click. After Eve’s announcement, Alice and Bob announce their encoded intensities $\mu_a, \phi_a; \mu_b, \phi_b$. They maintain the signal if $\mu_a = \mu_b$ and $|\phi_a - \phi_b| = 0$ or $\pi$. Bob applies a Pauli $Y$-gate to his qubit if $|\phi_a - \phi_b| = \pi$.

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

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

Finally, we need to reduce the entanglement-based protocol to a prepare-and-measure protocol. Following the Shor-Preskill argument, we move the key measurement in Step 6 before the EDP, the parameter estimation and the $C_\pi$ gates. That is, they measure the systems $A'$ and $B'$ at the beginning. Therefore, the entanglement-based protocol (Protocol IV) becomes the PM-QKD protocol, as shown in Fig. 2(b).

**PM-QKD protocol**

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

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

3. Announcement: Eve announces the detection result, $L/R$-click for failure, for each round.

4. Sifting: when Eve announces an $L/R$-click, Alice and Bob keep the key bits, $\kappa_a$ and $\kappa_b$. Bob flips his key bit $\kappa_b$ if Eve’s announcement is $R$-click. After Eve’s announcement, Alice and Bob announce their encoded intensities and phases $\mu_a, \phi_a; \mu_b, \phi_b$. They maintain the signal if $\mu_a = \mu_b$ and $|\phi_a - \phi_b| = 0$ or $\pi$. Bob applies a Pauli $Y$-gate to his qubit if $|\phi_a - \phi_b| = \pi$.

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

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

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

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

1. The phase of Alice and Bob’s coherent state is locked, that is, the phase reference of Alice’s and Bob’s coherent state is the same.

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

We will discuss how to remove these two requirements in Section A6 and hence make the protocol practical.

### 6. Phase Post-Compensation

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

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

$$j_a = \lfloor \frac{\phi_a}{2\pi} M \rfloor \mod M, \quad j_b = \lfloor \frac{\phi_b}{2\pi} M \rfloor \mod M,$$

(A36)

where $\lfloor \cdot \rfloor$ is the round function to output the nearest integer. That is, Alice announces the $j_a$-th slice $\Delta_{j_a}$ where her random phase $\phi_a$ falls into. Similarly, Bob announces $j_b$. The sifting condition is $|j_a - j_b| = 0$ or $M/2$. This technique is first used in the phase-encoding
With $\phi_a, \phi_b; \mu_a, \mu_b$ announced

\[
|+i\rangle \quad \text{A}
|\sqrt{\mu_a/2}\rangle \quad B
|\phi_a\rangle \quad 0, \pi
\]

$\rho_0$

With $\phi_a, \phi_b; \mu_a, \mu_b$ announced

\[
|+i\rangle \quad \text{A}
|\sqrt{\mu_a/2}\rangle \quad B
|\phi_b\rangle \quad 0, \pi
\]

FIG. 7. (a) Schematic diagram of Protocol IV, where decoy-state method is applied. The random phase $\phi_a, \phi_b \in [0, 2\pi)$. (b) Schematic diagram of PM-QKD protocol.

measurement-device-independent quantum key distribution (MDI-QKD) \[15\]. Announcing the phase slices $j_a$ and $j_b$ rather than the exact phase $\phi_a$ and $\phi_b$ will only leak less information to Eve. Thus, all the security proof results from previous subsections apply here. Applying Eq. (A15), we also need to add a phase sifting factor $\Delta_f$ for Eve.

During sifting, Bob can estimate the offset $j_0$ for each pulse. The estimation accuracy would not affect the security. In fact, in the security proofs, we assume Eve knows the phase references ahead. Suppose Bob compensates the offset by $j_d$, and he has the freedom to choose $j_d$ from $\{0, 1, \ldots, M-1\}$. In a practical scenario, normally the phase references (and hence the offset $j_0$) change slowly with time. Then, Bob can figure out the proper phase compensation offset $j_d$ by minimizing the QBER from random sampling, as shown in Fig. 2.

For the case where phase reference difference $\phi_0$ varies, we can treat the changing caused by Eve. Such deviation will introduce bit errors, but not help Eve learn key information, since the variation of $\phi_0$ is independent of the key $\kappa_a, \kappa_b$. Note that in the security proof, we assume that Eve knows the phase references accurately.

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

**PM-QKD protocol with phase post-compensation**

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

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

3. **Announcement:** Eve announces the detection results, $L/R$-click or failure, for each round.

4. **Sifting:** when Eve announces an $L/R$ click, Alice and Bob keep the key bits, $\kappa_a$ and $\kappa_b$. Bob flips his key bit $\kappa_b$ if Eve’s announcement is $R$-click. After Eve’s announcement, Alice and Bob announce their encoded intensities $\mu_a$ and $\mu_b$, respectively. They keep the bits if $\mu_a = \mu_b$.

5. **Parameter estimation:** Alice and Bob run the above procedures many times and then run the following procedures.
(a) For each bit, Alice announces the phase slice index $j_a$, given in Eq. (A36), and she randomly samples a certain amount of key bits and announces them for QBER testing.

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

(c) Alice and Bob analyze the overall gain $Q_{\mu_i}$ and QBER $E_{\mu_i}$ for different values of intensities $\mu_a = \mu_b = \mu_i/2$. They estimate the phase error rate $E_{\mu_i}^{(X)}$ by Eq. (A38).

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

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

Now, we consider a practical example. Consider the slice number $M = 16$, the tolerable fluctuation should be about $\pi/M = 0.196$ rad. The phase of a continuous-wave (CW) laser pulse usually fluctuates randomly, whose behavior can be modeled as a random walk. In an experimental test performed 10 years ago [34], for a 36.5 km Mach-Zehnder interferometer, when the time duration 0.2 ms, the mean phase fluctuation is about 0.15 rad, which is less than $\pi/M$. Then, in this case, one can set $\tau_M = 0.2$ ms for testing. Consider a GHz QKD system, there are $2 \times 10^5$ signals sent out within $\tau_M$. Using the same parameters for a longer transmission distance of 150 km from Alice to Eve (same distance for Bob) using standard telecom fibre (0.2 dB/km), the transmission loss is $\eta = 30dB = 10^{-3}$, there will be 200 data left for post-processing, which is sufficient for sampling tests. From here, one can see that our phase post-compensation method is feasible by current technology.

Appendix B: Model and Simulation

Here, we show the details for the simulations different QKD schemes. We mainly follow the simulation model used in literature [19, 35]. We calculate the detection probabilities of PM-QKD in Section B1 and then evaluate the yields, gains, and error rates in Section B2. In simulation, we also compare the performance of PM-QKD with the decoy-state BB84 [1], MDI-QKD [15], and the linear key rate bound [10, 11]. We list the used formulas and simulation parameters in Section B3.

1. Detection probabilities

The channel is assumed to be a pure loss one and symmetric for Alice and Bob with transmittance $\eta$ (with detector efficiency $\eta_d$ taken into account). We suppose that the lights from Alice and Bob faithfully interfered and measured with dark-count rate $\rho_d$. Without loss of generality, we only consider the case where $\kappa_a = \kappa_b = 0$, $j_a = j_b = 0$.

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

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

$$(e^{i\phi_a}a^\dagger + e^{i\phi_b}b^\dagger)|00\rangle_{A_0B_0} = (a^\dagger + e^{i\phi_b}b^\dagger)|0\rangle.$$  

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

$$a^\dagger \rightarrow \sqrt{\eta}a^\dagger + \sqrt{1-\eta}\delta^\dagger,$$

$$b^\dagger \rightarrow \sqrt{\eta}b^\dagger + \sqrt{1-\eta}\delta^\dagger,$$

where $\delta^\dagger, \delta^\dagger$ are the modes coupled to the environment. Before Eve’s interference, the state is

$$(\sqrt{\eta}(a^\dagger + e^{i\phi_b}b^\dagger) + \sqrt{1-\eta}(s^\dagger + e^{i\phi_s}t^\dagger))|0\rangle,$$

and after Eve’s interference, the state becomes

$$\sqrt{\frac{\eta}{2}}[(1+e^{i\phi_c})s^\dagger + (1-e^{i\phi_c})r^\dagger]\rightarrow \sqrt{1-\eta}(s^\dagger + e^{i\phi_st}t^\dagger)|0\rangle,$$

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

$$p_{0}^{(1)} = 1 - \eta,$$

$$p_{l}^{(1)} = \eta \cos^2(\frac{\phi_b}{2}),$$

$$p_{r}^{(1)} = \eta \sin^2(\frac{\phi_b}{2}),$$

$$p_{lr}^{(1)} = 0.$$
where \( p^{(1)}_0, p^{(1)}_1, p^{(1)}_r \), and \( p^{(1)}_c \) are, respectively, the probabilities for no-click, L-click, R-click, and double-click for the single-photon case.

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

\[
\begin{align*}
p^{(k)}_0 &= (p^{(1)}_0)^k, \\
p^{(k)}_L &= (p^{(1)}_0 + p^{(1)}_c - (p^{(1)}_0)^k, \\
p^{(k)}_R &= (p^{(1)}_0 + p^{(1)}_r - (p^{(1)}_0)^k, \\
p^{(k)}_{L,R} &= 1 - p^{(k)}_0 - p^{(k)}_L - p^{(k)}_R, \\
&= 1 + (p^{(1)}_0)^k - (p^{(1)}_0 + p^{(1)}_c)^k - (p^{(1)}_0 + p^{(1)}_r)^k, \\
\end{align*}
\]

where \( p^{(k)}_0, p^{(k)}_L, p^{(k)}_R, \) and \( p^{(k)}_{L,R} \) are, respectively, the probabilities for no-click, L-click, R-click, and double-click for the \( k \)-photon case.

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

\[
\begin{align*}
P^{(k)}_0 &= (1 - p_d)^2 p^{(k)}_0, \\
P^{(k)}_L &= (1 - p_d)^2 p^{(k)}_L + p_d(1 - p_d)(p^{(k)}_0 + p^{(k)}_c) \\
&= p_d(1 - p_d)(p^{(k)}_0 + p^{(k)}_c), \\
P^{(k)}_R &= (1 - p_d)^2 p^{(k)}_R + p_d(1 - p_d)(p^{(k)}_0 + p^{(k)}_r) \\
&= p_d(1 - p_d)(p^{(k)}_0 + p^{(k)}_r), \\
P^{(k)}_{L,R} &= (1 - p_d)^2 p^{(k)}_{L,R} + p_d(1 - p_d)(p^{(k)}_L + p^{(k)}_R) + p_d^2 \\
&= (1 - p_d)^2 p^{(k)}_{L,R} + p_d(1 - p_d)(p^{(k)}_L + p^{(k)}_R) + p_d^2. \\
\end{align*}
\]

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

\[
\begin{align*}
|\alpha_L\rangle &= \frac{\sqrt{\mu}}{2} (e^{i\phi_a} + e^{i\phi_b}) = \frac{\sqrt{\mu}}{2} e^{i\phi_a} (1 + e^{i\phi_b}), \\
|\alpha_R\rangle &= \frac{\sqrt{\mu}}{2} (e^{i\phi_a} - e^{i\phi_b}) = \frac{\sqrt{\mu}}{2} e^{i\phi_a} (1 - e^{i\phi_b}).
\end{align*}
\]

Then, the detection click probabilities are,

\[
\begin{align*}
P_{\mu}(\bar{L}) &= (1 - p_d) \exp (-|\alpha_L|^2) \\
&= (1 - p_d) \exp (-\eta \mu \cos^2(\frac{\phi_a}{2})), \\
P_{\mu}(L) &= 1 - P_{\mu}(\bar{L}), \\
P_{\mu}(\bar{R}) &= (1 - p_d) \exp (-|\alpha_R|^2) \\
&= (1 - p_d) \exp (-\eta \mu \sin^2(\frac{\phi_a}{2})), \\
P_{\mu}(R) &= 1 - P_{\mu}(\bar{R}),
\end{align*}
\]

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

All the above probability formulas are functions of the phase difference \( \phi_s \). In the simulation, one needs to integrate \( \phi_s \) over its probability distribution \( f_{\phi_s}(\phi) \). Recall that the phase reference deviation between Alice and Bob is \( \phi_0 \). Here, with the phase post-compensation method introduced in Section A.6, we assume \( \phi_0 \) is uniformly distributed in \([-\pi/M, \pi/M]\), denoted by

\[
\phi_0 \sim U[-\pi/M, \pi/M].
\]  

In this case, \( \phi_a \) and \( \phi_b \) are uniformly distributed in \([0, 2\pi/M]\) and \([\phi_0, 2\pi/M + \phi_0]\), respectively,

\[
\begin{align*}
\phi_a &\sim U[0, 2\pi/M], \\
\phi_b &\sim U[\phi_0, 2\pi/M + \phi_0].
\end{align*}
\]

For a fixed \( \phi_0 \), the probability distribution of the phase difference \( \phi_s \) is given by

\[
\begin{align*}
f_{\phi_s}(\phi) &= \begin{cases} 
\frac{M}{\pi} [\phi + (\frac{2\pi}{M} - \phi_0)] & \phi \in [\phi_0 - \frac{2\pi}{M}, \phi_0), \\
\frac{M}{\pi} [\phi - (\frac{2\pi}{M} + \phi_0)] & \phi \in [\phi_0, \phi_0 + \frac{2\pi}{M}), \\
0 & \text{otherwise.}
\end{cases}
\end{align*}
\]

Furthermore, in the simulation, one needs to take another integration of \( \phi_0 \) over \([-\pi/M, \pi/M]\) to get the yields, gain, and error rates.

2. Yields, gain, and error rates

We first analyze the yield \( \{Y_k\} \) for \( k \geq 0 \) and the total gain \( Q_{\mu} \), according to the probability formulas given in Section B.1. Note that in PM-QKD, both no-click and double-click events are regarded as failure detection. The yield \( Y_k \) of the \( k \)-photon state is given by Eq. (B5), (B6), and (B7).


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

| Dark count condition | Contributions to the overall click probabilities |
|----------------------|-----------------------------------------------|
|                      | L-dark count | R-dark count | no-click $P_0^{(k)}$ | L-click $P_L^{(k)}$ | R-click $P_R^{(k)}$ | double-click $P_{L/R}^{(k)}$ |
| (1 - $p_d$)          | (1 - $p_d$) | $p_0^{(k)}$ | 0 | 0 | $p_0^{(k)}$ + $p_d^{(k)}$ |
| (1 - $p_d$)          | $p_d$       | $p_0^{(k)}$ | 0 | 0 | $p_0^{(k)}$ + $p_d^{(k)}$ |
| $p_d$                | (1 - $p_d$) | 0           | $p_0^{(k)}$ + $p_d^{(k)}$ | 0 | 0 | $p_d^{(k)} + p_0^{(k)}$ |
| $p_d$                | $p_d$       | 0           | $p_0^{(k)}$ + $p_d^{(k)}$ | 0 | 0 | $p_d^{(k)} + p_0^{(k)}$ |

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

\[
Y_k = P_L^{(k)} + P_R^{(k)} = (1 - p_d)(p_1^{(k)} + p_r^{(k)}) + 2p_d(1 - p_d)p_0^{(k)} = (1 - p_d)(1 - \eta \sin^2(\phi_\delta/2) + (1 - \eta \cos^2(\phi_\delta/2))k - 2(1 - p_d)^2(1 - \eta)^k \approx (1 - p_d)(1 + (1 - \eta)^k) - 2(1 - p_d)^2(1 - \eta)^k = (1 - p_d)[1 - (1 - 2p_d)(1 - \eta)^k] \approx 1 - (1 - 2p_d)(1 - \eta)^k. \tag{B13}
\]

The total gain $Q_\mu$ is given by Eq. (B9),

\[
Q_\mu = P(L)P(R) = (1 - p_d) \exp(-\eta \mu \sin^2(\phi_\delta/2))[1 - (1 - p_d) \exp(-\eta \mu \cos^2(\phi_\delta/2))] + (1 - p_d) \exp(-\eta \mu \cos^2(\phi_\delta/2))[1 - (1 - p_d) \exp(-\eta \mu \sin^2(\phi_\delta/2))] \approx (1 - p_d)[1 - (1 - p_d) \exp(-\eta \mu)] + p_d(1 - p_d) \exp(-\eta \mu) \approx 1 - e^{-\eta \mu} + 2p_d e^{-\eta \mu}, \tag{B14}
\]

where the two approximations are the same as the ones used in Eq. (B13). Since $\phi_\delta$ does not affect the yields $Y_k$ and gain $Q_\mu$ much with the first-order approximation, the average yields $Y_k$ and gain $Q_\mu$ over $\phi_\delta \in [-\pi/M, \pi/M]$ can be regarded as the ones when $\phi_\delta = 0$. Also, the results of Eq. (B13) and (B14) are consistent with the ones presented in the regular QKD model \cite{35}, as shown in Eq. (B29) and (B30).

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

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

where $P_L^{(k)}$ and $P_R^{(k)}$ are given by Eq. (B5), (B6), and (B7). The average bit error rate of $e_k^Z$ over $\phi_\delta$ is given by the following integral,

\[
e_k^Z = \frac{M}{2\pi} \int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi f^{(\phi_0)}(\phi)e_k^Z(\phi), \tag{B16}
\]

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

\[
e_1^Z(\phi_\delta) = \frac{(1 - p_d)^2 p_1^{(1)} + p_d(1 - p_d)(p_0^{(1)} + p_1^{(1)})}{(1 - p_d)^2 \eta + p_d(1 - p_d)(2 - \eta)} = \frac{\sin^2(\phi_\delta/2)\eta + p_d(1 - \eta)}{\eta + 2p_d(1 - \eta)}, \tag{B17}
\]

(1 - 2p_d)(1 - \eta)^k = O(p_d^2 + p_d\eta)$, since normally $p_d$ is small.
and integrate Eq. (B17) by Eq. (B16),
\[
e^Z_k = \frac{M}{2\pi} \int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi f_{\phi_0}(\phi) e^Z_k(\phi)
\]
\[
= e_\delta \eta + p_d(1-\eta) \eta + 2p_d(1-\eta),
\]
(B18)
where
\[
e_\delta = \frac{\pi}{M} - \frac{M^2}{\pi^2} \sin^3 \left( \frac{\pi}{M} \right)
\]
(B19)
can be regarded as the misalignment error rate. Eq. (B18) can be understood that if a signal causes a click, the error rate is \(e_\delta\); and if a dark count causes a click, the error rate is \(e_0 = 1/2\). Since the double-click events are discarded, when both a signal and a dark count cause clicks, the error rate is \(e_\delta\). Then, we can approximate \(e^Z_k\) with the same spirit, for the contributions in \(Y_k\), given in Eq. (B13),
\[
e^Z_k \approx p_d(1-\eta)^k + e_\delta [1 - (1-\eta)^k] \int_{Y_k}.
\]
(B20)
Here, note that in Eq. (B20), we ignore the double clicks caused by multi-photon signals, which would further reduce the misalignment error and hence the value of \(e^Z_k\).

The QBER \(E^Z_\mu(\phi_\delta)\) for a given \(\phi_\delta\) is given by substituting Eq. (B19),
\[
E^Z_\mu(\phi_\delta) = \frac{P(L)P(R)}{P(L)P(R) + P(L)P(R)}
\]
\[
= \frac{1}{Q_\mu} \left[ 1 - p_d \exp(-\eta_\mu \cos^2(\phi_\delta/2)) \right] \left[ 1 - (1-\eta_\mu) \exp(-\eta_\mu \sin^2(\phi_\delta/2)) \right]
\]
\[
= \frac{1}{Q_\mu} (1 - p_d) \left[ \exp(-\eta_\mu \cos^2(\phi_\delta/2)) - (1-\eta_\mu) e^{-\eta_\mu} \right]
\]
\[
\approx \frac{e^{-\eta_\mu}}{Q_\mu} \left[ p_d + \eta_\mu \sin^2(\phi_\delta/2) \right]
\]
(B21)
similar to Eq. (B18),
\[
E^Z_\mu = \frac{M}{2\pi} \int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi f_{\phi_0}(\phi) E^Z_\mu(\phi_\delta)
\]
\[
= \frac{(p_d + \eta_\mu e_\delta) e^{-\eta_\mu}}{Q_\mu},
\]
(B22)
where \(e_\delta\) is given in Eq. (B19). The results of Eq. (B22) and (B19) are consistent with the one presented in the regular QKD model [35], as shown in Eq. (B29) and (B30), with a slight difference. The difference is caused by how the double-click events are processed. In BB84, Alice and Bob need to randomly assign a bit to double-clicks, while PM-QKD, double-clicks are discarded.

Now, we can evaluate the key rate with the above model. Let us restate the key rate formula, Eq. (A37),
\[
R_{PM} \geq \frac{2}{M} Q_\mu \left[ 1 - f H(E^X_\mu) - H(E^X_\mu) \right],
\]
(B23)
where the phase error rate is given by Eq. (A33),
\[
E^X_\mu = \sum_{k=0}^{\infty} q_{2k+1} e^Z_{2k+1} + \sum_{k=0}^{\infty} q_{2k} (1 - e^Z_{2k})
\]
\[
\leq q_0 e^Z_0 + \sum_{k=0}^{\infty} e^Z_{2k+1} q_{2k+1} + (1 - q_0 - q_{odd}).
\]
(B24)
In simulation, \(Q_\mu\) and \(E^Z_\mu\) are given by Eq. (B14) and (B22). The fractions, \(\{q_k\}\) with \(k \geq 0\), of different photon components \(k\) contributing to the valid detections (L/R-clicks) are given by
\[
q_k = \frac{P(k)Y_k}{Q_\mu} = e^{-\mu k} \frac{Y_k}{k!} Q_\mu.
\]
(B25)
For the odd-photon-number component, we have
\[
q_{odd} = \sum_{k=0}^{\infty} q_{2k+1}
\]
\[
= \frac{1}{Q_\mu} \sum_{k=0}^{\infty} \frac{Y_{2k+1} \mu^{2k+1} e^{-\mu}}{(2k+1)!}
\]
\[
= \frac{e^{-\mu}}{Q_\mu} \sum_{k=0}^{\infty} \left[ \frac{\mu^{2k+1}}{(2k+1)!} - (1 - 2p_d) \frac{(\eta_\mu)^{2k+1}}{(2k+1)!} \right]
\[
= \frac{e^{-\mu}}{Q_\mu} \{ \sinh(\mu) - (1 - 2p_d) \sinh[(1-\eta)_\mu] \}.
\]
(B26)
To simplify the simulation, we explicitly calculate the \(e^Z_k\) and \(q_k\) for \(0 \leq k \leq 5\). Further zoom the Eq. (B24),
we have

\[ E^X_\mu = \sum_{k=0}^{\infty} q_{2k+1} e^{Z}_{2k+1} + \sum_{k=0}^{\infty} q_{2k}(1 - e^{Z}_{2k}), \]

\[ \leq q_0 e_0 Z + (q_1 e_1 Z + q_3 e_3 Z + q_5 e_5 Z) + (1 - q_0 - q_1 - q_3 - q_5), \]

where \( e_k \) and \( q_k \) are given by Eq. [B15] and [B25], respectively.

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

We compare our derived key rate with that of the prepare-and-measure BB84 [1] protocol, whose key rate is given by the GLLP-decoy method [22].

The key rate of the decoy-state BB84 protocol is given by [24],

\[ R_{BB84} = \frac{1}{2} Q_\mu \{ - f H(E^Z_\mu) + q_1[1 - H(e_1^X)] \}, \]  (B28)

where 1/2 is the basis sifting factor.

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

\[ Y_k = 1 - (1 - Y_0)(1 - \eta)^k, \]

\[ e_k = e_d + \frac{(e_0 - e_d)Y_0}{Y_k}, \]  (B29)

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

\[ Q_\mu = \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!} Y_k, \]

\[ = 1 - (1 - Y_0)e^{-\eta}, \]  (B30)

\[ E_\mu = \sum_{k=0}^{\infty} \frac{\mu^k e^{-\mu}}{k!} e_k Y_k, \]

\[ = e_d + \frac{(e_0 - e_d)Y_0}{Q_\mu}, \]

where \( Y_0 = 2p_d \) and \( e_0 = 1/2 \).

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

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

where \( Q_{11} = \mu a e^{-\mu_a}\mu_b Y_{11} \) and 1/2 is the basis sifting factor. We take this formula from Eq. (B27) in Ref. [18].

In simulation, the gain and error rates are given by,

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

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

\[ Q_{rect} = Q^{(C)}_{rect} + Q^{(E)}_{rect}, \]

\[ Q^{(C)}_{rect} = 2(1 - p_d)^2 e^{-\mu'/2} [1 - (1 - p_d)e^{-\eta_a /2}][1 - (1 - p_d)e^{-\eta_b /2}], \]

\[ Q^{(E)}_{rect} = 2p_d(1 - p_d) e^{-\mu'/2} [1(2x) - (1 - p_d)e^{-\mu'/2}], \]

\[ E_{rect} Q_{rect} = e_d Q^{(C)}_{rect} + (1 - e_d)Q^{(E)}_{rect}. \]  (B32)

Here,

\[ \mu' = \eta_a \mu_a + \eta_b \mu_b, \]

\[ x = \frac{1}{2} \sqrt{\eta_a \mu_a \eta_b \mu_b}, \]  (B33)

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

We take these formulae from Eq. (A9, A11) and (B7, B28-B31) in [18].

The linear key rate bound used in the main text in given by [10 11],

\[ R_{lin} = - \log_2(1 - \eta). \]  (B34)

Appendix C: Beam-splitting Attack: Invalidation of the photon number channel model

Here, we argue that the tagging technique does not work for PM-QKD, by showing that the lower bound of the key rate from naïvely employing the tagging technique can be higher than a upper bound derived from a specific attack, in some parameter regime. The failure of the tagging technique stems from the failure of the photon number channel model used in the security proof [19]. In other words, the photon number channel model does not hold for the case when the random phases are announced during postprocessing.
1. Key rate with/without the photon number channel

Assuming the existence of the photon number channel model in PM-QKD, we can apply the tagging method and obtain a key rate formula following the GLLP analysis \cite{23,24},

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

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

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

\[
    r_{PM} = 1 - H(E_\mu^X) - H(E_\mu^X),
\]

where \( E_\mu^X \) is bounded by Eq. (B27)

\[
    E_\mu^X = \sum_{k=0}^{\infty} q_{2k+1} e_{2k+1}^Z + \sum_{k=0}^{\infty} q_{2k}(1 - e_{2k}^Z),
\]

\[
    \leq q_0 e_0^Z + (q_1 e_1^Z + q_3 e_3^Z + q_5 e_5^Z) + (1 - q_0 - q_1 - q_3 - q_5).
\]

2. Beam-splitting attack

Now we consider a beam-splitting (BS) attack where Eve sets beam splitters with transmittance \( \eta \) on both Alice and Bob’s side to simulate a lossy channel. She intercepts the pulses on \( A \) and \( B \), regardless of the keys and bases of the pulses, store the reflected lights on her quantum memories, modes \( A0 \) and \( B0 \). Eve interferes the two transmitted pulses, modes \( A1 \) and \( B1 \) and announces the results. After Alice’s and Bob’s phase announcements, Eve performs an unambiguous state discrimination (USD) \cite{36} on the states on modes \( A0 \) and \( B0 \) separately to guess the key information. Since the states on \( A0(B0) \) and \( A1(B1) \) are uncorrelated due to the beam splitting of coherent states, the BS attack will not introduce any error or other detectable effects. Apparently, this BS attack is an individual attack. We will calculate Eve’s successful probability for guessing the key bits unambiguously, and calculate the mutual information \( I(\kappa_a(b) : E) \), from which we can derive an upper bound on the secure key rate.

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

\[
    |\sqrt{(1-\eta)}\mu_a e^{i(\phi_a+\kappa_a)}\rangle_{A0},
\]

\[
    |\sqrt{(1-\eta)}\mu_b e^{i(\phi_b+\kappa_b)}\rangle_{B0}.
\]

The two remaining pulses on system, \( A1, B1 \), used for interference are given by,

\[
    |\sqrt{\eta}\mu_a e^{i(\phi_a+\kappa_a)}\rangle_{A1},
\]

\[
    |\sqrt{\eta}\mu_b e^{i(\phi_b+\kappa_b)}\rangle_{B1}.
\]

Suppose Eve performs interfere systems \( A1 \) and \( B1 \), then the total gain \( Q_\mu \) is given by,

\[
    Q_\mu = 1 - e^{-\eta \mu}.
\]

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

\[
\frac{1}{2\pi} \int_0^{2\pi} d\phi_a |\sqrt{(1-\eta)}\mu_a e^{i(\phi_a+\kappa_a)}\rangle_{A0} \langle \sqrt{(1-\eta)}\mu_a e^{i(\phi_a+\kappa_a)}| = \sum_{k=0}^{\infty} P^{(1-\eta)\mu_a}(k) |k\rangle_{A0} \langle k|,
\]

where

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

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

\[
\frac{1}{2}(|\sqrt{(1-\eta)}\mu_a\rangle_{A0} \langle \sqrt{(1-\eta)}\mu_a| - |\sqrt{(1-\eta)}\mu_a\rangle_{A0} \langle -\sqrt{(1-\eta)}\mu_a|).
\]

Then, Eve only needs to determine whether the phase \( \kappa_a \) is 0 or \( \pi \) to obtain the key information. As shown in \cite{36}, if two pure states \( |p\rangle \) and \( |q\rangle \) are prepared with the same a priori \( 1/2 \), the maximum probability of unambiguous discrimination is:

\[
    P_{des} = 1 - |\langle p | q \rangle|.
\]

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

\[
    P_{suc} = 1 - |\langle \sqrt{(1-\eta)}\mu_a - \sqrt{(1-\eta)}\mu_a | - 1 = e^{-(1-\eta)\mu}.
\]

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

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

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

With unambiguous state discrimination, the mutual information of Eve’s measurement result (denoted by variable $E$) and Alice’s and Bob’s key $\kappa_a$ ($\kappa_b$) is

$$I(\kappa_a(b) : E) = P_{BS} = 1 - e^{-2(1-\eta)\mu}. \quad (C13)$$

Suppose that there is no extra error induced by other factors, then the BS-attack provides an upper bound on the key rate,

$$r_{BS} = [1 - I(\kappa_a(b) : E)] = e^{-2(1-\eta)\mu} = e^{-2\mu/ (1 - Q\mu)^2}. \quad (C14)$$

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

3. Comparison

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

First, under BS attack, the yield is given by

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

and the fraction of the $k$-photon component is

$$q_k = (e^{-\mu\mu k} k!)\frac{Y_k}{Q\mu} = (1 - (1 - \eta)^k)\frac{e^{-\mu\mu k}}{k!Q\mu}. \quad (C16)$$

Note that $q_0 = 0$.

Second, in the BS attack scenario, Eve’s operations will not introduce any error, hence

$$e_k^Z = 0, \quad \forall k \geq 0,$$

$$E_k^Z = 0,$$

then Eq. (C1), (A15) and (B27) can be simplified to

$$r_{GLLP} = q_1 = \eta\mu e^{-\mu}, \quad (C18)$$

$$r_{PM} = \left[1 - H(E^X)\right] \geq \left[1 - H(1 - q_1 - q_3 - q_5)\right].$$

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

![Key rate comparison with fixed light intensity $\mu = 0.5$. Here we can see that the GLLP “tagging” formula for the “single-photon” component cannot hold under the BS attack when the transmittance $\eta < 0.6$.](image1)

![Key rate comparison with fixed transmittance $\eta = 0.2$. The GLLP “tagging” formula for the “single-photon” component cannot hold under the BS attack.](image2)
ist, since the announcement of phase $\phi_a$, $\phi_b$ will leak more information of the key bits $\kappa_a$ and $\kappa_b$.

Recently, Wang et al. proposed an eavesdropping strategy to the twin-field QKD protocol [37]. The attack can also be performed against the PM-QKD protocol. Under such an attack, Eve can learn all the key bits. The key rate provided by the GLLP formula, Eq. (C1), is 0.5 (for all the clicked signals) while that given by our security proof is strictly 0. This also shows the invalidation of GLLP key rate formula, and our security proof is still valid under such an attack.

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

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

[3] D. Mayers, Journal of the ACM (JACM) **48**, 351 (2001).

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

[5] P. W. Shor and J. Preskill, Physical Review Letters **85**, 441 (2000).

[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of cryptology **5**, 3 (1992).

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

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

[9] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Phys. Rev. Lett.* **92**, 217903 (2004).

[10] M. Takeoka, S. Guha, and M. M. Wilde, Nature Communications **5**, 5235 (2014).

[11] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature Communications **5**, 5235 (2014).

[12] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993).

[13] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).

[14] K. Azuma, K. Tamaki, and H.-K. Lo, Nature Communications **6** (2015).

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

[16] M. Lucamarini, Z. Yuan, J. Dynes, and A. Shields, Nature (2018), 10.1038/s41586-018-0066-6.

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

[18] X. Ma and M. Razavi, *Phys. Rev. A* **86**, 062319 (2012).

[19] X. Ma, *Quantum cryptography: from theory to practice*, Ph.D. thesis, University of Toronto (2008), also available in arXiv:0808.1385.

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

[21] J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, *Phys. Rev. Lett.* **114**, 180502 (2015).

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

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

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

[25] X.-B. Wang, *Phys. Rev. Lett.* **94**, 230503 (2005).

[26] C. W. Lim, B. Korzh, A. Martin, F. Bussieres, R. Thew, and H. Zbinden, *Applied Physics Letters* **105**, 221112 (2014).