Interfering-or-not-interfering quantum key distribution

Yang Yu [1], Wei Li [1,2], Le Wang [1], and Shengmei Zhao [1,2,*]

[1] *Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China*

[2] *Key Lab of Broadband Wireless Communication and Sensor Network Technology, Ministry of Education, Nanjing 210003, China*

(Received 15 December 2023; accepted 8 April 2024; published 6 May 2024)

Single-photon interference is the essential key for the recently well-known twin-field quantum key distribution (TF-QKD) to break the linear rate-distance limit and requires beams with identical polarizations. Inspired by this fact and aiming to improve the secret key rate, we propose a hybrid high-dimensional QKD named the interfering-or-not-interfering QKD (INI-QKD), in which both the polarization and phase degrees of freedom (DOFs) are adopted as information carriers. The protocol's security proof is analyzed based on entanglement distillation and three defined effective events, X_1, X_2, and X_3. The simulation shows that the X_1 event, from which only the phase information is extracted, exceeds TF-QKD's variants, while the X_2 and X_3 events, in which both types of information are decoded, can achieve twice the secret key rate as measurement-device-independent QKD (MDI-QKD). It is also proven that by adding the polarization DOF, INI-QKD obtains more resistance to phase mismatch than TF-QKD. Remarkably, these can all be achieved by simply altering the TF-QKD's measurement setup to that of MDI-QKD.

DOI: 10.1103/PhysRevA.109.052609

I. INTRODUCTION

Based on information-theoretic security guaranteed by quantum physics mechanics [1–3], quantum key distribution (QKD), one of the maturest quantum information implementations, has gone through rapid development [4–9]. In 2012, measurement-device-independent QKD (MDI-QKD) [10,11], in which the measurement site is placed in the middle, was proposed to prevent detection attacks and leakage of side-channel information. However, due to the transmission loss of photons, most of the protocols' performances are bounded by the rate-distance limit of a repeaterless QKD, or, in other words, the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [6]. It was not until 2018 that a MDI-type phase-encoding scheme called twin-field QKD (TF-QKD) was presented and showed the capacity of beating the PLOB bound [12]. TF-QKD's variants, such as phase-matching QKD (PM-QKD) [13–15], no-phase-postselection TF-QKD (NPP-TF-QKD) [16,17], and sending-or-not-sending TF-QKD (SNS-TF-QKD) [18,19], inherit its capacity of overcoming the limit with simpler procedures and more complete security analysis. Proof-of-principle experiments for them have all been implemented [20–24].

Despite the breakthroughs, the limited secret key rate has always been an obstacle to the requirement of current high-speed communication. One possible solution is the high-dimensional QKD (HD-QKD), which uses d-dimensional ($d > 2$) quantum states (qudits). It is shown that a qudit can carry more information and is more robust to eavesdropping compared with a qubit [25,26]. There have been extensive studies on various physical degrees of freedom (DOFs) to realize HD-QKD, such as orbital angular momentum [27–29], spatial modes [30], spin-orbit hybrid states [31], temporal modes [32], and so on. However, these protocols may be difficult to realize in practice because it is challenging to prepare and measure discrete HD states. Some of the schemes' switching speeds of the encoding and decoding devices are relatively low, limiting their ability to achieve a high secret key rate. Moreover, there has rarely been any HD-QKD research in the form of TF-QKD. So far, the polarization and phase are the most popular DOFs used in QKD schemes, and the related technologies have become mature. Multiple protocols based on these two DOFs have been proposed and experimentally implemented [10,20–24,33]. However, for all these QKD protocols, only one DOF is utilized, and the other one is not, which is wasteful and inefficient.

In this paper, we propose a so-called interfering-or-not-interfering QKD (INI-QKD) protocol to overcome the problem mentioned above, in which the key information is encoded in both the polarization and phase DOFs, and their corresponding bits are named the polarization bit and the phase bit. In the protocol, three effective events, X_1, X_2, and X_3, are defined according to the detection results. The users decide whether to extract both types of key bits or just the phase bit based on the three events. Also, the security is analyzed based on entanglement distillation [1,2]: Suppose that the users each have local qubits entangled with the prepared states and they measure these qubits after the interference to see their correlations.

The advantages of this protocol are as follows: (1) INI-QKD utilizes both the polarization and phase DOFs as information carriers, so that INI-QKD has a higher secret-key-rate performance. (2) The protocol's four-dimensional encoding system makes it leak less information under Eve's attack than two-dimensional protocols. (3) INI-QKD uses a

*zhaosm@njupt.edu.cn

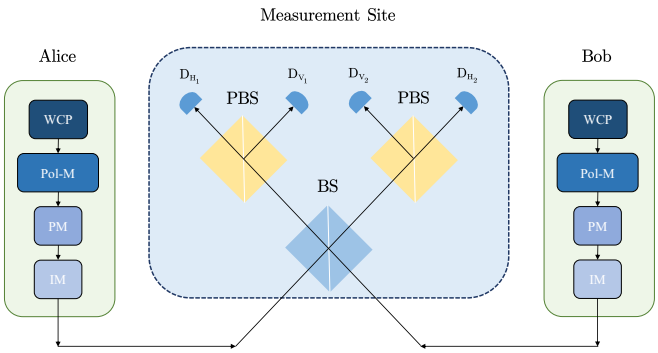

FIG. 1. Schematic diagram of INI-QKD: WCP, weak coherent pulse; Pol-M, polarization modulator; PM, phase modulator; IM, intensity modulator; BS, beam splitter; PBS, polarization beam splitter.

specific phase value and cuts off phase postselection and phase randomization, which can simplify the protocol's process and avoid intrinsic misalignment error caused by continuous phase postselection. (4) The protocol can rely less on the stabilization of phases than TF-QKD variants like PM-QKD. (5) INI-QKD's experimental structure is basically a combination of MDI-QKD and the phase-locking technique, which is utilized to lock the frequencies and phases of the users' lasers. This will make the protocol's practical implementation within the reach of current technologies.

The structure of this paper is organized as follows: A schematic description of the INI-QKD is presented in Sec. II. Section III demonstrates numerical simulations of the protocol's performance. Finally, Sec. IV summarizes the whole work.

II. PROTOCOL

A. Detailed description

The idea of INI-QKD protocol originates from the fact that two coherent light beams with the same polarizations can interfere, whereas the interference cannot occur if the two beams' polarizations are orthogonal. This distinguishable results makes it possible to simultaneously utilize both the polarization and phase DOFs as information carriers during the key distribution. A schematic diagram of INI-QKD is shown in Fig. 1. The authorized users prepare weak coherent pulses (WCPs), and each uses a polarization modulator and phase modulator to encode their polarization and phase bits into the pulses. Different light intensities in both bases are modulated by the intensity modulators. After traveling through two independent channels, the pulses from both sides interfere at a 50:50 beam splitter (BS) whose output arms each have a polarizing beam splitter (PBS) attached to project the light into two orthogonal polarization states in the rectilinear basis. Four single-photon detectors, D_{H_1}, D_{V_1}, D_{H_2}, and D_{V_2}, are employed to detect the photons. The protocol's detailed procedures are as follows.

Step 1. Alice (Bob) randomly decides whether the coherent states in each round should be prepared in the X basis or Z basis. In both bases, she (he) should choose the polarization bit $\kappa_{a(b)}^{\mathrm{pol}}$ and the polarization bit $\kappa_{a(b)}^{\mathrm{ph}}$ from $\{0, 1\}$ with *a priori* probability distribution $\{0.5, 0.5\}$. Once the X basis is chosen, Alice (Bob) prepares $|\sqrt{\mu}e^{i\pi\kappa_a^{\mathrm{ph}}}\rangle_{A_+}$ ($|\sqrt{\mu}e^{i\pi\kappa_b^{\mathrm{ph}}}\rangle_{B_+}$) if $\kappa_{a(b)}^{\mathrm{pol}} = 0$. Likewise, if $\kappa_{a(b)}^{\mathrm{pol}} = 1$, she (he) should prepare $|\sqrt{\mu}e^{i\pi\kappa_a^{\mathrm{ph}}}\rangle_{A_-}$ ($|\sqrt{\mu}e^{i\pi\kappa_b^{\mathrm{ph}}}\rangle_{B_-}$). Similarly, the states prepared in the Z basis should be $|\sqrt{\mu_A}e^{i\pi\kappa_a^{\mathrm{ph}}}\rangle_{A_H}$ ($|\sqrt{\mu_B}e^{i\pi\kappa_b^{\mathrm{ph}}}\rangle_{B_H}$) or $|\sqrt{\mu_A}e^{i\pi\kappa_a^{\mathrm{ph}}}\rangle_{A_V}$ ($|\sqrt{\mu_B}e^{i\pi\kappa_b^{\mathrm{ph}}}\rangle_{B_V}$). Here, the subscripts H, V, $+$, and $-$ denote the polarization states in rectilinear and diagonal bases, respectively. It should be noted that the intensities μ_A and μ_B are not fixed and are randomly chosen from a predetermined set.

Step 2. The states prepared by the authorized users are sent to the measurement site controlled by Charlie, who can be malicious. Charlie then performs measurements using the devices shown in Fig. 1 and reports only one of the following effective events:

(1) In the X_1 event, only D_{H_1} or D_{H_2} responds.

(2) In the X_2 event, detection event (D_{H_1}, D_{V_1}) or (D_{H_2}, D_{V_2}) happens.

(3) In the X_3 event, detection event (D_{H_1}, D_{V_2}) or (D_{V_1}, D_{H_2}) happens.

Step 3. The users along with Charlie repeat the above steps for sufficient times.

Step 4. The users announce their choices of bases for each round. They keep those rounds with the effective events in the same basis. X-basis effective events are used to generate the raw key bits, while those in Z basis help monitor Eve's eavesdropping.

Step 5. Some raw key bits are sampled for error tests. The rest are distilled for the final key bits after error correction and privacy amplification.

Note that to simplify the protocol's process and avoid possible intrinsic misalignment error, phase postselection operation and phase randomization are cut off. And the phase-locking technique used in TF-QKD is also required for INI-QKD.

It should also be noted that only when two detectors respond can Alice and Bob correlate each other's polarization and phase information; i.e., if the two detectors are on the same side, interference happens, but if both sides have one responding detector with orthogonal polarizations, e.g., (D_{H_1}, D_{V_2}), no interference occurs. These two cases correspond to the X_2 event and the X_3 event. In such events, the users can judge their polarizations' relation: They are identical (orthogonal) when the X_2 (X_3) event happens. After that, the users can relate their phases. However, if only one detector among the four clicks, the users will no longer confirm the correlation between their polarizations. When only D_{H_1} or D_{H_2} clicks, which corresponds to the X_1 event, the users can only correlate each other's phases. Thus, even though two sets of bit information are encoded in each WCP, it cannot be ensured that both sets are extracted in all effective events. In other words, the X_2 and X_3 parts of the protocol can be treated as a HD-QKD protocol, but the X_1 event cannot. That is the reason why INI-QKD is a hybrid HD-QKD protocol. In step 4, to generate raw key bits, the users correlate only their phase bits or both bits based on different X-basis effective events. Under certain events Bob should flip one or even both of his bits because the users' bits are anticorrelated. The details are given in Table I.

TABLE I. The correlations between users' polarization and phase bits under different effective events. "None" means that no related information can be extracted. "Same" indicates that Alice and Bob share the same bit. "Opposite" indicates that Alice and Bob share the opposite bit, and Bob should flip his bit.

	Effective events					
Key	X_1 event		X_2 event		X_3 event	
bits	D_{H_1}	D_{H_2}	(D_{H_1}, D_{V_1})	(D_{H_2}, D_{V_2})	(D_{H_1}, D_{V_2})	(D_{V_1}, D_{H_2})
$\kappa^{\text{pol}}_{a(b)}$	None	None	Same	Same	Opposite	Opposite
$\kappa^{\text{ph}}_{a(b)}$	Same	Opposite	Same	Opposite	Same	Opposite

As can be seen, Alice and Bob can correlate both their polarization bits and phase bits when X_2 or X_3 events happen. But they can only extract phase information when X_1 event happens.

B. Secret key rate

As mentioned above, there are three effective events defined in the proposed protocol. Since the cases for the three events are different, the total secret key rate can be estimated from three parts, which can be calculated separately, similar to those discussed in Refs. [34,35]. Based on the security analysis using entanglement distillation, INI-QKD's secret key rate can be given as

$$R = \sum_{i=1}^{3} R^{X_i}, \quad i \in \{1,2,3\},$$
$$R^{X_i} = Q_\mu^{X_i}\left[1 - H\left(E_\mu^{\text{ph},X_i}\right) - I_E^U - fH\left(E_\mu^{\text{bit},X_i}\right)\right], \quad (1)$$

where R is the secret key rate per pulse; Q_μ, E_μ^{ph}, and E_μ^{bit} denote the overall gain, phase-error rate, and quantum-bit-error rate (QBER), respectively; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function; and the superscripts X_i $(i \in \{1,2,3\})$ represent the three effective events. It should be noted that there is an upper bound of mutual information I_E^U in Eq. (1) that the eavesdropper Eve could have (on users' key bits) by using beam-splitting attack. For simplicity, the transmission loss is neglected when the security is analyzed. However, since the secret bits are encoded into the polarization and phase, Eve may obtain the information by *collecting* and measuring the states lost during transmission. The beam-splitting attack is one of the possible attack strategies for the proposed protocol. The details are analyzed in Appendix B.

Device imperfections along with the environment may not allow the right effective events, which leads to bit errors. Since those errors could happen in both the polarization bit and phase bit or only one of them, all possible situations should be analyzed under different encoded bit combinations to calculate the QBER. Without loss of generality, one may consider only two polarization bit combinations with $\kappa_a^{\text{ph}} = \kappa_b^{\text{ph}} = 0$ because of the symmetry. Table II lists the accuracy of decoded bits under certain encoded information combinations and effective events. It is helpful for calculating the protocol's QBER (see the details in Appendix C). For example, when both users' polarization bits are zero, the right detection event is (D_{H_1}, D_{V_1}) or only D_{H_1}. Thus, if (D_{H_1}, D_{V_2}) happens, a bit-flip error will occur in the polarization bit.

TABLE III. The parameters adopted in the simulations. P_d is the detectors' dark-count rate, η_d is the detection efficiency, α is the channel's loss rate, f denotes the error-correction efficiency, and M represents the number of phase slices over $[0, 2\pi)$ in PM-QKD.

	Parameter				
	P_d	η_d	α	f	M
Value	8×10^{-8}	0.145	0.2	1.15	16

III. SIMULATION

In this section, the numerical simulations of INI-QKD are presented under the assumption of symmetrical lossy channels and identical detectors. The simulation parameters are listed in Table III. With the method of full optimization, the optimized secret key rates for each effective event and the whole protocol are presented. For comparison, the performance of three well-known TF-QKD variants, NPP-TF-QKD (phase encoding, no phase randomization, no phase postselection) [16], SNS-TF-QKD (intensity encoding, phase randomization) [18], and PM-QKD (phase encoding, phase randomization, phase postselection) [13], along with phase-encoding MDI-QKD [33], is also presented. All the results are demonstrated in Fig. 2. It should be noted that no optical misalignment is considered during the simulation except that caused by phase postselection in PM-QKD.

The results in Fig. 2 show that the proposed protocol has a considerably high secret key rate composed of three parts,

TABLE II. The accuracy of decoded bits under certain encoded information combinations and effective events.

	Effective events					
	X_1 event		X_2 event		X_3 event	
$(\kappa_a^{\text{pol}}, \kappa_b^{\text{pol}})$	D_{H_1}	D_{H_2}	(D_{H_1}, D_{V_1})	(D_{H_2}, D_{V_2})	(D_{H_1}, D_{V_2})	(D_{V_1}, D_{H_2})
(0,0)	$\kappa^{\text{pol}}_{a(b)}$: none $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: none $\kappa^{\text{ph}}_{a(b)}$: wrong	$\kappa^{\text{pol}}_{a(b)}$: right $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: right $\kappa^{\text{ph}}_{a(b)}$: wrong	$\kappa^{\text{pol}}_{a(b)}$: wrong $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: wrong $\kappa^{\text{ph}}_{a(b)}$: wrong
(0,1)	$\kappa^{\text{pol}}_{a(b)}$: none $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: none $\kappa^{\text{ph}}_{a(b)}$: wrong	$\kappa^{\text{pol}}_{a(b)}$: wrong $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: wrong $\kappa^{\text{ph}}_{a(b)}$: wrong	$\kappa^{\text{pol}}_{a(b)}$: right $\kappa^{\text{ph}}_{a(b)}$: right	$\kappa^{\text{pol}}_{a(b)}$: right $\kappa^{\text{ph}}_{a(b)}$: wrong

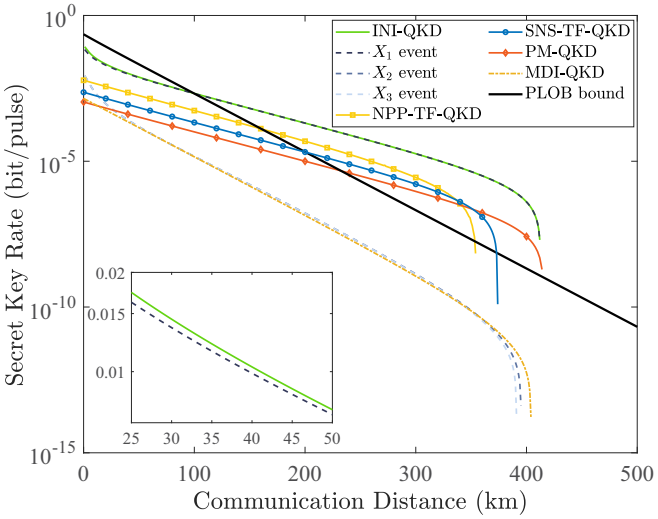

FIG. 2. The simulations of INI-QKD and all three of its effective events' secret-key-rate performances, along with those of NPP-TF-QKD, SNS-TF-QKD, PM-QKD, and MDI-QKD. The PLOB bound is also illustrated.

the X_1, X_2, and X_3 events. The X_2 and X_3 events together make up the high-dimensional part of INI-QKD and have definitions similar to MDI-QKD. The simulation result shows that the performance of each one is almost the same as that of MDI-QKD. Thus, these two events may be treated as a high-dimensional MDI-QKD. Compared to X_2 and X_3 events, the X_1 event provides a much higher secret key rate and can surpass the PLOB bound. Therefore, the secrete-key-rate performance of the proposed protocol is slightly higher than that contributed by the X_1 event. The reason is that the X_1 event is a one-photon-order detection event, while X_2 and X_3 events are two-photon-order detection events, which causes their secret key rates to be bounded by $O(\sqrt{\eta})$ and $O(\eta)$, respectively.

Mutual information obtained by a potential eavesdropper using the beam-splitting attack is considered in the protocol. Its upper bound can be calculated based on the largest probability of Eve unambiguously discriminating the prepared states, which is $I_E^U = 1 - \frac{1}{9}[e^{-2(1-\eta_t)\mu} + 2e^{-(1-\eta_t)\mu}]^2$. Note that I_E^U remains in all three effective events. That is because both the polarization and phase DOFs are implemented in INI-QKD, and there are four total states prepared by the users. Even when the X_1 event happens and only the phase bit is extracted, from Eve's perspective, she still cannot judge the users' polarization choices and needs to identify the states she has out of four states. Meanwhile, just like X_1 event, TF-QKD and its variants all have a secret key rate which is bounded by $O(\sqrt{\eta})$. Compared with TF-QKD's notable variants (NPP-TF-QKD, SNS-TF-QKD, and PM-QKD), the X_1 event performs better. The reason is that there is a big difference between them. Take PM-QKD as an example. The users encode only one bit of information into phases of each WCP, and that means Eve needs to distinguish between only two states after phase postselection. This indicates that INI-QKD has more uncertainty than PM-QKD; i.e., INI-QKD's states are less likely to be identified by Eve than PM-QKD's counterparts. The greatest information that Eve can get from PM-QKD through the beam-splitting attack is $I_E^{\mathrm{PM},U} = 1 - e^{-4(1-\eta_t)\mu}$ [13], which is clearly larger than I_E^U, meaning the PM-QKD may leak more information than INI-QKD (see the details in Appendix B). This result can be similarly applied to TF-QKD's other variants.

Furthermore, we discuss the secret key rate's relationships with the polarization misalignment as well as the phase mismatch. Here, we adopt the model in Ref. [36] to describe the polarization misalignment error. Because of the channels' symmetry, we assume that $\sin^2(\theta_A) = \sin^2(\theta_B) = e_d/2$, where $\theta_{A(B)}$ is the polarization-rotation angle and e_d is the total polarization-misalignment-error rate. Thus, there are two cases from this assumption, that is, $\theta_A = \theta_B = \arcsin\sqrt{e_d/2}$ (case I) and $\theta_A = -\theta_B = \arcsin\sqrt{e_d/2}$ (case II). From

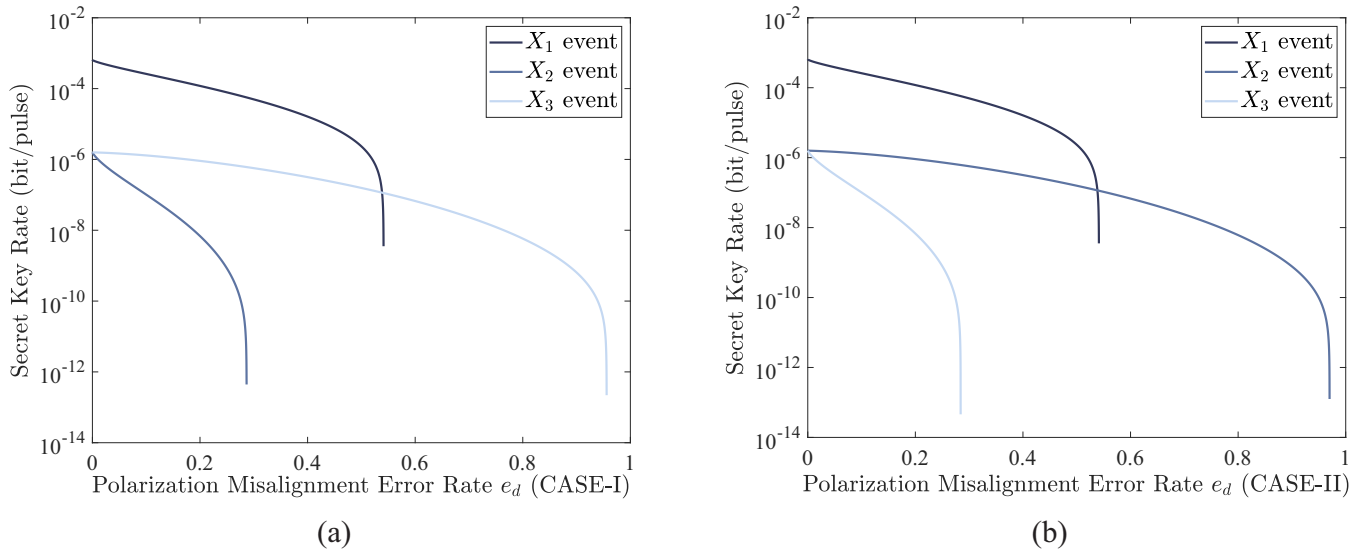

FIG. 3. Secret key rate against the polarization-misalignment-error rate e_d of all three of INI-QKD's effective events in both cases. (a) Case I. (b) Case II.

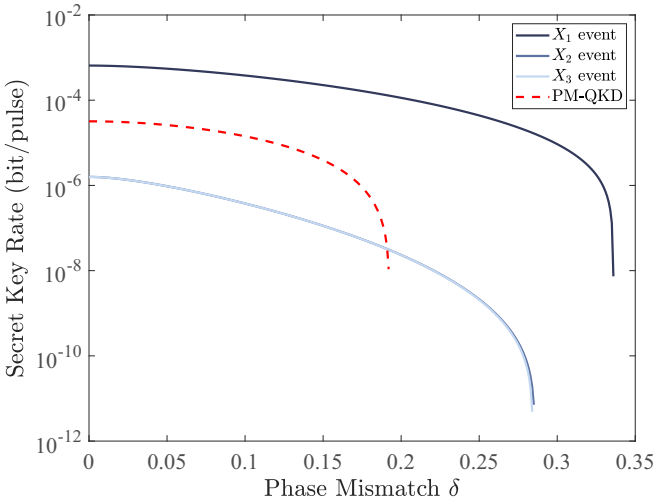

FIG. 4. Secret key rate against the phase mismatch δ of all three of INI-QKD's effective events and PM-QKD.

Appendix C, it can be seen that the light intensities of the detectors are not relevant to the global phases of both sides (ϕ_A and ϕ_B), but their difference $\phi_\delta = \phi_B - \phi_A$. So we use $\phi_\delta = \delta\pi$ to represent phase mismatch in the following. We first demonstrate the secret key rate of the proposed INI-QKD against the polarization-misalignment-error rate e_d with the communication distance fixed at 150 km in Fig. 3, where Fig. 3(a) shows case I and Fig. 3(b) shows case II. It is shown that, for case I, the X_3 event is most robust against the polarization misalignment, while the X_2 event's performance drops sharply with increasing e_d. When e_d exceeds 0.54, the X_3 event has a larger secret key rate than that of the X_1 event. For case II, as shown in Fig. 3(b), the performance by the X_1 event is the same as that in case I, while the X_2 event is most robust against polarization misalignment, and the secret-key-rate performance of the X_3 event drops quickly. Moreover, we demonstrate the secret-key-rate performance against phase mismatch at a distance of 150 km in Fig. 4. The simulation of PM-QKD is also plotted for comparison. The results show that the phase-mismatch tolerances of the X_2 and X_3 events are mostly the same. But the X_1 event's secret-key-rate performance drops a little slower than that of the X_2 or X_3 event when δ becomes larger. The results also show that the performance of PM-QKD completely vanishes when δ reaches 0.2, while the phase mismatches for the X_1 event and the X_2 and X_3 events are 0.336 and 0.285, respectively. This hints that INI-QKD has a little more robustness against phase mismatch than the TF-QKD variants.

IV. CONCLUSION

In this paper, we proposed a hybrid-encoding QKD protocol named interfering-or-not-interfering QKD. The proposed INI-QKD has a structure similar to MDI-QKD. However, its information is encoded in both the polarizations and phases of the coherent states. Three effective events, the encoding and decoding principles and possible error-generating situations, were well defined and discussed. The protocol's security was analyzed by using the entanglement distillation, and the mutual information obtained by a potential eavesdropper using the beam-splitting attack was discussed. The simulation results showed that the X_1 event, in which only the phase bit is encoded, performs better than the variants of TF-QKD, while the X_2 and X_3 events, in which users decode both the polarization and phase bits, obtain a secret key rate 2 times higher than that of MDI-QKD. In addition, the relationships between the protocol's performance and polarization misalignment along with phase mismatch were also discussed. When both channels' polarization-rotation angles are the same, the X_3 event can endure high polarization misalignment. As for the opposite-angle case, the X_2 event has the ability to tolerate the highest polarization misalignment. All three events are more robust against the phase match than those of the TF-QKD variants. The protocol is a promising candidate for quantum key distribution because of its high performance and experimental feasibility under current technologies.

ACKNOWLEDGMENTS

This work was partially supported by the National Natural Science Foundation of China (Grants No. 62375140, No. 62001249, and No. 61871234) and the Postgraduate Research and Practice Innovation Program of Jiangsu Province (Grant No. KYCX22_0958).

APPENDIX A: SECURITY PROOF

In this Appendix, a security proof for the INI-QKD protocol based on entanglement distillation is presented. Suppose that the users each have two local qubits entangled with the coherent light that they prepare. Since both the polarization bit and phase bit are chosen with the *a priori* probability distribution {0.5, 0.5}, Alice's prepared state can be written as

$$\frac{1}{2}\big[\,|0\rangle_a^{\rm pol}|0\rangle_a^{\rm ph}|\sqrt{\mu}\rangle_{A_+} + |0\rangle_a^{\rm pol}|1\rangle_a^{\rm ph}|-\sqrt{\mu}\rangle_{A_+} + |1\rangle_a^{\rm pol}|0\rangle_a^{\rm ph}|\sqrt{\mu}\rangle_{A_-} + |1\rangle_a^{\rm pol}|1\rangle_a^{\rm ph}|-\sqrt{\mu}\rangle_{A_-}\,\big], \tag{A1}$$

where $|\cdot\rangle_a^{\rm pol}$ and $|\cdot\rangle_a^{\rm ph}$ represent Alice's polarization and phase qubits and $|\cdot\rangle_{A_\pm}$ denotes the coherent state prepared in one of the diagonal polarizations. For simplicity, we shall express $|\cdot\rangle_a^{\rm pol}|\cdot\rangle_a^{\rm ph}$ as $|\cdot\cdot\rangle_a$. Bob's state has a similar expression.

For simplicity, we may neglect the effect of dark count and channel loss for now. Thus, after passing through the BS and PBSs at the measurement site, the users' states evolve as

$$\begin{aligned}\frac{1}{4}\big[\,&|0000\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_1} + |0001\rangle_{ab}|\sqrt{\mu}\rangle_{H_2}|\sqrt{\mu}\rangle_{V_2} + |0010\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_2}\\ &+ |0011\rangle_{ab}|\sqrt{\mu}\rangle_{V_1}|\sqrt{\mu}\rangle_{H_2} + |0100\rangle_{ab}|-\sqrt{\mu}\rangle_{H_2}|-\sqrt{\mu}\rangle_{V_2} + |0101\rangle_{ab}|-\sqrt{\mu}\rangle_{H_1}|-\sqrt{\mu}\rangle_{V_1}\\ &+ |0110\rangle_{ab}|-\sqrt{\mu}\rangle_{V_1}|-\sqrt{\mu}\rangle_{H_2} + |0111\rangle_{ab}|-\sqrt{\mu}\rangle_{H_1}|-\sqrt{\mu}\rangle_{V_2} + |1000\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|-\sqrt{\mu}\rangle_{V_2}\end{aligned}$$

$$+|1001\rangle_{ab}|-\sqrt{\mu}\rangle_{V_1}|\sqrt{\mu}\rangle_{H_2}+|1010\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|-\sqrt{\mu}\rangle_{V_1}+|1011\rangle_{ab}|\sqrt{\mu}\rangle_{H_2}|-\sqrt{\mu}\rangle_{V_2}$$
$$+|1100\rangle_{ab}|\sqrt{\mu}\rangle_{V_1}|-\sqrt{\mu}\rangle_{H_2}+|1101\rangle_{ab}|-\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_2}+|1110\rangle_{ab}|-\sqrt{\mu}\rangle_{H_2}|\sqrt{\mu}\rangle_{V_2}$$
$$+|1111\rangle_{ab}|-\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_1}\big]. \tag{A2}$$

Since the coherent state can be expressed as

$$|\sqrt{\mu}\rangle=e^{-\frac{\mu}{2}}\sum_{i=0}^{\infty}\sqrt{\frac{\mu^i}{i!}}|i\rangle=e^{-\frac{\mu}{2}}|0\rangle+e^{-\frac{\mu}{2}}\sum_{i=1}^{\infty}\sqrt{\frac{\mu^i}{i!}}|i\rangle=e^{-\frac{\mu}{2}}|0\rangle+|\sqrt{\mu'}\rangle, \tag{A3}$$

Eq. (A2) can be further derived. Take the $|0000\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_1}$ part as an example:

$$|0000\rangle_{ab}|\sqrt{\mu}\rangle_{H_1}|\sqrt{\mu}\rangle_{V_1}=|0000\rangle_{ab}\big(e^{-\mu}|0\rangle_{H_1}|0\rangle_{V_1}+e^{-\frac{\mu}{2}}|0\rangle_{H_1}|\sqrt{\mu'}\rangle_{V_1}+e^{-\frac{\mu}{2}}|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}+|\sqrt{\mu'}\rangle_{H_1}|\sqrt{\mu'}\rangle_{V_1}\big), \tag{A4}$$

where $|0\rangle_{H_1}|0\rangle_{V_1}$ causes no detectors to respond, $|0\rangle_{H_1}|\sqrt{\mu'}\rangle_{V_1}$ and $|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}$ make only D_{V_1} and D_{H_1} click, respectively, and $|\sqrt{\mu'}\rangle_{H_1}|\sqrt{\mu'}\rangle_{V_1}$ makes both detectors click. With this method, the protocol's security analysis can go forward according to different effective events.

1. X_1 event

In this section, we mainly focus on those which can cause only D_{H_1} to click as an example of an X_1 effective event in Eq. (A2):

$$\begin{aligned}
&e^{\frac{-\mu}{2}}\big[|0000\rangle_{ab}|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}+|0010\rangle_{ab}|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_2}+|0101\rangle_{ab}|-\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}\\
&\quad+|0111\rangle_{ab}|-\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_2}+|1000\rangle_{ab}|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_2}+|1010\rangle_{ab}|\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}\\
&\quad+|1101\rangle_{ab}|-\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_2}+|1111\rangle_{ab}|-\sqrt{\mu'}\rangle_{H_1}|0\rangle_{V_1}\big]\\
&=2e^{-\mu}\sum_{m=1}^{\infty}\sqrt{\frac{\mu^m}{m!}}|m\rangle_{H_1}\otimes\Big\{\frac{1}{\sqrt{2}}\big(|00\rangle_{ab}^{\mathrm{pol}}+|11\rangle_{ab}^{\mathrm{pol}}\big)\otimes\frac{1}{\sqrt{2}}\big[|00\rangle_{ab}^{\mathrm{ph}}+(-1)^m|11\rangle_{ab}^{\mathrm{ph}}\big]\\
&\quad+\frac{1}{\sqrt{2}}\big(|01\rangle_{ab}^{\mathrm{pol}}+|10\rangle_{ab}^{\mathrm{pol}}\big)\otimes\frac{1}{\sqrt{2}}\big[|00\rangle_{ab}^{\mathrm{ph}}+(-1)^m|11\rangle_{ab}^{\mathrm{ph}}\big]\Big\}\\
&=2\sqrt{2}e^{-\mu}\sum_{m=1}^{\infty}\sqrt{\frac{\mu^m}{m!}}|m\rangle_{H_1}\otimes\left[\frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{ab}^{\mathrm{pol}}+|\Psi^+\rangle_{ab}^{\mathrm{pol}}\big)\otimes|\Phi^{\pm}\rangle_{ab}^{\mathrm{ph}}\right].
\end{aligned} \tag{A5}$$

It can be seen that the polarization bit's correlation is not certain. That is the reason why the phase bit is decoded when X_1 event happens. If we take away the polarization bit, Eq. (A5) can be further derived as

$$4\sqrt{2}e^{-\mu}\sum_{m=1}^{\infty}\sqrt{\frac{\mu^m}{m!}}|m\rangle_{H_1}\otimes|\Phi^{\pm}\rangle_{ab}^{\mathrm{ph}}. \tag{A6}$$

From Eq. (A6), it can be seen that an Einstein-Podolsky-Rosen pair, say, a Bell state, has been distilled. This means that in INI-QKD when the X_1 event occurs, a Bell-state measurement is implemented in the users' phase bits. One can also see that phase error occurs in the extracted Bell state when m, the number of photons arriving at detector D_{H_1}, is even. The result is similar to that derived in Ref. [14]. Thus, the phase-error rate of only D_{H_1} responding can be presented as follows:

$$\begin{aligned}
E_{\mu}^{\mathrm{ph},H_1}&=\frac{EQ_{\mu}^{\mathrm{ph},H_1}}{Q_{\mu}^{H_1}}=\frac{1}{Q_{\mu}^{H_1}}\big[\Pr\big(\mathrm{even},D_{H_1},++\big)+\Pr\big(\mathrm{even},D_{H_1},+-\big)+\Pr\big(\mathrm{even},D_{H_1},-+\big)+\Pr\big(\mathrm{even},D_{H_1},--\big)\big]\\
&=\frac{1}{2Q_{\mu}^{H_1}}\big[\Pr\big(\mathrm{even},D_{H_1}|++\big)+\Pr\big(\mathrm{even},D_{H_1}|+-\big)\big],
\end{aligned} \tag{A7}$$

where even means $m\in$ even. $\Pr(\mathrm{even},D_{H_1}|++)$ and $\Pr(\mathrm{even},D_{H_1}|+-)$ can be formulated as

$$\begin{aligned}
\Pr(\mathrm{even},D_{H_1}|++)&=(1-P_d)^3P_{I_{V_1}^{++}}(0)P_{I_{H_2}^{++}}(0)P_{I_{V_2}^{++}}(0)\sum_{m\in\mathrm{even}}^{\infty}P_{I_{H_1}^{++}}(m)\\
&=(1-P_d)^3\exp\big(-I_{H_1}^{++}-I_{V_1}^{++}-I_{H_2}^{++}-I_{V_2}^{++}\big)\big[\cosh\big(I_{H_1}^{++}\big)-1+P_d\big],\\
\Pr(\mathrm{even},D_{H_1}|+-)&=(1-P_d)^3\exp\big(-I_{H_1}^{+-}-I_{V_1}^{+-}-I_{H_2}^{+-}-I_{V_2}^{+-}\big)\big[\cosh\big(I_{H_1}^{+-}\big)-1+P_d\big].
\end{aligned} \tag{A8}$$

$P_{I_X}(m)$ is the probability of the I_X-intensity coherent light which arrives at detector D_X containing m photons.

TABLE IV. The distilled Bell states under different circumstances. m and n denote the photon number of the coherent light that arrives at D_{H_1} and D_{V_1}, respectively.

	n	
m	Odd	Even
Odd	$\|\Phi^-\rangle_{ab}^{\text{pol}} \otimes \|\Phi^+\rangle_{ab}^{\text{ph}}$ phase error: 0	$\|\Phi^+\rangle_{ab}^{\text{pol}} \otimes \|\Phi^-\rangle_{ab}^{\text{ph}}$ phase error: 2
Even	$\|\Phi^-\rangle_{ab}^{\text{pol}} \otimes \|\Phi^-\rangle_{ab}^{\text{ph}}$ phase error: 1	$\|\Phi^+\rangle_{ab}^{\text{pol}} \otimes \|\Phi^+\rangle_{ab}^{\text{ph}}$ phase error: 1

2. X_2 and X_3 events

For symmetry reasons, X_2 and X_3 events are discussed together, and we will take the (D_{H_1}, D_{V_1}) click event as an example. However, in this case, instead of one Bell state from the users' phase bits, the users actually distill Bell states from both the phase bit and polarization bit using the same method as in Eq. (A5). Thus, when the X_2 or X_3 event happens in the protocol, two independent Bell-state measurements are implemented. The details of the Bell states and corresponding phase errors under different circumstances are shown in Table IV.

The phase-error rate when a (D_{H_1}, D_{V_1}) click event happens can be calculated as

$$E_\mu^{\text{ph},H_1V_1} = \frac{1}{2Q_\mu^{H_1V_1}}\big[\Pr(\text{ phase error}, D_{H_1}D_{V_1}|++) + \Pr(\text{ phase error}, D_{H_1}D_{V_1}|+-)\big]. \tag{A9}$$

Based on Table IV, one can get the expression for $\Pr(\text{ phase error}, D_{H_1}D_{V_1}|++)$,

$$\begin{aligned}\Pr(\text{ phase error}, D_{H_1}D_{V_1}|++) &= 2\Pr\big[(o,e), D_{H_1}D_{V_1}|++\big] + \Pr\big[(e,o), D_{H_1}D_{V_1}|++\big] + \Pr\big[(e,e), D_{H_1}D_{V_1}|++\big] \\ &= (1-P_d)^2 \exp\big(-I_{H_1}^{++} - I_{V_1}^{++} - I_{H_2}^{++} - I_{V_2}^{++}\big)\big\{2\sinh\big(I_{H_1}^{++}\big)\big[\cosh(I_{V_1}^{++}) - 1 + P_d\big] \\ &\quad + \big[\cosh\big(I_{H_1}^{++}\big) - 1 + P_d\big]\sinh\big(I_{V_1}^{++}\big) + \big[\cosh\big(I_{H_1}^{++}\big) - 1 + P_d\big]\big[\cosh(I_{V_1}^{++}) - 1 + P_d\big]\big\}.\end{aligned} \tag{A10}$$

where (o,e) is short for $(m,n) \in (\text{odd}, \text{even})$, with similar meanings for (e,o) and (e,e). The formula for $\Pr(\text{ phase error}, D_{H_1}D_{V_1}|+-)$ can be derived using the same method.

APPENDIX B: BEAM-SPLITTING ATTACK: MUTUAL INFORMATION

In the security analysis in Appendix A, channel loss is neglected. However, the situation where eavesdropper Eve obtains key information using the states coupled to the environment should be considered. Here, we refer to the beam-splitting attack.

In the beam-splitting attack, Eve puts BSs with transmittance η_t, the same as that of the channel, on both users' sides and replace the lossy lines with an ideal loss-free one to simulate the channels. The output reflected light from the BSs is then stored in Eve's quantum memory. When the basis announcement is over, Eve picks the stored states from the rounds that form the final key bits and performs unambiguous state discrimination on them. Eve's devices are all perfect. We can first calculate Eve's largest probability of unambiguously discriminating the prepared states, with which the uncertainty of Eve using a beam-splitting attack can be quantified, i.e., the mutual information.

We first consider Eve's attack on Alice. Alice's stored state in the X basis is equally likely to be one of the following four states:

$$\begin{aligned}|\psi_0\rangle &= |\sqrt{(1-\eta_t)\mu}\rangle_+ = |\sqrt{(1-\eta_t)\mu/2}\rangle_H |\sqrt{(1-\eta_t)\mu/2}\rangle_V, \\ |\psi_1\rangle &= |-\sqrt{(1-\eta_t)\mu}\rangle_+ = |-\sqrt{(1-\eta_t)\mu/2}\rangle_H |-\sqrt{(1-\eta_t)\mu/2}\rangle_V, \\ |\psi_2\rangle &= |\sqrt{(1-\eta_t)\mu}\rangle_- = |\sqrt{(1-\eta_t)\mu/2}\rangle_H |-\sqrt{(1-\eta_t)\mu/2}\rangle_V, \\ |\psi_3\rangle &= |-\sqrt{(1-\eta_t)\mu}\rangle_- = |-\sqrt{(1-\eta_t)\mu/2}\rangle_H |\sqrt{(1-\eta_t)\mu/2}\rangle_V.\end{aligned} \tag{B1}$$

The upper bound of Eve's successful unambiguous identification probability P_{success} can be given according to the formula in Ref. [37],

$$P_{\text{success}} \leqslant 1 - \frac{1}{N-1}\sum_{i\neq j}\sqrt{p_i p_j}\,|\langle\psi_i|\psi_j\rangle|, \tag{B2}$$

where in this case $N = 4$ and $p_i = p_j = 1/4$ are prepared probabilities of the states. The result turns out to be a function of η_t and the intensity μ,

$$P_{\text{success}}^U = 1 - \tfrac{1}{12}[4e^{-2(1-\eta_t)\mu} + 8e^{-(1-\eta_t)\mu}] = 1 - \tfrac{1}{3}[e^{-2(1-\eta_t)\mu} + 2e^{-(1-\eta_t)\mu}]. \tag{B3}$$

A similar result can be applied to Bob's side. With the largest probability of the states from both sides being unambiguously identified, the upper bound of the mutual information from the beam-splitting attack is

$$I_E^U = 1 - \left(1 - P_{\text{success}}^U\right)^2 = 1 - \tfrac{1}{9}[e^{-2(1-\eta_t)\mu} + 2e^{-(1-\eta_t)\mu}]^2. \tag{B4}$$

It should be noted that this bound is identical for all three effective events. Even though the users extract phase information only when the X_1 event happens, Eve still does not know both sides' polarizations. Thus, she still needs to identify the states out of four total states. Hence, the mutual information still remains. Meanwhile, we take PM-QKD, which is a phase-encoding variant of TF-QKD, as an example for comparison. Its largest probability of the prepared states being unambiguously discriminated in the protocol in Eq. (B2) can be calculated as

$$P_{\text{success}}^{\text{PM},U} = 1 - |\langle\sqrt{(1-\eta_t)\mu}| - \sqrt{(1-\eta_t)\mu}\rangle| = 1 - e^{-2(1-\eta_t)\mu}. \tag{B5}$$

With the probability, the upper bound of the mutual information that Eve is able to get using the beam-splitter attack can be obtained:

$$I_E^{\text{PM},U} = 1 - \left(1 - P_{\text{success}}^{\text{PM},U}\right)^2 = 1 - e^{-4(1-\eta_t)\mu}. \tag{B6}$$

Clearly, it can be seen that $I_E^U < I_E^{\text{PM},U}$, which indicates that compared with the phase-encoding TF-QKD variants, INI-QKD leaks less information due to high-dimensional encoding.

APPENDIX C: OVERALL GAINS AND QBERS

In this Appendix, we present the calculation of detection probabilities in this protocol in different situations. The overall gains and QBERs can be further evaluated. Without loss of generality, we consider only the cases where $(\kappa_a^{\text{pol}}, \kappa_b^{\text{pol}}) = (0, 0)$ and $(0, 1)$ and $\kappa_a^{\text{ph}} = \kappa_b^{\text{ph}} = 0$.

Practically, we take polarization misalignment and phase mismatch into consideration. For simplicity, we assume that polarization misalignment is mainly caused by the states' polarization rotation during their transmission, which can be modeled with a unitary operator,

$$U_{A(B)} = \begin{pmatrix} \cos\theta_{A(B)} & -\sin\theta_{A(B)} \\ \sin\theta_{A(B)} & \cos\theta_{A(B)} \end{pmatrix}. \tag{C1}$$

As for phase mismatch, we shift the phases of Alice's and Bob's by angles ϕ_A and ϕ_B, with the difference $\phi_\delta = \phi_B - \phi_A$.

1. Case 1: $(|\sqrt{\mu}\rangle_{A_+}, |\sqrt{\mu}\rangle_{B_+})$

In this case, the states evolve as

$$\begin{aligned}
|\sqrt{\mu}e^{i\phi_A}\rangle_{A_+}|\sqrt{\mu}e^{i\phi_B}\rangle_{B_+} &\xrightarrow{\text{channel}} \left|(\cos\theta_A - \sin\theta_A)\sqrt{\frac{\mu\eta}{2}}e^{i\phi_A}\right\rangle_{A_H}\left|(\sin\theta_A + \cos\theta_A)\sqrt{\frac{\mu\eta}{2}}e^{i\phi_A}\right\rangle_{A_V} \\
&\quad\otimes\left|(\cos\theta_B - \sin\theta_B)\sqrt{\frac{\mu\eta}{2}}e^{i\phi_B}\right\rangle_{B_H}\left|(\sin\theta_B + \sin\theta_B)\sqrt{\frac{\mu\eta}{2}}e^{i\phi_B}\right\rangle_{B_V} \\
&\xrightarrow{\text{BS,PBSs}} \left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A - \sin\theta_A) + e^{i\phi_\delta}(\cos\theta_B - \sin\theta_B)]\right\rangle_{H_1} \\
&\quad\otimes\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A + \sin\theta_A) + e^{i\phi_\delta}(\cos\theta_B + \sin\theta_B)]\right\rangle_{V_1} \\
&\quad\otimes\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A - \sin\theta_A) - e^{i\phi_\delta}(\cos\theta_B - \sin\theta_B)]\right\rangle_{H_2} \\
&\quad\otimes\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A + \sin\theta_A) - e^{i\phi_\delta}(\cos\theta_B + \sin\theta_B)]\right\rangle_{V_2}.
\end{aligned} \tag{C2}$$

Using the above formulas, we can obtain the intensities of the light arriving at the detectors, $I_{H_1}^{++}$, $I_{V_1}^{++}$, $I_{H_2}^{++}$, and $I_{V_2}^{++}$. Then, the detection-click probabilities can be calculated:

$$\begin{aligned}
&\Pr(\overline{H_1}|+,+) = (1-P_d)e^{-I_{H_1}^{++}}, \quad \Pr(\overline{V_1}|+,+) = (1-P_d)e^{-I_{V_1}^{++}}, \\
&\Pr(\overline{H_2}|+,+) = (1-P_d)e^{-I_{H_2}^{++}}, \quad \Pr(\overline{V_2}|+,+) = (1-P_d)e^{-I_{V_2}^{++}}, \\
&\Pr(H_1|+,+) = 1 - \Pr(\overline{H_1}|+,+), \quad \Pr(V_1|+,+) = 1 - \Pr(\overline{V_1}|+,+), \\
&\Pr(H_2|+,+) = 1 - \Pr(\overline{H_2}|+,+), \quad \Pr(V_2|+,+) = 1 - \Pr(\overline{V_2}|+,+),
\end{aligned} \tag{C3}$$

where $\Pr(\overline{H_1}|+,+)$, $\Pr(\overline{V_1}|+,+)$, $\Pr(\overline{H_2}|+,+)$, and $\Pr(\overline{V_2}|+,+)$ are the probabilities of no corresponding detector click, while $\Pr(H_1|+,+)$, $\Pr(V_1|+,+)$, $\Pr(H_2|+,+)$, and $\Pr(V_2|+,+)$ denote the click probabilities. With these, we can evaluate the probabilities of the effective events, say, the probability of only D_{H_1} responding, $\Pr(D_{H_1}|+,+) = \Pr(H_1|+,+)\Pr(\overline{V_1}|+,+)\Pr(\overline{H_2}|+,+)\Pr(\overline{V_2}|+,+)$.

2. Case 2: $(|\sqrt{\mu}\rangle_{A_+}, |\sqrt{\mu}\rangle_{B_-})$

After an evolution similar to that in Eq. (C2), the result of this case turns out to be

$$\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A-\sin\theta_A)+e^{i\phi_\delta}(\cos\theta_B+\sin\theta_B)]\right\rangle_{H_1}\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A+\sin\theta_A)-e^{i\phi_\delta}(\cos\theta_B-\sin\theta_B)]\right\rangle_{V_1}$$
$$\otimes\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A-\sin\theta_A)-e^{i\phi_\delta}(\cos\theta_B+\sin\theta_B)]\right\rangle_{H_2}\left|\frac{\sqrt{\mu\eta}}{2}e^{i\phi_A}[(\cos\theta_A+\sin\theta_A)+e^{i\phi_\delta}(\cos\theta_B-\sin\theta_B)]\right\rangle_{V_2}. \quad \text{(C4)}$$

Just as in the above case, we can calculate the detectors' intensities, then the detection probabilities, and, finally, the probabilities of the effective events.

After all the calculations above are done, we can finally obtain the overall gains and QBERs under different effective events. We first consider these parameters for the X_1 event:

$$\begin{aligned}Q_\mu^{X_1} &= \Pr(D_{H_1}) + \Pr(D_{H_2}) = \tfrac{1}{4}\big[\Pr(D_{H_1}|++) + \Pr(D_{H_1}|+-) + \Pr(D_{H_1}|-+) + \Pr(D_{H_1}|--)\\ &\quad + \Pr(D_{H_2}|++) + \Pr(D_{H_2}|+-) + \Pr(D_{H_2}|-+) + \Pr(D_{H_2}|--)\big]\\ &= \tfrac{1}{2}\big[\Pr(D_{H_1}|++) + \Pr(D_{H_1}|+-) + \Pr(D_{H_2}|++) + \Pr(D_{H_2}|+-)\big]. \quad \text{(C5)}\end{aligned}$$

As listed in Table II, under the two polarization combinations discussed here, a bit error occurs in the phase bit when the D_{H_2} click event happens. Thus, the QBER can be calculated as

$$E_\mu^{\mathrm{bit},X_1} = \frac{1}{2Q_\mu^{X_1}}\big[\Pr(D_{H_2}|++) + \Pr(D_{H_2}|+-)\big]. \quad \text{(C6)}$$

Using the same method, we can get the overall gains and QBERs of the X_2 and X_3 events,

$$\begin{aligned}Q_\mu^{X_2} &= \Pr(D_{H_1}D_{V_1}|++) + \Pr(D_{H_1}D_{V_1}|+-) + \Pr(D_{H_2}D_{V_2}|++) + \Pr(D_{H_2}D_{V_2}|+-),\\ E_\mu^{\mathrm{bit},X_2} &= \frac{1}{2Q_\mu^{X_2}}\big[\Pr(D_{H_1}D_{V_1}|+-) + \Pr(D_{H_2}D_{V_2}|++) + 2\Pr(D_{H_2}D_{V_2}|+-)\big],\\ Q_\mu^{X_3} &= \Pr(D_{H_1}D_{V_2}|++) + \Pr(D_{H_1}D_{V_2}|+-) + \Pr(D_{V_1}D_{H_2}|++) + \Pr(D_{V_1}D_{H_2}|+-),\\ E_\mu^{\mathrm{bit},X_3} &= \frac{1}{2Q_\mu^{X_3}}\big[\Pr(D_{H_1}D_{V_2}|++) + 2\Pr(D_{V_1}D_{H_2}|++) + \Pr(D_{V_1}D_{H_2}|+-)\big]. \quad \text{(C7)}\end{aligned}$$

[1] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[2] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

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

[4] K. Inoue, E. Waks, and Y. Yamamoto, Differential phase shift quantum key distribution, Phys. Rev. Lett. **89**, 037902 (2002).

[5] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[7] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference, PRX Quantum **3**, 020315 (2022).

[8] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).

[9] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, and J.-W. Pan, Experimental mode-pairing measurement-device-independent quantum key distribution without global phase locking, Phys. Rev. Lett. **130**, 030801 (2023).

[10] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[11] S. L. Braunstein and S. Pirandola, Side-channel-free quantum key distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[12] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[13] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).
[14] P. Zeng, W. Wu, and X. Ma, Symmetry-protected privacy: Beating the rate-distance linear bound over a noisy channel, Phys. Rev. Appl. **13**, 064013 (2020).
[15] Y. Yu, L. Wang, S. Zhao, and Q. Mao, Decoy-state phase-matching quantum key distribution with source errors, Opt. Express **29**, 2227 (2021).
[16] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).
[17] F.-Y. Lu, Z.-Q. Yin, R. Wang, G.-J. Fan-Yuan, S. Wang, D.-Y. He, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Practical issues of twin-field quantum key distribution, New J. Phys. **21**, 123030 (2019).
[18] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[19] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution: Breaking the direct transmission key rate, Phys. Rev. A **101**, 042330 (2020).
[20] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, Measurement-device-independent quantum key distribution over a 404 km optical fiber, Phys. Rev. Lett. **117**, 190501 (2016).
[21] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, Phys. Rev. X **9**, 021046 (2019).
[22] X.-T. Fang *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).
[23] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).
[24] S. Wang *et al.*, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).
[25] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Security of quantum key distribution using d-level systems, Phys. Rev. Lett. **88**, 127902 (2002).
[26] F. Bouchard, R. Fickler, R. W. Boyd, and E. Karimi, High-dimensional quantum cloning and applications to quantum hacking, Sci. Adv. **3**, e1601915 (2017).
[27] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, High-dimensional quantum cryptography with twisted light, New J. Phys. **17**, 033033 (2015).
[28] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, C. Marquardt, G. Leuchs, R. W. Boyd, and E. Karimi, High-dimensional intracity quantum cryptography with structured photons, Optica **4**, 1006 (2017).
[29] F.-X. Wang, W. Chen, Z.-Q. Yin, S. Wang, G.-C. Guo, and Z.-F. Han, Characterizing high-quality high-dimensional quantum key distribution by state mapping between different degrees of freedom, Phys. Rev. Appl. **11**, 024070 (2019).
[30] Z.-X. Cui, W. Zhong, L. Zhou, and Y.-B. Sheng, Measurement-device-independent quantum key distribution with hyper-encoding, Sci. China: Phys., Mech. Astron. **62**, 110311 (2019).
[31] I. Nape, E. Otte, A. Vallés, C. Rosales-Guzmán, F. Cardano, C. Denz, and A. Forbes, Self-healing high-dimensional quantum key distribution using hybrid spin-orbit bessel states, Opt. Express **26**, 26946 (2018).
[32] D.-D. Li, M.-S. Zhao, Z. Li, Y.-L. Tang, Y.-Q. Dai, S.-B. Tang, and Y. Zhao, High dimensional quantum key distribution with temporal and polarization hybrid encoding, Opt. Fiber Technol. **68**, 102828 (2022).
[33] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).
[34] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).
[35] J. Teng, Z.-Q. Yin, G.-J. Fan-Yuan, F.-Y. Lu, R. Wang, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Sending-or-not-sending twin-field quantum key distribution with multiphoton states, Phys. Rev. A **104**, 062441 (2021).
[36] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).
[37] S. Zhang, Y. Feng, X. Sun, and M. Ying, Upper bound for the success probability of unambiguous discrimination among quantum states, Phys. Rev. A **64**, 062103 (2001).