


Twin-Field Quantum Key Distribution without Phase Postselection

Chaohan Cui,^{1,2} Zhen-Qiang Yin,^{1,2,*} Rong Wang,^{1,2} Wei Chen,^{1,2} Shuang Wang,^{1,2,†}
Guang-Can Guo,^{1,2} and Zheng-Fu Han^{1,2}

¹*CAS Key Laboratory of Quantum Information, CAS Center For Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China*

²*State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China*

 (Received 4 July 2018; revised manuscript received 27 February 2019; published 21 March 2019)

The twin-field quantum key distribution (TFQKD) protocol and its variants, e.g., phase-matching (PM) QKD and TFQKD based on sending or not sending, are highly attractive since they are able to overcome the well-known rate-loss limit for QKD protocols without a repeater: $R = O(\eta)$, with η standing for the channel transmittance. However, all these protocols require active phase randomization and postselection that play an essential role together in their security proof. Counterintuitively, we find that in TFQKD, beating the rate-loss limit is still possible even if phase randomization and postselection in the coding mode are both removed, which means our final secure key rate $R = O(\sqrt{\eta})$. Furthermore, our protocol is more feasible in practice and more promising according to its higher final key rate in the valid distance. Our security proof counters a collective attack and can also counter a coherent attack in the asymptotical case.

DOI: [10.1103/PhysRevApplied.11.034053](https://doi.org/10.1103/PhysRevApplied.11.034053)

I. INTRODUCTION

With the help of quantum key distribution (QKD), two distant agents (Alice and Bob) are able to share secret key bits in the sense of information-theoretical security [1–7]. Albeit impressive progress in QKD experiments [8–14] has been made, there is a fundamental limit on the secret key rate R versus channel transmittance η . This limit has been sufficiently discussed by researchers [15,16] and was finally revealed as the linear key rate bound $R \leq -\log_2(1 - \eta)$ [16]. For a long distance, the transmittance is much smaller; then, $R = O(\eta)$. Surprisingly, this limit was overcome by the twin-field (TF) QKD protocol proposed in 2018 [17]. One may note that the security proof of TFQKD has been rebuilt in Ref. [18], although its original security analysis in Ref. [17] is not strict. The physics behind TFQKD is that Alice and Bob prepare photon-number superposition remotely via coherent states and postselection.

Inspired by TFQKD, phase-matching (PM) QKD protocol is introduced in Ref. [19]. In the PMQKD protocol, Alice (Bob) prepares weak coherent states $|\pm\sqrt{\mu}\rangle$ randomly and adds a random phase ϕ_A (ϕ_B) to each of her (his) weak coherent states, and then sends them to an untrusted party Charlie located in the middle of the channel. Depending on the measurement results declared by Charlie, Alice

and Bob are able to generate raw key bits after postselection of the cases satisfying $\phi_A \approx \phi_B$. Another variant of TFQKD is based on sending or not sending a weak coherent pulse, which can be very robust under a large optical misalignment error [20], but the final key rate is not satisfactory. In its decoy mode, phase randomization and postselection are still necessary. Consequently, in TFQKD and its variants, active phase randomization and postselection seem indispensable to the security of sifted key bits.

However, the phase postselection may impair its secret key rate in practice. It is still an open question if the active phase randomization and phase postselection can be removed. Here, we firstly introduce a simplified TFQKD protocol, in which its key bit is encoded in phase 0 or π , but unlike PMQKD, the coding mode does not employ active phase randomization and, thus, phase postselection is also circumvented. Therefore, its coding mode is simple and the security proof is totally different from previous protocols. In Sec. III, the security proof of the proposed protocol is given by estimating the upper bound for latent information leakage. In Secs. IV and V, the numerical simulations with practical imperfections show that the performance of the proposed protocol without active phase randomization is satisfactory and even better; i.e., it can beat the linear key rate bound at an even shorter distance than other protocols. So far, we only consider threats of collective attack or coherent attack with an infinite key length. The conclusion is given in Sec. VI.

*yinqz@ustc.edu.cn

†wshuang@ustc.edu.cn

II. SIMPLIFIED TFQKD

Our simplified TFQKD protocol removes the postselection part of original TFQKD. Firstly, let us introduce the flow of this simplified protocol as follows.

Step 1. Alice and Bob randomly choose code mode or decoy mode [21–23] in each trial.

Step 2. a. If code mode is selected, Alice (Bob) prepares a weak coherent state $|\pm\sqrt{\mu}\rangle_{A\text{-out}}$ ($\pm|\sqrt{\mu}\rangle_{B\text{-out}}$) according to her (his) random classical key bit 0 or 1 and sends the prepared state to the untrusted measurement device controlled by Eve.

Step 2. b. If decoy mode is selected, Alice (Bob) emits a phase-randomized weak coherent state with mean photon number ν_a (ν_b), where ν_a (ν_b) is randomly chosen from a predecided set. Note that the phase of a weak coherent state in decoy mode will never be publicly announced. Thus, in decoy mode, Alice (Bob) actually prepares a mixed state in Fock space.

Step 3. For each trial, the middle receiver Eve must publicly announce a successful message $|1\rangle_M$ or a failure message $|0\rangle_M$ to Alice and Bob. If she announces $|1\rangle_M$, she has to simultaneously declare which message she obtained, $|L\rangle_M$ or $|R\rangle_M$. For an honest Eve, $|L\rangle_M$ and $|R\rangle_M$ reveal which detector clicks [19]. For simplicity, we treat the double-click event as message $|L\rangle_M$ or $|R\rangle_M$ at random. Note that $|1\rangle_M$, $|0\rangle_M$, $|L\rangle_M$, and $|R\rangle_M$ are all classical messages announced by Eve, though we use bra-ket notation to describe them.

Step 4. After repeating steps 1 to 3 for sufficient times, Alice and Bob publicly announce which trials are code modes and which trials are decoy modes. For the trials in which Alice and Bob both select the code mode and Eve announces $|L\rangle_M$ or $|R\rangle_M$, the raw key bits are generated. Here, Bob should flip his bit if Eve announces $|R\rangle_M$. For the trials in which Alice and Bob both select decoy mode, Alice and Bob can estimate the yield $Y_{n,m}$, which means the probability of Eve announcing $|1\rangle_M$ provided Alice emits an n -photon state and Bob emits an m -photon state in a decoy mode. With these parameters, information leakage is bounded so that secret key bits can be generated from raw key bits by error correction and privacy amplification.

In the following paper, we focus on the upper bound for the information leakage through the whole protocol.

III. MAIN RESULTS OF SECURITY PROOF

For readability, we sketch the security proof and its main results here. One may refer to Appendix A for detailed derivations. We make no more assumptions to Eve than assumptions applied in measurement-device-independent (MDI) QKD [6,7]. Accordingly, Eve’s general collective attack to the above simplified TFQKD protocol can be

defined as an arbitrary measurement after an arbitrary unitary operation operating on the whole system with her prepared ancilla [4,5]. Under photon-number representation, this collective attack is given by

$$\hat{U}|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}|E_0\rangle_{Ea}|0\rangle_M = \sqrt{Y_{n,m}}|\gamma_{n,m}\rangle_E|1\rangle_M + \sqrt{1 - Y_{n,m}}|\text{other}\rangle_E|0\rangle_M, \quad (1)$$

where $|n\rangle_{A\text{-out}}$ and $|m\rangle_{B\text{-out}}$ represent the photon-number bases of the quantum states prepared by Alice and Bob respectively, the state $|E_0\rangle_{Ea}$ is the ancilla of Eve, and $Y_{n,m} \in [0, 1]$ is a probabilitylike value showing the portion in which Alice and Bob receive the message $|1\rangle_M$ from Eve. On the right side of Eq. (1), $|\gamma_{n,m}\rangle_E$ and $|\text{other}\rangle_E$ are the quantum states of the compound system including Eve’s ancilla Ea , $A\text{-out}$ and $B\text{-out}$, which are all in the hands of Eve now. Note that any phases of the states on the right-hand side of Eq. (1) are absorbed into the definition of those states. For simplicity, let us denote Eve’s message $|L\rangle_M$ and $|R\rangle_M$ as the same one $|1\rangle_M$, since we are only concerned with Alice’s key bit here, but not Bob’s bit and his flipping operation. We aim to bound Eve’s information I_{AE} on Alice’s key bit when Eve announces message $|1\rangle_M$. Through derivations given in Appendix A, it is proved that this upper bound I_{AE}^u can be solved by the following optimization problem given by

$$I_{AE}^u = \max h\left(\frac{x_{00}}{Q_\mu}, \frac{x_{10}}{Q_\mu}\right) + h\left(\frac{x_{11}}{Q_\mu}, \frac{x_{01}}{Q_\mu}\right),$$

$$\text{s.t.} \begin{cases} 0 \leq x_{00} \leq \left| \sum_{n,m=0} \sqrt{P_{2n}P_{2m}Y_{2n,2m}} \right|^2, \\ 0 \leq x_{10} \leq \left| \sum_{n,m=0} \sqrt{P_{2n+1}P_{2m}Y_{2n+1,2m}} \right|^2, \\ 0 \leq x_{11} \leq \left| \sum_{n,m=0} \sqrt{P_{2n+1}P_{2m+1}Y_{2n+1,2m+1}} \right|^2, \\ 0 \leq x_{01} \leq \left| \sum_{n,m=0} \sqrt{P_{2n}P_{2m+1}Y_{2n,2m+1}} \right|^2, \\ x_{00} + x_{10} + x_{11} + x_{01} = Q_\mu, \end{cases} \quad (2)$$

with the definition $h(x, y) = -x \log_2 x - y \log_2 y + (x + y) \log_2(x + y)$. Here, $P_k = e^{-\mu} \mu^k / k!$ is the probability of coherent state $\pm|\sqrt{\mu}\rangle$ containing k -photons and Q_μ is the probability of Alice obtaining a raw key bit in code mode, which is directly observed experimentally. In practice, agents can observe the parameters P_n , P_m , Q_μ , and $Y_{n,m}$. Then, the information leakage bound can be estimated by the above optimization problem. According to Devetak-Winter’s bound [24], the secret key rate per trial in a code mode is then given by

$$R = Q_\mu [1 - fh(e_\mu, 1 - e_\mu) - I_{AE}^u], \quad (3)$$

in which e_μ is the error rate of raw key bits. This security proof assumes that Eve only launches a collective attack; however, this restriction can be removed by following the

results in Refs. [25] and [26]. Hence, our proof can guarantee security against the coherent attacks asymptotically. It also ends our security proof rigorously.

Before proceeding, let us roughly estimate the performance of the protocol under the ideal case, in which only channel transmission efficiency η is considered, while all other imperfections, e.g., dark counts of single-photon detectors, are absent. Then, it is expected that $x_{00} \sim x_{11} \sim \mu^2 O(\sqrt{\eta})$, since the main contribution of x_{00} and x_{11} comes from the yield of the total photon number from Alice and Bob is 2. With a similar argument, we have $x_{01} \sim x_{10} \sim \mu O(\sqrt{\eta})$. Thus, from Eq. (2), we can see $I_{AE}^u \ll 1$ for any η provided a proper value of μ is assumed. Also, it is obvious that $Q_\mu \sim \mu O(\sqrt{\eta})$ and $e_\mu = 0$ in the ideal case. Accordingly, from the above formulas, we have $R = O(\sqrt{\eta})$. This result does reconfirm the expectation that the TFQKD can overcome the linear bound even if phase randomization and postselection are both removed. In the next two sections, through numerical simulations with practical imperfections, we show the performance of our protocol with both infinite and finite decoy state techniques compared with other states of the art.

IV. ESTIMATION AND SIMULATION WITH INFINITE DECOY STATES

In a practical system, Alice and Bob can emit phase-randomized decoy states [21] to estimate $Y_{n,m}$. The gain of the decoy states in which Alice emits a pulse with a mean photon-number ν_a and Bob emits a pulse with a mean photon-number ν_b satisfies

$$Q_d^{\nu_a, \nu_b} = \sum_{n,m} P_n^{\nu_a} P_m^{\nu_b} Y_{n,m}, \quad (4)$$

where $P_k^\nu = e^{-\nu} \nu^k / k!$ is known by both agents. Considering the ideal case with infinite decoy states ν_a and ν_b , we can list infinite linear equations like Eq. (4) to calculate $Y_{n,m}$ accurately. Therefore, the secure key rate can be easily calculated using Eq. (3) with I_{AE}^u given by Eq. (2). Here, we simulate the maximum secure key rates related to different losses for multiple protocols with infinite decoy states implemented and practical parameters of experiments. Details can be found in Appendix B. The results are shown in Fig. 1. We can see that, with infinite decoy states, our protocol has a higher key rate than original PMQKD because our protocol is phase postselection free and independent with extra error estimations. Note that the slope of the key rate in our protocol is the same as the linear bound with a single repeater [27] when the fiber loss is less than 60 dB, which shows that the advantage of beating a well-known linear bound is also reconfirmed through 30- to 60-dB fiber loss. In other words, $R = O(\sqrt{\eta})$. It is also remarkable that our protocol can outperform BB84, with a lower channel loss compared to the original PMQKD.

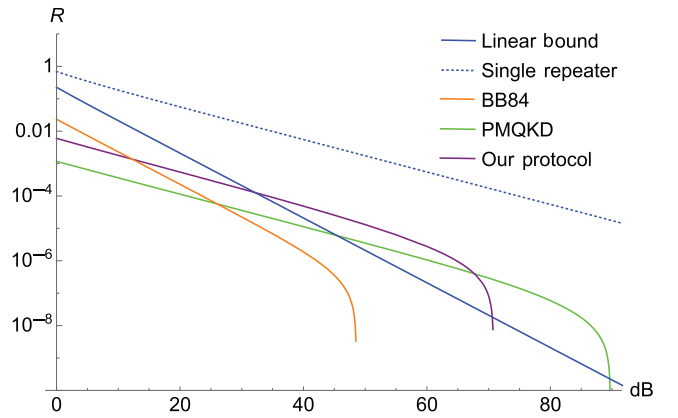


FIG. 1. Key rates (R) of our protocol (purple curve), PMQKD (green) [19], and BB84 (orange) with all infinite decoy states versus different optical fiber losses (dB). Note that we assume zero optical misalignment, except the misalignment due to phase postselection ($M = 16$) of original PMQKD in Ref. [19]. The linear key rate bound (blue) [16] and the bound with a single repeater (dotted blue) [27] are also shown in the figure.

V. ESTIMATION AND SIMULATION WITH FINITE DECOY STATES

Finite decoy states can also help to estimate the lower bound for yields [22,23,28]. In a practical system, this implement is much more feasible than the infinite one. Here, we apply decoy states with four different intensities: μ , ν_1 , ν_2 , and 0. After the announcement of decoy modes and each applied intensity, we have the following gains: $Q_d^{0,0}$, $Q_d^{\mu,0}$, $Q_d^{\nu_1,0}$, $Q_d^{\nu_2,0}$, $Q_d^{0,\mu}$, Q_d^{0,ν_1} , Q_d^{0,ν_2} , $Q_d^{\mu,\mu}$, $Q_d^{\nu_1,\nu_1}$, and $Q_d^{\nu_2,\nu_2}$.

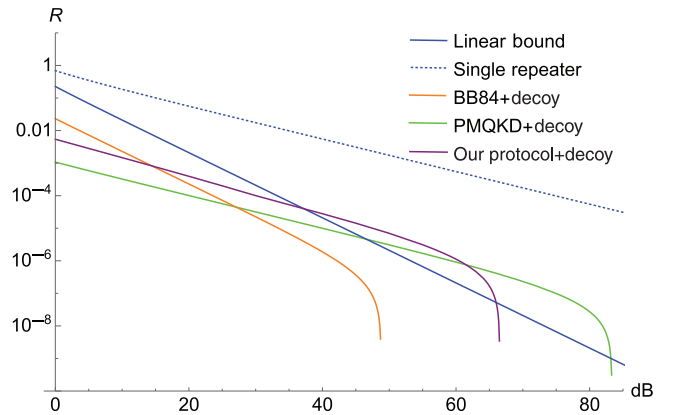


FIG. 2. Key rates (R) of our protocol (purple curve), PMQKD (green) [19], and BB84 (orange) with all finite decoy states versus different optical fiber losses (dB). Note that we assume zero optical misalignment, except the misalignment due to phase postselection ($M = 16$) of original PMQKD in Ref. [19]. The linear key rate bound (blue) [16] and the bound with a single repeater (dotted blue) [27] are also shown in the figure.

Then, we show how those statistics can give good approximations to $Y_{0,0}$, $Y_{0,1}$, $Y_{1,0}$, $Y_{2,0}$, $Y_{0,2}$, and Y_2 , where Y_2 means the yields that are from decoy trials in which Alice and Bob share two photons in total. From $Q_d^{\mu,0}$, $Q_d^{\nu_1,0}$, $Q_d^{\nu_2,0}$, and $Q_d^{0,0}$, we can obtain lower bounds and upper bounds of $Y_{0,0}$, $Y_{0,1}$, and $Y_{0,2}$ by linear programming using Eq. (4). Similarly, lower bounds and upper bounds of $Y_{1,0}$ and $Y_{2,0}$ can be estimated from $Q_d^{0,\mu}$, Q_d^{0,ν_1} , Q_d^{0,ν_2} , and $Q_d^{0,0}$. Upper bounds and lower bounds of Y_2 could also be bounded by the linear programming on four linear equations of $Q_d^{\mu,\mu}$, $Q_d^{\nu_1,\nu_1}$, $Q_d^{\nu_2,\nu_2}$, and $Q_d^{0,0}$. In the following text, we use the superscript u or l to label the upper or lower bound for Y obtained here. To estimate $Y_{1,1}$, through the relation $Y_2 = \sum_i P_i^\mu P_{2-i}^\mu Y_{i,2-1} / \sum_i P_i^\mu P_{2-i}^\mu$, $Y_{1,1}$ could be

bounded by

$$\begin{aligned} & \frac{(2P_0^\mu P_2^\mu + P_1^\mu P_1^\mu)Y_2^l - P_0^\mu P_2^\mu (Y_{0,2}^u + Y_{2,0}^u)}{P_1^\mu P_1^\mu} = Y_{1,1}^l \\ & \leq Y_{1,1} \leq Y_{1,1}^u = \frac{(2P_0^\mu P_2^\mu + P_1^\mu P_1^\mu)Y_2^u - P_0^\mu P_2^\mu (Y_{0,2}^l + Y_{2,0}^l)}{P_1^\mu P_1^\mu}. \end{aligned} \quad (5)$$

Then, the remaining task is constraining x_{00} , x_{01} , x_{10} , and x_{11} with these lower bounds and upper bounds generated from decoy statistics.

Let us take x_{00} as an example. From Eq. (2), we have a general bound that limits the x_{00} as

$$\begin{aligned} x_{00} \leq & \left| \sum_{n,m=0} \sqrt{P_{2n}^\mu P_{2m}^\mu Y_{2n,2m}} \right|^2 \leq \max_{k \geq 2} \left| \sqrt{P_0^\mu P_0^\mu Y_{0,0}^u} + \sqrt{P_0^\mu P_2^\mu Y_{0,2}^u} + \sqrt{P_2^\mu P_0^\mu Y_{2,0}^u} \right. \\ & \left. + \sqrt{\frac{(k+4)(k-1)}{2} (Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i}^\mu P_{2(n-i)}^\mu - \sum_{n=0}^2 \sum_{i=0}^n P_i^\mu P_{n-i}^\mu Y_{i,n-i}^l) + \sum_{n=k+1}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^\mu P_{2(n-i)}^\mu}} \right|^2. \end{aligned} \quad (6)$$

The details of the derivation are included in the Appendix B. Now, we obtain the bounds of these four values based on all the observables in our protocol. The final step is only making an optimization to find the best information-theoretical secure key rate with Eq. (3) limited by these bounds.

So far, we show how Alice and Bob can estimate the lower bound for the key rates under different losses with four decoy states. We simulate a practical case for multiple protocols. The results are shown in Fig. 2. Even in the case of finite decoy states, our protocol's key rate holds the relation with transmittance as $R = O(\sqrt{\eta})$. Consequently, it can still beat the linear bound in the loss range from 40 to 60 dB.

VI. CONCLUSION

Inspired by TFQKD protocol and its variants such as PMQKD, we propose a simplified protocol with a higher final key rate, in which the raw key bits are generated without active phase randomization and phase postselection. A meticulous security proof is presented by estimating the information leakage in our protocol. Counterintuitively, our bound for latent information leakage does not rely on the error rate. Meanwhile, its advantage of beating the linear rate-loss limit is still available here, showing the final key rate $R = O(\sqrt{\eta})$ over transmittance η . Also, thanks to the removal of phase postselection, our scheme can perform over the well-known BB84 at a shorter channel

distance compared to the original PMQKD protocol, which means that the proposed protocol could be very competitive when the channel loss is around 15 to 60 dB.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2016YFA0302600); the National Natural Science Foundation of China (Grants No. 61822115, No. 61775207, No. 61622506, No. 61627820, No. 61575183); and the Anhui Initiative in Quantum Information Technologies.

Note added.—Recently, two other groups provided similar ideas [29,30] independently but did not include the practical case with finite decoy states. In our methodology, our work is based on the analysis of collective attack while the authors of Ref. [29] present a proof based on an equivalent entanglement distillation protocol. Also, both Refs. [29] and [30] use infinite decoy states, which is not feasible in the experiments.

APPENDIX A: SECURITY PROOF

We make no more assumptions for Eve than the assumptions applied in MDIQKD [6,7]. In order to bound the information leakage to Eve, we have to describe the ultimate power of Eve under the assumptions. Also, Eve's strategy must obey the time line through this protocol. Therefore, Eve's general collective attack to the above

simplified TFQKD protocol can be defined as an arbitrary measurement after an arbitrary unitary operation operating on the whole system with her prepared ancilla [4,5]. Furthermore, the message Eve announces should also be obtained from the measurement results. Under photon-number representation, this collective attack is given by

$$\begin{aligned} & \hat{U}|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}|E_0\rangle_{Ea}|0\rangle_M \\ & = \sqrt{Y_{n,m}}|\gamma_{n,m}\rangle_E|1\rangle_M + \sqrt{1-Y_{n,m}}|\text{other}\rangle_E|0\rangle_M, \end{aligned} \quad (\text{A1})$$

where $|n\rangle_{A\text{-out}}$ and $|m\rangle_{B\text{-out}}$ represent the photon-number bases of the quantum states prepared by Alice and Bob respectively, the state $|E_0\rangle_{Ea}$ is the ancilla of Eve, and $Y_{n,m} \in [0, 1]$ is a probabilitylike value showing the portion in which Alice and Bob receive the message $|1\rangle_M$ from Eve. On the right side of Eq. (A1), $|\gamma_{n,m}\rangle_E$ and $|\text{other}\rangle_E$ are the quantum states of the compound system including Eve's ancilla Ea , $A\text{-out}$ and $B\text{-out}$, which are all in the hands of Eve. Note that any phases of the states on the right-hand side of Eq. (A1) are absorbed into the definition of those states. For simplicity, let us denote Eve's message $|L\rangle_M$ and $|R\rangle_M$ as the same one $|1\rangle_M$, since we are only concerned with Alice's key bit here, but not Bob's bit or his flipping operation. Note that this expression does give the most general collective attack, including possible attacks trying to distinguish between decoy mode and code mode and treat them differently, since Eve's ancilla is arbitrary. Indeed, any measurement and following transformation depending on the output of the measurement can be described as a "giant" unitary operator applied to a larger Hilbert space.

Suppose Alice and Bob each has an ancillary qubit to store their classical key bit in code mode. For simplicity, here we assume that Alice's and Bob's random binary bits come from measurements of their qubits in Z bases. So they set their initial qubits to $|+\rangle$ and prepare a weak coherent state light pulse with average photon number μ . Then, the initial prepared state is

$$|+\rangle_A|+\rangle_B|\sqrt{\mu}\rangle_{A\text{-out}}|\sqrt{\mu}\rangle_{B\text{-out}}. \quad (\text{A2})$$

Then, Alice and Bob apply a Controlled- π gate to upload their information on the output coherent state and measure their private qubits. Recall Eve's attack given by Eq. (A1). For the ease of representation, we define four intermediate unnormalized states labeled by the photon number's parity of $A\text{-out}$ and $B\text{-out}$,

$$\begin{aligned} |\psi_{ee}\rangle & = \sum_{n,m} \sqrt{P_{2n}P_{2m}Y_{2n,2m}}|\gamma_{2n,2m}\rangle, \\ |\psi_{oo}\rangle & = \sum_{n,m} \sqrt{P_{2n+1}P_{2m+1}Y_{2n+1,2m+1}}|\gamma_{2n+1,2m+1}\rangle, \end{aligned}$$

$$\begin{aligned} |\psi_{eo}\rangle & = \sum_{n,m} \sqrt{P_{2n}P_{2m+1}Y_{2n,2m+1}}|\gamma_{2n,2m+1}\rangle, \\ |\psi_{oe}\rangle & = \sum_{n,m} \sqrt{P_{2n+1}P_{2m}Y_{2n+1,2m}}|\gamma_{2n+1,2m}\rangle, \end{aligned} \quad (\text{A3})$$

where the subscript E is dropped for simplicity. Since Alice's and Bob's encoding phases are 0 or π , the phase of Fock state $|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}$ does not change if both n and m are odd or even, while $|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}$ changes to $-|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}$ if only one of n or m is odd. Thus, in code mode, under the same combination of coding phases, the phase of superposition of $|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}$ can be divided into four groups depending on the parity of n and m . This result implies that we can define Eq. (A3), which is just the superposition of $|n\rangle_{A\text{-out}}|m\rangle_{B\text{-out}}$ with different parities. Those states $|\psi_{ee}\rangle$, $|\psi_{oo}\rangle$, $|\psi_{eo}\rangle$, and $|\psi_{oe}\rangle$ are quite useful for simplifying the following derivations.

It should be taken into account that Eq. (A1) never implies whether $|\gamma_{n,m}\rangle$ are orthogonal to each other or not. It is obvious that Alice and Bob cannot obtain any direct knowledge of them because they are measured by Eve. After tracing Bob's qubit out and measuring Alice's qubit in the Z basis, the unnormalized density matrix of Eve's system E and Alice's ancillary qubit A conditioned such that $|1\rangle_M$ is announced becomes

$$\begin{aligned} \rho_{AE} & = \frac{1}{2}\Pi\{|0\rangle_A\} \otimes (\Pi\{|\psi_{ee}\rangle + |\psi_{oe}\rangle\} \\ & \quad + \Pi\{|\psi_{oo}\rangle + |\psi_{eo}\rangle\}) + \frac{1}{2}\Pi\{|1\rangle_A\} \\ & \quad \otimes (\Pi\{|\psi_{ee}\rangle - |\psi_{oe}\rangle\} + \Pi\{|\psi_{oo}\rangle - |\psi_{eo}\rangle\}), \end{aligned} \quad (\text{A4})$$

where $\Pi\{|\psi\rangle\} = |\psi\rangle\langle\psi|$. Then, the Holevo bound of ρ_{AE} is upper-bounded by

$$\begin{aligned} \chi(\rho_{AE}) & \leq \frac{h(\|\psi_{ee}\|^2, \|\psi_{oe}\|^2) + h(\|\psi_{oo}\|^2, \|\psi_{eo}\|^2)}{\|\psi_{ee}\|^2 + \|\psi_{oe}\|^2 + \|\psi_{oo}\|^2 + \|\psi_{eo}\|^2} \\ & = h\left(\frac{\|\psi_{ee}\|^2}{Q_\mu}, \frac{\|\psi_{oe}\|^2}{Q_\mu}\right) + h\left(\frac{\|\psi_{oo}\|^2}{Q_\mu}, \frac{\|\psi_{eo}\|^2}{Q_\mu}\right), \end{aligned} \quad (\text{A5})$$

with the definition $h(x, y) = -x \log_2 x - y \log_2 y + (x + y) \log_2(x + y)$, which is different from the definition of binary von Neumann entropy. To get the inequality of Eq. (A5), we first note that Eve's system E is a mixture of $\Pi\{|\psi_{ee}\rangle + |\psi_{oe}\rangle\}$, $\Pi\{|\psi_{ee}\rangle - |\psi_{oe}\rangle\}$, $\Pi\{|\psi_{oo}\rangle + |\psi_{eo}\rangle\}$, and $\Pi\{|\psi_{oo}\rangle - |\psi_{eo}\rangle\}$. Moreover, without compromising the security, one may assume that Eve gets some side-channel information or a partial purification of ρ_E , which just honestly tells Eve that her system is one of $\Pi\{|\psi_{ee}\rangle + |\psi_{oe}\rangle\}$ and $\Pi\{|\psi_{ee}\rangle - |\psi_{oe}\rangle\}$ or one of $\Pi\{|\psi_{oo}\rangle + |\psi_{eo}\rangle\}$ and $\Pi\{|\psi_{oo}\rangle - |\psi_{eo}\rangle\}$. This assumption just helps Eve to guess Alice's key bit and simplifies the calculation of

$\chi(\rho_{AE})$ greatly. The probability of Alice obtaining a raw key bit in code mode can be presented by $Q_\mu = \|\psi_{ee}\rangle|^2 + \|\psi_{oe}\rangle|^2 + \|\psi_{eo}\rangle|^2 + \|\psi_{oo}\rangle|^2$. Now, we have clearly shown that Eve's information on Alice's classical key bit is bounded by Eq. (A5) as $I(A : E) \leq \chi(\rho_{AE})$, even when the active phase randomization is removed. According to Devetak-Winter's bound [24], the secret key rate per trial in code mode is

$$R = Q_\mu \left[1 - fh(e_\mu, 1 - e_\mu) - h\left(\frac{\|\psi_{ee}\rangle|^2}{Q_\mu}, \frac{\|\psi_{oe}\rangle|^2}{Q_\mu}\right) - h\left(\frac{\|\psi_{oo}\rangle|^2}{Q_\mu}, \frac{\|\psi_{eo}\rangle|^2}{Q_\mu}\right) \right], \quad (\text{A6})$$

in which e_μ is the error rate of raw key bits. To calculate $\chi(\rho_{AE})$, these four values $\|\psi_{ee}\rangle|^2$, $\|\psi_{oo}\rangle|^2$, $\|\psi_{oe}\rangle|^2$, and $\|\psi_{eo}\rangle|^2$ must be estimated. Obviously, Alice and Bob can relate these values to the direct observables and statistics, i.e.,

$$\begin{aligned} \|\psi_{ee}\rangle|^2 &\leq \left| \sum_{n,m=0} \sqrt{P_{2n}P_{2m}Y_{2n,2m}} \right|^2, \\ \|\psi_{oe}\rangle|^2 &\leq \left| \sum_{n,m=0} \sqrt{P_{2n+1}P_{2m}Y_{2n+1,2m}} \right|^2, \\ \|\psi_{oo}\rangle|^2 &\leq \left| \sum_{n,m=0} \sqrt{P_{2n+1}P_{2m+1}Y_{2n+1,2m+1}} \right|^2, \\ \|\psi_{eo}\rangle|^2 &\leq \left| \sum_{n,m=0} \sqrt{P_{2n}P_{2m+1}Y_{2n,2m+1}} \right|^2, \\ \|\psi_{ee}\rangle|^2 + \|\psi_{oe}\rangle|^2 + \|\psi_{oo}\rangle|^2 + \|\psi_{eo}\rangle|^2 &= Q_\mu. \end{aligned} \quad (\text{A7})$$

With these constraints, one can estimate the upper bound of $\chi(\rho_{AE})$. By defining $x_{00} \triangleq \|\psi_{ee}\rangle|^2$, $x_{10} \triangleq \|\psi_{oe}\rangle|^2$, $x_{11} \triangleq \|\psi_{oo}\rangle|^2$, and $x_{01} \triangleq \|\psi_{eo}\rangle|^2$, we reach Eq. (2) in the main text.

APPENDIX B: DETAILS OF MATHEMATICS IN SIMULATION

We derive a simulation scheme for our protocol and give out numerical results. Suppose the dark count of each detector is p_d per trial and each partner sends a coherent state carrying an average of μ photons. After the

lossy channel and the interference of Alice's and Bob's pulses, the coherent state flows to the correct detector with zero misalignment of devices and no attack. However, because of the loss and the dark count, the response probability is less than 1 and may come from the wrong detector. For each trial, the correct case is when the correct detector provides a response (no matter whether it comes from a dark count or a real signal) and simultaneously there is no dark count from another detector. The probability $P_c = (1 - p_d)[1 - (1 - p_d) \exp(-2\eta\mu)]$. Also, an error case occurs when the wrong detector clicks for a dark count while the correct detector gets nothing, with a probability $P_e = (1 - p_d) \exp(-2\eta\mu)p_d$. The gain Q_μ of code mode should be

$$Q_\mu = P_c + P_e = (1 - p_d)[1 - (1 - p_d) \exp(-2\eta\mu)] + (1 - p_d) \exp(-2\eta\mu)p_d. \quad (\text{B1})$$

The error rate should be

$$e_\mu = \frac{P_e}{P_c + P_e} = \frac{\exp(-2\eta\mu)p_d}{1 - (1 - 2p_d) \exp(-2\eta\mu)}. \quad (\text{B2})$$

The above formulas are in accord with the results of Ref. [19] with zero misalignment. The misalignment can also be included both in the gain and error rate, but, in our phase-randomization-free protocol, we assume the best performance such that the misalignment is zero.

If we apply infinite decoy states, the approximation of $Y_{n,m}$ can be calculated as

$$Y_{n,m} = 1 - (1 - p_d)^2(1 - \eta)^{n+m}. \quad (\text{B3})$$

Here, without compromising security, we treat the double-click event as message $|L\rangle_M$ or $|R\rangle_M$ at random to simplify the bound of $Y_{n,m}$. With the above equation, Eq. (A7) is bounded by parameters in real experiments.

If we apply finite decoy states, we can only obtain good bounds for several $Y_{n,m}$ with small n and m . For the case considered in the main text, linear programming on statistics and Eq. (5) helps to bound $Y_{0,0}$, $Y_{0,1}$, $Y_{1,0}$, $Y_{2,0}$, $Y_{0,2}$, and $Y_{1,1}$. The upper bound for the right-hand values in Eq. (A7) could be calculated as an optimization problem with constraints. Recall the example in the main text:

$$\begin{aligned} x_{00} &\leq \left| \sum_{n,m=0}^{+\infty} \sqrt{P_{2n}^\mu P_{2m}^\mu Y_{2n,2m}} \right|^2 = \left| \sum_{n=0}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^\mu P_{2(n-i)}^\mu Y_{2i,2(n-i)}} \right|^2 \\ &\leq \left| \sqrt{P_0^\mu P_0^\mu Y_{0,0}} + \sqrt{P_0^\mu P_2^\mu Y_{0,2}} + \sqrt{P_2^\mu P_0^\mu Y_{2,0}} + \sum_{n=2}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^\mu P_{2(n-i)}^\mu Y_{2i,2(n-i)}} \right|^2. \end{aligned} \quad (\text{B4})$$

$\sum_{n=2}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)}}$ is untouchable by statistics from only four decoy states. But the constraints of the total gain give an upper bound for this term. The optimization problem can be described as

$$\begin{aligned} \max \quad & \sum_{n=2}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)}}, \\ \text{s.t.} \quad & \begin{cases} \sum_{n=2}^{+\infty} \sum_{i=0}^n P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)} \leq Q_d^{\mu,\mu} - \sum_{n=0}^2 \sum_{i=0}^n P_i^{\mu} P_{n-i}^{\mu} Y_{i,n-i}^l, \\ 0 \leq Y_{i,j} \leq 1 \quad \forall i, j \in \mathbb{Z}, \end{cases} \end{aligned} \quad (\text{B5})$$

which could be easily solved numerically. On the other side, we can use an analytical approach for the upper bound of the aimed function in Eq. (B5). Since all known probability terms are positive and decrease to zero exponentially, the above optimization problem satisfies the well-known Karush-Kuhn-Tucker [31] conditions. Therefore, the maximum is located at the boundary where any $Y_{q,t-q}$ with $t > k$ reaches its upper bound and others hold the conditions. Then, the problem is simplified to finding an integer $k \geq 2$ that reaches the maximum value of the aimed function in Eq. (B5), say,

$$\sum_{n=2}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)}} \leq \max_{k \geq 2} \sum_{n=2}^k \sqrt{(n+1) \sum_{i=0}^n P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)}} + \sum_{n=k+1}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu}}. \quad (\text{B6})$$

Here, on the right-hand side, $k \geq 2$ is an integer waiting for optimization. This inequality is based on the inequality between the arithmetic mean and quadratic mean. Then, the optimization problem Eq. (B5) becomes

$$\begin{aligned} \max_{k \geq 2} \quad & \sum_{n=2}^k \sqrt{(n+1)\alpha_n} + \sum_{n=k+1}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu}}, \\ \text{s.t.} \quad & \begin{cases} \sum_{n=2}^k \alpha_n \leq Q_d^{\mu,\mu} - \sum_{n=0}^2 \sum_{i=0}^n P_i^{\mu} P_{n-i}^{\mu} Y_{i,n-i}^l, \\ 0 \leq \alpha_n \leq \sum_{i=0}^n P_{2i}^{\mu} P_{2(n-i)}^{\mu}, \quad \forall 2 \leq n \leq k, \end{cases} \end{aligned} \quad (\text{B7})$$

$$\begin{aligned} \sum_{n=2}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu} Y_{2i,2(n-i)}} & \leq \max_{k \geq 2} \sum_{n=2}^k \sqrt{(n+1)\alpha_n} + \sum_{n=k+1}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu}} \\ & \leq \max_{k \geq 2} \sqrt{\frac{(k+4)(k-1)}{2} \left(Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i}^{\mu} P_{2(n-i)}^{\mu} - \sum_{n=0}^2 \sum_{i=0}^n P_i^{\mu} P_{n-i}^{\mu} Y_{i,n-i}^l \right)} + \sum_{n=k+1}^{\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu}}, \end{aligned} \quad (\text{B8})$$

where the Cauchy-Schwarz inequality is also used. So the optimization problem Eq. (B5) becomes finding k that can maximize the right-hand side of Eq. (B8). So far, we get the last line of Eq. (B9) in the main text:

$$\begin{aligned} x_{00} & \leq \max_{k \geq 2} \left| \sqrt{P_0^{\mu} P_0^{\mu} Y_{0,0}^u} + \sqrt{P_0^{\mu} P_2^{\mu} Y_{0,2}^u} + \sqrt{P_2^{\mu} P_0^{\mu} Y_{2,0}^u} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^{\mu} P_{2(n-i)}^{\mu}} \right. \\ & \quad \left. + \sqrt{\frac{(k+4)(k-1)}{2} \left(Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i}^{\mu} P_{2(n-i)}^{\mu} - \sum_{n=0}^2 \sum_{i=0}^n P_i^{\mu} P_{n-i}^{\mu} Y_{i,n-i}^l \right)} \right|^2. \end{aligned} \quad (\text{B9})$$

This method is also effective for estimating upper bounds of x_{10} , x_{01} , and x_{11} . We just post the results below:

$$x_{10} \leq \max_{k \geq 1} \left| \sqrt{P_1^\mu P_0^\mu Y_{1,0}^u} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i+1}^\mu P_{2(n-i)}^\mu} \right. \\ \left. + \sqrt{\frac{(k+3)k}{2} \left(Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i+1}^\mu P_{2(n-i)}^\mu - \sum_{n=0}^2 \sum_{i=0}^n P_i^\mu P_{n-i}^\mu Y_{i,n-i}^l \right)} \right|^2, \quad (\text{B10})$$

$$x_{01} \leq \max_{k \geq 1} \left| \sqrt{P_0^\mu P_1^\mu Y_{0,1}^u} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i}^\mu P_{2(n-i)+1}^\mu} \right. \\ \left. + \sqrt{\frac{(k+3)k}{2} \left(Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i}^\mu P_{2(n-i)+1}^\mu - \sum_{n=0}^2 \sum_{i=0}^n P_i^\mu P_{n-i}^\mu Y_{i,n-i}^l \right)} \right|^2, \quad (\text{B11})$$

$$x_{11} \leq \max_{k \geq 1} \left| \sqrt{P_1^\mu P_1^\mu Y_{1,1}^u} + \sum_{n=k+1}^{+\infty} \sum_{i=0}^n \sqrt{P_{2i+1}^\mu P_{2(n-i)+1}^\mu} \right. \\ \left. + \sqrt{\frac{(k+3)k}{2} \left(Q_d^{\mu,\mu} - \sum_{n=k+1}^{+\infty} \sum_{i=0}^n P_{2i+1}^\mu P_{2(n-i)+1}^\mu - \sum_{n=0}^2 \sum_{i=0}^n P_i^\mu P_{n-i}^\mu Y_{i,n-i}^l \right)} \right|^2. \quad (\text{B12})$$

-
- [1] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), p. 175.
 - [2] Peter W. Shor, and John Preskill, Simple Proof of Security of the bb84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
 - [3] Daniel Gottesman, Hoi-Kwong Lo, Norbert Lütkenhaus, and John Preskill, Security of quantum key distribution with imperfect devices, *Quantum Inf. Comput.* **4**, 325 (2004).
 - [4] Renato Renner, Security of quantum key distribution, *Int. J. Quantum Inf.* **6**, 1 (2008).
 - [5] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [6] Samuel L. Braunstein, and Stefano Pirandola, Side-channel-free Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130502 (2012).
 - [7] Hoi-Kwong Lo, Marcos Curty, and Bing Qi, Measurement-device-independent Quantum Key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
 - [8] Damien Stucki, Nino Walenta, Fabien Vannel, Robert Thomas Thew, Nicolas Gisin, Hugo Zbinden, S. Gray, C. R. Towery, and S. Ten, High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres, *New. J. Phys.* **11**, 075003 (2009).
 - [9] Shuang Wang, Wei Chen, Jun-Fu Guo, Zhen-Qiang Yin, Hong-Wei Li, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han, 2 GHz Clock quantum key distribution over 260 km of standard telecom fiber, *Opt. Lett.* **37**, 1008 (2012).
 - [10] Hiroyuki Shibata, Toshimori Honjo, and Kaoru Shimizu, Quantum key distribution over a 72 db channel loss using ultralow dark count superconducting single-photon detectors, *Opt. Lett.* **39**, 5078 (2014).
 - [11] Stefano Pirandola, Carlo Ottaviani, Gaetana Spedalieri, Christian Weedbrook, Samuel L. Braunstein, Seth Lloyd, Tobias Gehring, Christian S. Jacobsen, and Ulrik L. Andersen, High-rate measurement-device-independent quantum cryptography, *Nat. Photon.* **9**, 397 (2015).
 - [12] Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden, Provably secure and practical quantum key distribution over 307 km of optical fibre, *Nat. Photon.* **9**, 163 (2015).
 - [13] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, and Wei-Jun Zhang *et al.*, Measurement-device-independent Quantum Key Distribution over a 404 km Optical Fiber, *Phys. Rev. Lett.* **117**, 190501 (2016).
 - [14] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, and Hui Dai *et al.*, Satellite-based entanglement distribution over 1200 kilometers, *Science* **356**, 1140 (2017).
 - [15] Masahiro Takeoka, Saikat Guha, and Mark M Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
 - [16] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
 - [17] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate-distance limit of quantum key

- distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [18] Kiyoshi Tamaki, Hoi-Kwong Lo, Wenyan Wang, and Marco Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, arXiv:1805.05511 (2018).
- [19] Xiongfeng Ma, Pei Zeng, and Hongyi Zhou, Phase-matching Quantum Key Distribution, *Phys. Rev. X* **8**, 031043 (2018).
- [20] Xiang-Bin Wang, Zong-Wen Yu, and Xiao-Long Hu, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* **98**, 062323 (2018).
- [21] Won-Young Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [22] Xiang-Bin Wang, Beating the Photon-number-splitting Attack in Practical Quantum Cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [23] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen, Decoy State Quantum Key Distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [24] Igor Devetak, and Andreas Winter, in *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* (The Royal Society, London, 2005), Vol. 461, p. 207.
- [25] Carlton M. Caves, Christopher A. Fuchs, and Rüdiger Schack, Unknown quantum states: The quantum de finetti representation, *J. Math. Phys.* **43**, 4537 (2002).
- [26] Matthias Christandl, Robert König, and Renato Renner, Postselection Technique for Quantum Channels with Applications to Quantum Cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [27] Stefano Pirandola, Capacities of repeater-assisted quantum communications, arXiv:1601.00966 (2016).
- [28] Yi-Heng Zhou, Zong-Wen Yu, and Xiang-Bin Wang, Making the decoy-state measurement-device-independent quantum key distribution practically useful, *Phys. Rev. A* **93**, 042324 (2016).
- [29] Marcos Curty, Koji Azuma, and Hoi-Kwong Lo, Simple security proof of twin-field type quantum key distribution protocol, arXiv:1807.07667 (2018).
- [30] Jie Lin, and Norbert Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [31] Stephen Boyd, and Lieven Vandenberghe, *Convex optimization* (Cambridge University Press, Cambridge, 2004).