Higher key rate of measurement-device-independent quantum key distribution through joint data processing

Cong Jiang¹, Zong-Wen Yu²,⁴, Xiao-Long Hu², and Xiang-Bin Wang¹,²,³,⁵,†

¹ Jinan Institute of Quantum technology, SAICT, Jinan 250101, China
² State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China
³ Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
⁴ Data Communication Science and Technology Research Institute, Beijing 100191, China
⁵ Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China

We propose a method named as double-scanning method, to improve the key rate of measurement-device-independent quantum key distribution (MDI-QKD) drastically. In the method, two parameters are scanned simultaneously to tighten estimate the counts of single-photon pairs and the phase-flip error rate jointly. Numerical results show that the method in this work can improve the key rate by 50% – 250% in a typical experimental set-up. Besides, we study the optimization of MDI-QKD protocol with all parameters including the source parameters and failure probability parameters, over symmetric channel or asymmetric channel. Numerical results show that compared with the optimized results with only the source parameters, the all-parameter-optimization method could improve the key rate by about 10%.

I. INTRODUCTION

The first quantum key distribution (QKD) protocol, BB84 protocol [1] is proposed by Bennett and Brassard in 1984. Based on the quantum laws, QKD could provide unconditionally secure communication between two parties, Alice and Bob [2–7]. But the security of the original BB84 protocol is under the assumption of single photon sources, or else its security would be destroyed by photon number splitting (PNS) attack [8, 9]. The decoy-state method [10–12] is proposed to assure the security of BB84 protocol with imperfect single photon sources such as weak coherent state (WCS) sources. The decoy-state BB84 protocol greatly improves the secure QKD distance in practical and has been widely studied in theory [13–21]. Many experiments of decoy-state BB84 protocol have been reported [22–25]. And the fastest secure QKD distance of BB84 protocol in fiber reaches up to 421 km [25]. The decoy-state BB84 protocol is also applied to QKD between ground and satellite [26] and QKD networks [28, 30]. Besides decoy-state method, the round-robin differential-phase-shift protocol can also effectively defend the PNS attack [31, 32].

Besides the imperfect single photon sources, the imperfect detectors in Bob’s laboratory can also be attacked by Eve [33, 34]. Measurement-Device-Independent (MDI) QKD [35, 36] protocol was proposed to solve all possible detection loopholes. The security of decoy-state MDI-QKD protocol with imperfect sources and detectors has been proved in both infinite key size [36] and finite key size [37]. Many improved schemes of decoy-state MDI-QKD protocol have been proposed to improve the key rate [38–41] and assure its security in practical [42, 43]. The theories of decoy-state MDI-QKD protocol have been widely demonstrated in experiments [44–46]. Among all those theories and experiments, the 4-intensity MDI-QKD protocol [43] performs the best and has been the mainstream protocol of MDI-QKD. Our 4-intensity MDI-QKD protocol has been applied successfully in a number of important experiments: the long distance MDI-QKD over 404 km [52], the high rate MDI-QKD experiment [54], the fault-tolerant MDI-QKD experiment [53], and the on-chip MDI-QKD system [55, 56]. In theoretical studies, the 4-intensity has been further studied for the asymmetric channel [57, 58] which is useful for a network QKD [57] and the unstable channel [58] which is useful for the free-space QKD. Very recently, it is studied with new statistical inequalities [59] to improve the performance.

In original 4-intensity MDI-QKD protocol [43], an important idea is to consider the constraints jointly. Here, we add new joint constraints with a double-parameter scan: we simultaneously scan the error counts and the vacuum related counts and get the worst-case jointly for the counting rate of single-photon pulses and phase-flip error rate. Since new constraints are added, the key rate is improved drastically.

And the prior global optimization of the 4-intensity MDI-QKD protocol is restricted to the source parameters including the intensities of light sources and their corresponding sending probabilities. In this paper, we propose a double-scanning method of the 4-intensity MDI-QKD, and study the global optimization of the 4-intensity MDI-QKD protocol with finite-size effect. The optimized pa-
As the phases of Alice’s and Bob’s phase-randomized WCS pulse are never announced, those pulses are actually the classical mixture of different photon numbers. And the photon numbers distributions of Alice’s and Bob’s sources are

$$a_k^l = \frac{\mu_{k}^{l} e^{-\mu_{a_l}}}{k!}, \quad b_r^k = \frac{\mu_{k}^{r} e^{-\mu_{b_r}}}{k!}, (l, r = o, x, y, z), \quad (2)$$

where $k$ is the photon number in Fock space, and $a_k^l, b_r^k$ are the corresponding probabilities.

If the intensity of the phase-randomized WCS pulse is $\mu_{ax}$, or $\mu_{ay}$ ($\mu_{bx}$, or $\mu_{by}$), its polarization would be randomly modulated as $|+\rangle$ or $|-\rangle$ with equally probability. If the intensity of the phase-randomized WCS pulse is $\mu_{az}$ ($\mu_{bz}$), its polarization would be randomly modulated as $|H\rangle$ or $|V\rangle$ with equally probability. Here, $|+\rangle$ and $|-\rangle$ are the 45° and 135° polarization state respectively, and $|H\rangle$ and $|V\rangle$ are the horizontal and vertical polarization state respectively.

Then Alice and Bob send their prepared pulse to Charlie. Charlie is assumed to perform Bell measurement to the incident pulse pair as shown in Figure II. If only one $|H\rangle$ state detector and one $|V\rangle$ state detector, i.e. $(D_{1H}, D_{1V})$, $(D_{1H}, D_{2V})$, $(D_{2H}, D_{1V})$, or $(D_{2H}, D_{2V})$ click at the same time, Charlie announces to Alice and Bob in the public channel which two detectors clicks, and Alice and Bob take this event as an effective event.

After Alice and Bob repeat the above process for $N$ times, they announce the intensities of pulses in each time window firstly. We denote the two pulse source as $lr(l, r = o, x, y, z)$ if the intensity of Alice’s pulse is $\mu_{al}$ and the intensity of Bob’s pulse is $\mu_{br}$. The time windows with source $zz$ are signal windows. And for each effective event in signal windows, Alice (Bob) denotes it as bit 0 (1) if the polarization of her (his) pulse is modulated as $|H\rangle$, and denotes it as bit 1 (0) if the polarization of her (his) pulse is modulated as $|V\rangle$. Alice and Bob would get two bit strings $Z_A$ and $Z_B$ formed by the corresponding bits of effective events in signal windows.

For the time window with source $oo$, or $ox$, or $xo$, $oy$, or $yo$, $yx$, or $xy$, $gy$, or $yx$, $yy$, it is a decoy window. Alice and Bob also announces the polarization of pulses of decoy windows in the public channel. Without loss of generality, we assume the unitary operator of the beam splitter in Charlie’s detection set-up is

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \quad (3)$$

We denote the pulse pairs as $\alpha\beta(\alpha, \beta = +, -, H, V)$ if the modulated polarization of the pulses sent from Alice and Bob are $|\alpha\rangle$ and $|\beta\rangle$ respectively. Alice and Bob take the effective event of decoy windows as a wrong effective event if it is a $++$ or $--$ pulse pair and Charlie announces $(D_{1H}, D_{2V})$ or $(D_{2H}, D_{1V})$ clicks, or if it is a $+-$ or $-+$ pulse pair and Charlie announces $(D_{1H}, D_{1V})$ or $(D_{2H}, D_{2V})$ clicks. The data of wrong effective events

II. REVIEW OF THE 4-INTENSITY MDI-QKD PROTOCOL

In the 4-intensity MDI-QKD protocol [13], there are four different intensities of sources at Alice’s and Bob’s sides respectively. And the intensities of Alice need not to be the same with those of Bob, e.g., in the situation of asymmetric channel shown in Ref. [58]. In the whole protocol, Alice and Bob send $N$ pulse pairs to Charlie.

In the $i$th time window, as shown in Figure II, Alice (Bob) prepares a phase-randomized WCS pulse whose intensity is randomly chosen from $\mu_{ao} = 0$, $\mu_{az}$, $\mu_{ay}$, or $\mu_{ax}$ ($\mu_{bo} = 0$, $\mu_{bx}$, $\mu_{by}$, or $\mu_{bz}$) with probability $1 - p_{ax} - p_{ay} - p_{az} - p_{by}$, $p_{ax}$, $p_{ay}$, and $p_{az}$ ($1 - p_{bx} - p_{by} - p_{bz}$, $p_{bx}$, $p_{by}$, and $p_{bz}$) respectively. And we assume

$$\mu_{ax} < \mu_{ay}, \quad \mu_{bz} < \mu_{by}. \quad (1)$$

The prior optimization method [44] does not work well with so many parameters to be optimized, thus we propose a new optimize method to solve this problem. Besides, the formulas of the direct results of the joint constraints in the Gaussian model [42] can not be used to the joint constraints of Chernoff bound [60], and we derive the formulas of those in this paper. Based on the method proposed here, we simulate the key rate of the 4-intensity MDI-QKD protocol with symmetric and asymmetric channels.

The prior optimization method [44] does not work well with so many parameters to be optimized, thus we propose a new optimize method to solve this problem. Besides, the formulas of the direct results of the joint constraints in the Gaussian model [42] can not be used to the joint constraints of Chernoff bound [60], and we derive the formulas of those in this paper. Based on the method proposed here, we simulate the key rate of the 4-intensity MDI-QKD protocol with symmetric and asymmetric channels.

The prior optimization method [44] does not work well with so many parameters to be optimized, thus we propose a new optimize method to solve this problem. Besides, the formulas of the direct results of the joint constraints in the Gaussian model [42] can not be used to the joint constraints of Chernoff bound [60], and we derive the formulas of those in this paper. Based on the method proposed here, we simulate the key rate of the 4-intensity MDI-QKD protocol with symmetric and asymmetric channels.

The prior optimization method [44] does not work well with so many parameters to be optimized, thus we propose a new optimize method to solve this problem. Besides, the formulas of the direct results of the joint constraints in the Gaussian model [42] can not be used to the joint constraints of Chernoff bound [60], and we derive the formulas of those in this paper. Based on the method proposed here, we simulate the key rate of the 4-intensity MDI-QKD protocol with symmetric and asymmetric channels.
would help Alice and Bob estimate the upper bound of phase-flip error rate.

Finally, Alice and Bob perform an error correction scheme to correct the difference bits in strings $Z_A$ and $Z_B$, and then perform a privacy amplification scheme according to the key rate formula which is shown in Sec. III to obtain the secure final key strings.

### III. THE CALCULATION OF THE FINAL KEY RATE

To clearly show the calculation process, we have the following definitions. We denote the total number of instances of source $lr = oo, ox, xo, oy, yo, xy, yx, xx, yy$ as $N_{lr}$, and we have

$$N_{lr} = p_{all} p_{err} N.$$  \hspace{1cm} (3)

According to the data of decoy windows, Alice and Bob get the observed value of the number of effective events of source $lr$, $n_{lr}$. We denote the expected value of $n_{lr}$ as $(n_{lr})$, which is needed for the following process. We can estimate the lower and upper bounds of $(n_{lr})$ according to $n_{lr}$ with Chernoff bound which is shown in Appendix A. And we denote the lower and upper bounds of $(n_{lr})$ as $(n_{lr})^L$ and $(n_{lr})^U$ respectively. Besides, we denote the number of wrong effective events of source $xx$ as $m_{xx}$ whose corresponding expected value is $\langle m_{xx} \rangle$. Similarly, we denote the estimated lower and upper bounds of $\langle m_{xx} \rangle$ as $(m_{xx})^L$ and $(m_{xx})^U$ respectively, which can be estimated by the value of $m_{xx}$ with Chernoff bound.

#### A. The prior results

To calculate the final key rate of the 4-intensity MDI-QKD, we need to estimate the lower bound of the counting rate and the upper bound of phase-flip error rate of the single-photon pairs in signal windows, $s_{11,z}$ and $\epsilon_{11}^{ph,U}$. As shown in Ref. [43], in the asymptotic case, the counting rate and the bit-flip error rate of the single-photon pairs in the decoy windows, $\langle s_{11,x} \rangle$ and $\langle \epsilon_{11}^{bit} \rangle$ satisfy

$$\langle s_{11,x} \rangle = \langle s_{11,z} \rangle, \quad \langle \epsilon_{11}^{bit} \rangle = \langle \epsilon_{11}^{ph} \rangle,$$  \hspace{1cm} (4)

where $\langle s_{11,z} \rangle$ and $\langle \epsilon_{11}^{ph} \rangle$ are the expected values of $s_{11,z}$ and $\epsilon_{11}^{ph}$. Thus we can first estimate the lower bound of $\langle s_{11,x} \rangle$ and the upper bound of $\langle \epsilon_{11}^{bit} \rangle$ with the data of decoy windows, then we can get the estimated value of $s_{11,z}$ and $\epsilon_{11}^{ph,U}$ with Chernoff bound,

$$s_{11,z} = \frac{O^L(N_{xx}a_1^2b_1^2 \langle s_{11,x} \rangle_L, \xi_{s_{11}})}{N_{xz}a_1^2b_1^2},$$  \hspace{1cm} (5)

$$\epsilon_{11}^{ph,U} = \frac{O^U(N_{xx}a_1^2b_1^2 \langle s_{11,x} \rangle_L, \xi_{s_{11}})}{N_{xz}a_1^2b_1^2 \langle s_{11,x} \rangle^L},$$  \hspace{1cm} (6)

where $O^U(Y, \xi)$ and $O^L(Y, \xi)$ are defined in Eqs. (A4) and (A6).

According to the formulas in Ref. [43], if $\frac{\mu_{as}}{\mu_{as}} \leq \frac{\mu_{as}}{\mu_{as}}$, we have

$$\langle s_{11,x} \rangle^L = \frac{(S_+)^L - (S_-)^U - \alpha_1^2b_1^2H}{\alpha_1^2a_1^2(b_1^2b_2^2 - b_2^2b_3^2)},$$  \hspace{1cm} (7)

where

$$\langle S_+ \rangle = \frac{a_1^2b_1^2}{N_{xx}} \langle n_{xx} \rangle + \frac{a_1^2b_1^2a_0^2}{N_{oy}} \langle n_{oy} \rangle + \frac{a_1^2b_1^2b_0^2}{N_{yo}} \langle n_{yo} \rangle,$$  \hspace{1cm} (8)

$$\langle S_- \rangle = \frac{a_1^2b_1^2}{N_{yy}} \langle n_{yy} \rangle + \frac{a_1^2b_1^2a_0^2}{N_{oo}} \langle n_{oo} \rangle,$$  \hspace{1cm} (9)

$$\mathcal{H} = \frac{a_0^2}{N_{oo}} \langle n_{oo} \rangle + \frac{b_0^2}{N_{oo}} \langle n_{oo} \rangle - \frac{a_0^2b_0^2}{N_{oo}} \langle n_{oo} \rangle.$$  \hspace{1cm} (10)

And if $\frac{\mu_{as}}{\mu_{as}} \geq \frac{\mu_{as}}{\mu_{as}}$, we have

$$\langle s_{11,x} \rangle^L = \frac{(S_+)^L - (S_-)^L - \alpha_1^2b_1^2H}{b_1^2b_2^2(a_1^2a_2^2 - a_2^2a_3^2)},$$  \hspace{1cm} (11)

where

$$\langle S_+ \rangle' = \frac{a_2^2b_2^2}{N_{xx}} \langle n_{xx} \rangle + \frac{a_2^2b_2^2a_0^2}{N_{oy}} \langle n_{oy} \rangle + \frac{a_2^2b_2^2b_0^2}{N_{yo}} \langle n_{yo} \rangle,$$  \hspace{1cm} (12)

$$\langle S_- \rangle' = \frac{a_2^2b_2^2}{N_{yy}} \langle n_{yy} \rangle + \frac{a_2^2b_2^2a_0^2}{N_{oo}} \langle n_{oo} \rangle.$$  \hspace{1cm} (13)

And the upper bound of $\langle \epsilon_{11}^{bit} \rangle$ satisfies

$$\langle \epsilon_{11}^{bit} \rangle^U = \frac{\langle m_{xx} \rangle^U / N_{xx} - \mathcal{H}/2}{a_1^2b_1^2 \langle s_{11,x} \rangle^L}.$$  \hspace{1cm} (14)

Eqs. (7)(9)(11) are presented by expected values, but we only have observed values from the experiments. We need the Chernoff bound to help us close the gap between the expected values and observed values. And to get the best estimated values of $s_{11,z}^L$ and $\epsilon_{11}^{ph,U}$, we can use the technique of joint constraints [42]. The details of how to get the direct results of joint constraints are shown in Sec. III.C Also, we can get the lower and upper bounds of $\mathcal{H}, \mathcal{H}^L$ and $\mathcal{H}^U$ with the help of joint constraints. For a certain $\mathcal{H}(\mathcal{H} \in [\mathcal{H}^L, \mathcal{H}^U])$, the key rate [57][43] is

$$R(\mathcal{H}) = p_{aa}p_{ba} \{a_1^2b_1^2s_{11,z}^L[1 - h(\epsilon_{11}^{ph,U})] \} - f_{zz}h(E_{zz})$$

$$= - \frac{1}{N} \log_2 \frac{8}{\varepsilon_{cor}} + 2 \log_2 \frac{2}{\varepsilon_{err}^2} + 2 \log_2 \frac{1}{2\varepsilon_{PA}},$$  \hspace{1cm} (15)

where $S_{zz} = n_{zz}/N_{zz}$ is the counting rate of the pulse pairs in signal windows; $E_{zz}$ is the error rate of strings $Z_A$ and $Z_B$; $h(x) = -x \log_2(x) - (1 - x) \log_2(1 - x)$ is the Shannon entropy; $\varepsilon_{cor}$ is the failure probability of error correction; $\varepsilon_{PA}$ is the failure probability of privacy amplification; and $\varepsilon'$ and $\varepsilon$ are the coefficient while using the chain rules of smooth min- and max-entropy.
Finally, by scanning $\mathcal{H}$ in $[\mathcal{H}^L, \mathcal{H}^U]$, we can get the final key rate

$$R = \min_{\mathcal{H} \in [\mathcal{H}^L, \mathcal{H}^U]} R(\mathcal{H}).$$

(16)

With the formula in Eq. (16), the total secure coefficient of the 4-intensity MDI-QKD protocol, $\varepsilon_{\text{tol}}$ is

$$\varepsilon_{\text{tol}} = \varepsilon_{\text{cor}} + 2(\varepsilon' + \tilde{\varepsilon} + 2\varepsilon_c) + \varepsilon_1 + \varepsilon_{PA},$$

(17)

where $\varepsilon_c$ is the probability that the real value of the single-photon error rate of the effective events of single-photon pairs in the signal windows is larger than its estimated value $\varepsilon_{\text{ph},U}$, and $\varepsilon_1$ is the probability that the real value of the counting rate of the single-photon pairs in the signal windows is less than its estimated value $s_{11,2}^L$.

### B. The double-scanning method

In original 4-intensity MDI-QKD protocol, an important idea is to consider the constraints jointly. Here, we add new joint constraints with a double-parameter scan: we simultaneously scan the error counts $\mathcal{M}$ and the vacuum related counts $\mathcal{H}$ and get the worst-case jointly for the counting rate of single-photon pulses and phase-flip error rate, where $\mathcal{M}$ is explained below.

For the effective events of the $xx$ source, they can be divided into two kinds of events, the right effective events and the wrong effective events, which is

$$\langle n_{xx} \rangle = \langle \tilde{m}_{xx} \rangle + \langle m_{xx} \rangle,$$

(18)

where $\langle \tilde{m}_{xx} \rangle$ is the expected value of the number of right events of the $xx$ source, and its corresponding observed value is $\tilde{m}_{xx} = m_{xx} - m_{xx}$. Denote $\mathcal{M} = \langle m_{xx} \rangle$.

If $\frac{n_{xx}}{\mu_{xx}} \leq \frac{n_{ax}}{\mu_{ax}}$, we can rewrite Eq. (7) as

$$\langle s_{11,2}\rangle^L = \langle S_+^L \rangle + \frac{a_1^2 b_2^2}{a_2^2 b_2^2} \mathcal{M} - \langle S_-^U \rangle - \frac{a_1^2 b_2 y_v}{a_2^2 b_2 y_v} \mathcal{H},$$

(19)

where

$$\langle S_+^* \rangle = \frac{a_1^2 b_2^2}{N_{xx}} \langle \tilde{m}_{xx} \rangle + \frac{a_1^2 b_2 y_v}{N_{oy}} \langle n_{oy} \rangle + \frac{a_2^2 b_2 y_v}{N_{yy}} \langle n_{yy} \rangle,$$

(20)

$$\langle S_-^* \rangle = \frac{a_2^2 b_2^2}{N_{ax}} \langle n_{ax} \rangle + \frac{b_2^2}{N_{yo}} \langle n_{oy} \rangle - \frac{a_2^2 b_2}{N_{oo}} \langle n_{oo} \rangle,$$

(21)

$$\mathcal{H} = \frac{a_2^2 b_2}{N_{xx}} \langle n_{ax} \rangle + \frac{b_2^2}{N_{yo}} \langle n_{oy} \rangle - \frac{a_2^2 b_2}{N_{oo}} \langle n_{oo} \rangle.$$

(22)

For the case $\frac{n_{ax}}{\mu_{ax}} \geq \frac{n_{ax}}{\mu_{ax}}$, we can rewrite Eq. (11) in the similar way.

Then for each group $(\mathcal{H}, \mathcal{M})$, we can calculate $s_{11,2}^L$ and $\varepsilon_{\text{ph},U}$ with Eqs. (10,19) and

$$\langle s_{11,2}^L \rangle^U = \frac{\mathcal{M}/N_{xx} - \mathcal{H}/2}{a_1^2 b_2^2 (s_{11,2}^L)^L}. $$

(23)

Then we have

$$R^*(\mathcal{H}, \mathcal{M}) = p_{ax} p_{by} \left\{ a_1^2 b_2^2 s_{11,2}^L [1 - h(\varepsilon_{\text{ph},U})] - f S_{zz}(E_{zz}) \right\} - \frac{1}{N} \left( \log_2 \frac{8}{\varepsilon_{\text{cor}}} + 2 \log_2 \frac{2}{\varepsilon' \varepsilon_c} + 2 \log_2 \frac{1}{\varepsilon_{PA}} \right).$$

(24)

Finally, by scanning $(\mathcal{H}, \mathcal{M})$, we can get the final key rate

$$R^* = \min_{\mathcal{H} \in [\mathcal{H}^L, \mathcal{H}^U], \mathcal{M} \in [\mathcal{M}^L, \mathcal{M}^U]} R^*(\mathcal{H}, \mathcal{M}),$$

(25)

whose total secure coefficient $\varepsilon_{\text{tol}}^*$ is

$$\varepsilon_{\text{tol}}^* = \varepsilon_{\text{cor}} + 2(\varepsilon' + \tilde{\varepsilon} + 2\varepsilon_c) + \varepsilon_1^* + \varepsilon_{PA},$$

(26)

where $\varepsilon_1^*$ is the failure probability that the real value of the counting rate of the single-photon pairs in the signal windows is less than its estimated value $s_{11,2}^L$.

### C. The direct results of joint constraints with Chernoff bound

In this part, we would take Eq. (20) as an example to show how to get the direct results of joint constraints with Chernoff bound. To get the lower bound of $\langle S_+ \rangle^*$, we can apply the technique of linear programming to solve this problem, which is

$$\langle S_+ \rangle^* = \frac{a_1^2 b_2 y_v}{N_{xx}} \langle \tilde{m}_{xx} \rangle + \frac{a_1^2 b_2 y_v}{N_{yo}} \langle n_{oy} \rangle + \frac{a_2^2 b_2 y_v}{N_{yy}} \langle n_{yy} \rangle.$$

(27)

And if the pre-setted failure probability while using Chernoff bound is $\xi$, the failure probability in estimating $\langle S_+ \rangle^*$ is $3\xi$. But if we notice the following joint constraints

$$\langle m_{xx} \rangle \geq E^L(\tilde{m}_{xx}, \xi),$$

$$\langle n_{oy} \rangle \geq E^L(n_{oy}, \xi),$$

$$\langle n_{yy} \rangle \geq E^L(n_{yy}, \xi),$$

$$\langle \tilde{m}_{xx} \rangle + \langle n_{oy} \rangle \geq E^L(\tilde{m}_{xx} + n_{oy}, \xi),$$

$$\langle \tilde{m}_{xx} \rangle + \langle n_{yy} \rangle \geq E^L(\tilde{m}_{xx} + n_{yy}, \xi),$$

$$\langle \tilde{m}_{xx} \rangle + \langle n_{yy} \rangle \geq E^L(\tilde{m}_{xx} + n_{yy}, \xi),$$

we can apply the technique of linear programming to Eq. (20) to get better estimated $\langle S_+ \rangle^*$ with those constraints. And at most three of the constraints would be used in the final results, the failure probability in estimating $\langle S_+ \rangle^*$ with this method is still $3\xi$. If we run the program of linear programming to solve this problem, much time would be cost especially when we optimize the parameters to get the highest key rate. But fortunately, we have the following direct results of this special linear programming problem.
We can abstract the above linear programming problem into
\[
\begin{align*}
\min_{g_1, g_2, g_3} & \quad F = \gamma_1 g_1 + \gamma_2 g_2 + \gamma_3 g_3, \\
\text{s.t.} & \quad g_1 \geq E^L(\bar{g}_1, \xi_1), \\
& \quad g_2 \geq E^L(\bar{g}_2, \xi_1), \\
& \quad g_3 \geq E^L(\bar{g}_3, \xi_1), \\
& \quad g_1 + g_2 \geq E^L(\bar{g}_1 + \bar{g}_2, \xi_2), \\
& \quad g_2 + g_3 \geq E^L(\bar{g}_2 + \bar{g}_3, \xi_2), \\
& \quad g_1 + g_3 \geq E^L(\bar{g}_1 + \bar{g}_3, \xi_2), \\
& \quad g_1 + g_2 + g_3 \geq E^L(\bar{g}_1 + \bar{g}_2 + \bar{g}_3, \xi_3),
\end{align*}
\]
where \(\gamma_1, \gamma_2, \gamma_3, g_1, g_2, g_3, \bar{g}_1, \bar{g}_2, \bar{g}_3\) all are positive values and \(E^L(X, \xi)\) is defined in Eq. (21). And if we denote \(\{\gamma_1^*, \gamma_2^*, \gamma_3^*\}\) as the ascending order of \(\{\gamma_1, \gamma_2, \gamma_3\}\), and \(\{\bar{g}_1^*, \bar{g}_2^*, \bar{g}_3^*\}\) is the corresponding rearrange of \(\{\bar{g}_1, \bar{g}_2, \bar{g}_3\}\) according to the ascending order of \(\{\gamma_1, \gamma_2, \gamma_3\}\), we have the lower bound of \(F\) under those constraints
\[
\begin{align*}
F_L(\gamma_1, \gamma_2, \gamma_3, \bar{g}_1, \bar{g}_2, \bar{g}_3, \xi_1, \xi_2, \xi_3)
= & \gamma_1^* E^L(\bar{g}_1^* + \bar{g}_2^* + \bar{g}_3^*, \xi_3) + (\gamma_2^* - \gamma_1^*) E^L(\bar{g}_2^* + \bar{g}_3^*, \xi_2) \\
+ & (\gamma_3^* - \gamma_2^*) E^L(\bar{g}_3^*, \xi_1).
\end{align*}
\] (28)

Note that the results of Eq. (28) may not be the accessible minimum value of the above linear programming problem in some extreme case. But from the perspective of simplifying calculations, we can take Eq. (28) as the direct results and this does not affect the security of the protocol. And if we want to get the maximum value under the joint constraints, we can simply replace \(E^L(X, \xi)\) by \(E^U(X, \xi)\) in Eq. (28), where \(E^U(X, \xi)\) is defined in Eq. (22). Specifically, we have the upper bound of \(F\)
\[
\begin{align*}
F_U(\gamma_1, \gamma_2, \gamma_3, \bar{g}_1, \bar{g}_2, \bar{g}_3, \xi_1, \xi_2, \xi_3)
= & \gamma_1^* E^U(\bar{g}_1^* + \bar{g}_2^* + \bar{g}_3^*, \xi_3) + (\gamma_2^* - \gamma_1^*) E^U(\bar{g}_2^* + \bar{g}_3^*, \xi_2) \\
+ & (\gamma_3^* - \gamma_2^*) E^U(\bar{g}_3^*, \xi_1).
\end{align*}
\] (29)

IV. THE OPTIMIZATION METHOD

To get the final key rate with observed values of the experiment, we first calculate the lower bound of \(\langle S_+ \rangle^*\) with Eqs. (21) and (22), which is
\[
\langle S_+ \rangle^* = F_L\left( \frac{a_1 b_1^*}{N_{yy}} + \frac{a_2 b_2^* a_0^*}{N_{yy}} + \frac{a_3 b_3^* b_0^*}{N_{yy}}, m_{xx}, n_{yy}, n_{ox}, \xi_{S_1^+}, \xi_{S_2^+}, \xi_{S_3^+}, \xi_{S_4^+}, \xi_{S_5^+}, \xi_{S_6^+} \right),
\] (30)
where \(\xi_{S_1^+}, \xi_{S_2^+}, \xi_{S_3^+}\) are the failure probabilities while using Chernoff bound, and the following similar symbols are also the failure probabilities. Then we can calculate the upper bound of \(\langle S_- \rangle\) with Eqs. (21) and (20), which is
\[
\langle S_- \rangle^* = F_U\left( \frac{a_1 b_1^*}{N_{yy}} + \frac{a_2 b_2^* a_0^*}{N_{yy}} + \frac{a_3 b_3^* b_0^*}{N_{yy}}, 0, n_{yy}, n_{ox}, n_{xx}, n_{ox}, n_{xx}, n_{ox}, 0, \xi_{S_1^-}, \xi_{S_2^-}, \xi_{S_3^-}, \xi_{S_4^-}, \xi_{S_5^-}, \xi_{S_6^-} \right).
\] (31)
And with the similar method, we can get the lower and upper bounds of \(H\), which are
\[
\begin{align*}
H_L &= F_L\left( \frac{a_0^*}{N_{xo}}, \frac{b_0^*}{N_{xo}}, 0, n_{ox}, n_{xx}, n_{ox}, 0, \xi_{H_{1}^L}, \xi_{H_{2}^L} \right), \\
H_U &= F_U\left( \frac{a_0^*}{N_{xo}}, \frac{b_0^*}{N_{xo}}, 0, n_{ox}, n_{xx}, n_{ox}, 0, \xi_{H_{1}^U}, \xi_{H_{2}^U} \right).
\end{align*}
\] (32)
It is easy to check that
\[
\begin{align*}
\mathcal{M}_L &= E^L(m_{xx}, \xi_{m}^L), \\
\mathcal{M}_U &= E^U(m_{xx}, \xi_{m}^U).
\end{align*}
\] (33)
For each group \((\mathcal{H}, \mathcal{M})\), we can calculate the value of \(s_{11,1}^{\text{ph},L}\) with Eqs. (19)-(31) and the value of \(e_{11}^{\text{ph},U}\) with Eqs. (23). Finally, by scanning \((\mathcal{H}, \mathcal{M})\), we can get the final key rate \(R^*\) with Eqs. (21) and (24).

With the calculation method above, the failure probability of the estimation of \(s_{11,1}^{\text{ph},L}\) is
\[
\begin{align*}
\varepsilon_{11}^L &= \xi_{S_1^+} + \xi_{S_2^+} + \xi_{S_3^+} + \xi_{S_4^+} + \xi_{S_5^+} + \xi_{S_6^+}, \\
&+ \xi_{H_{1}^L} + \xi_{H_{2}^L} + \xi_{H_{1}^U} + \xi_{H_{2}^U} + \xi_{m} + \xi_{m}^U,
\end{align*}
\] (34)
and the failure probability of the estimation of \(e_{11}^{\text{ph},U}\) is
\[
\varepsilon_{e} = \xi_{e_{11}}.
\]
If we set \(\varepsilon_{\text{tol}}^*\) as a fixed value, then we can regard \(R^*\) as the function of those failure probabilities. With the observed values of experiment, we can optimize \(R^*\) to get the highest key rates. Besides, in the view of numerical simulation, the observed values could be regarded as the function of source parameters if the channel loss and the properties of detection set-ups are known. That is to say, \(R^*\) have the following functional form
\[
R^* = R^*(\text{paraA}, \text{paraB}),
\] (35)
where
\[
\begin{align*}
\text{paraA} &= [ \mu_{ox}, \mu_{ay}, \mu_{az}, \mu_{ay}, \mu_{az}, \mu_{ox}, \mu_{ox}, \mu_{ay}, \mu_{ay}, \mu_{az}, \mu_{az}, \mu_{ox}, \mu_{ox}, \mu_{ay}, \mu_{ay}, \mu_{az}, \mu_{az} ], \\
\text{paraB} &= [ \xi_{S_1^+}, \xi_{S_2^+}, \xi_{S_3^+}, \xi_{S_4^+}, \xi_{S_5^+}, \xi_{S_6^+}, \xi_{H_{1}^L}, \xi_{H_{1}^U}, \xi_{H_{2}^L}, \xi_{H_{2}^U}, \xi_{m}, \xi_{m}^L, \xi_{m}^U, \varepsilon_{\text{cor}}, \varepsilon^e, \xi_{e_{11}} ].
\end{align*}
\] (36)
There are 29 parameters needed to be optimized if we want to get the highest \(R^*\), which is much more than the
6 parameters in Ref. 43 or 12 parameters in Ref. 58. Thus the optimization method shown in Ref. 58 does not work well in this optimization problem. In this paper, we would use the random direction method to optimize \( R^* \) with 29 parameters. And the details of the random direction method are shown in Appendix B.

V. NUMERICAL SIMULATION

In this part, we show the simulation results of this work and compare with the results of prior art works.

![Graph](image1)

**Figure 2**: The key rates of this work and the original 4-intensity MDI-QKD protocol in the symmetric channel. The experimental parameters used here are listed in Table I. The ‘Improved-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Improved-6-parameter’ line is the results of this work with only the source parameters optimized. The ‘Original-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Original-6-parameter’ line is the results of this work with only the source parameters optimized.

![Graph](image2)

**Figure 3**: The key rates of this work and the original 4-intensity MDI-QKD protocol in the asymmetric channel. The distance difference between Alice to Charlie and Bob to Charlie is set as 20 km. The ‘Improved-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Improved-6-parameter’ line is the results of this work with only the source parameters optimized. The ‘Original-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Original-6-parameter’ line is the results of this work with only the source parameters optimized.

| \( p_d \) | \( e_d \) | \( \eta_d \) | \( f \) | \( \alpha_f \) | \( \varepsilon_{tol} \) | \( N \) |
|---|---|---|---|---|---|---|
| \( 1.0 \times 10^{-7} \) | 1.5\% | 40.0\% | 1.1 | 0.2 | \( 1.0 \times 10^{-10} \) | \( 1.0 \times 10^{10} \) |

**TABLE I**: List of experimental parameters used in numerical simulations. Here \( p_d \) is the dark counting rate per pulse of Charlie’s detectors; \( e_d \) is the misalignment-error probability; \( \eta_d \) is the detection efficiency of Charlie’s detectors; \( f \) is the error correction inefficiency; \( \alpha_f \) is the fiber loss coefficient \((dB/km)\); \( \varepsilon_{tol} \) is the total secure coefficient; \( N \) is the number of total pulse pairs sent out in the protocol.

We use the linear model to simulate the observed values. The experimental parameters used in the numerical simulation are listed in Table I. Without loss of generality, we assume the property of Charlie’s detectors are the same. The distance between Alice and Charlie is \( L_A \), and that between Bob and Charlie is \( L_B \). The total distance between Alice and Bob is \( L = L_A + L_B \). In our numerical simulation, we set \( L_A = L_B \) for the symmetric case and \( L_A - L_B = \) constant for the asymmetric case.

Figure 2 and Figure 3 are the numerical results of this work and the original 4-intensity MDI-QKD protocol with the symmetric channel and asymmetric channel, respectively. In the symmetric case, we set symmetric source parameters for Alice and Bob, that is to say, \( p_{ax} = p_{bx} \), \( \mu_{ax} = \mu_{bx} \) and so on. In the asymmetric case, the distance difference between Alice to Charlie and Bob to Charlie is set as 20 km. The ‘Improved-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Improved-6-parameter’ or ‘Improved-12-parameter’ line is the results of this work with only the source parameters optimized. The ‘Original-all-parameter’ line is the results of this work optimized with all the parameters including the source parameters and failure probability parameters. The ‘Original-6-parameter’ or ‘Original-12-parameter’ line is the results of this work with only the source parameters optimized.
parameters.

Table I is the comparison of the key rates of this work and the original 4-intensity MDI-QKD protocol in the symmetric channel. The experimental parameters used here are listed in Table I. The results show that the improved method proposed here could improve the key rates of 4-intensity MDI-QKD protocol by more than 50%-250%. Compare with the optimized results with only the source parameters, the all-parameter optimize rates of 4-intensity MDI-QKD protocol by more than 10%.

VI. CONCLUSION

Based on the 4-intensity MDI-QKD protocol, we propose a double-scanning method to further improve the key rate. Numerical results show that the method in this work can improve the key rate by 50%—250%. The method in this work can directly apply to the existing experimental parameters; If \( R_{opt} > R_{temp} \), then let \( Para := Para + d_{step} \times D_{dir} \), \( R_{temp} = R_{temp} \), \( C = 1 \); if \( R_{temp} \leq R_{opt} \), then let \( C := C + 1 \). Finally go to step (ii).

Appendix A: Chernoff bound

The Chernoff bound can help us estimate the expected value from their observed values. Similar to Eqs. (A1)–(A4), the observed value, \( O \), and its expected value, \( Y \), satisfy

\[
O^L(Y, \xi) = [1 + \delta_1'(Y, \xi)]Y, \quad (A5)
\]

\[
O^U(Y, \xi) = [1 - \delta_2'(Y, \xi)]Y, \quad (A6)
\]

where we can obtain the values of \( \delta_1'(Y, \xi) \) and \( \delta_2'(Y, \xi) \) by solving the following equations

\[
\left( \frac{e^{\delta_1'}}{(1 + \delta_1')^{1+\delta_1'}} \right)^{\frac{X}{1+\delta_1'}} = \xi, \quad (A7)
\]

\[
\left( \frac{e^{-\delta_2'}}{(1 - \delta_2')^{1-\delta_2'}} \right)^{\frac{X}{1-\delta_2'}} = \xi, \quad (A8)
\]

where \( \xi \) is the failure probability.

Besides, we can use the Chernoff bound to help us estimate their real values from their expected values. Similar to Eqs. (A1)–(A4), the observed value, \( O \), and its expected value, \( Y \), satisfy

\[
O^L(Y, \xi) = [1 + \delta_1(Y, \xi)]Y, \quad (A5)
\]

\[
O^U(Y, \xi) = [1 - \delta_2(Y, \xi)]Y, \quad (A6)
\]

where we can obtain the values of \( \delta_1(Y, \xi) \) and \( \delta_2(Y, \xi) \) by solving the following equations

\[
\left( \frac{e^{\delta_1}}{(1 + \delta_1)^{1+\delta_1}} \right)^{\frac{X}{1+\delta_1}} = \xi, \quad (A7)
\]

\[
\left( \frac{e^{-\delta_2}}{(1 - \delta_2)^{1-\delta_2}} \right)^{\frac{X}{1-\delta_2}} = \xi, \quad (A8)
\]

Appendix B: The random direction method

Here we introduce the random direction method as follows:

Initialization Find a original point \( Para = [paraA_o, paraB_o] \) where \( R^*(Para) > 0 \). Set initial step \( d_{step} \) and minimum step \( d_{min} \). Set the maximum number of cycles \( C_{max} \).

(i). If \( d_{step} < d_{min} \), stop the optimization programme and output the value of \( R_{opt} = R^*(Para) \) as the optimal key rate, where \( Para \) is the corresponding optimal parameters; If \( d_{step} > d_{min} \), set the cycle count \( C = 1 \). Then go to step (ii).

(ii). If \( C > C_{max} \), let \( d_{step} := d_{step}/5 \), then go to step (i); if \( C \leq C_{max} \), go to step (iii).

(iii). Use a Gaussian random number generator to generate 29 random numbers, then normalize these random numbers and put them into the array \( D_{dir} \). Then calculate \( R_{temp} = R^*(Para + d_{step} \times D_{dir}) \). If \( R_{temp} > R_{opt} \), then let \( Para := Para + d_{step} \times D_{dir}, R_{opt} = R_{temp}, C = 1 \); if \( R_{temp} \leq R_{opt} \), then let \( C := C + 1 \). Finally go to step (ii).

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (1984), pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics 74, 145 (2002).
[3] N. Gisin and R. Thew, Nature Photonics 1, 165 (2007).
[4] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Reviews of Modern Physics 92, 025002 (2020).
[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring,
TABLE II: The key rates of this work and the original 4-intensity MDI-QKD protocol in the symmetric channel. The experimental parameters used here are listed in Table I.

| L       | 30 km   | 60 km   | 90 km   |
|---------|---------|---------|---------|
| method  | SPO     | APO     | SPO     | APO     |
| Ref. [43]| 1.33 × 10^{-4} | 1.36 × 10^{-4} | 9.94 × 10^{-6} | 1.04 × 10^{-5} | 1.83 × 10^{-7} | 2.08 × 10^{-7} |
| This work| 1.63 × 10^{-4} | 1.68 × 10^{-4} | 1.5 × 10^{-5} | 1.58 × 10^{-5} | 6.46 × 10^{-7} | 7.17 × 10^{-7} |

SPO: source-parameter-optimization; APO: all-parameter-optimization.
M. Zhang, G.-C. Guo, and Z.-F. Han, Physical Review Letters 115, 160502 (2015).

[51] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nature Photonics 10, 312 (2016).

[52] 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, et al., Physical Review Letters 117, 190501 (2016).

[53] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Optica 4, 1016 (2017).

[54] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics 9, 397 (2015).

[55] H. Semenenko, P. Sibson, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Optica 7, 238 (2020).

[56] L. Cao, W. Luo, Y. Wang, J. Zou, R. Yan, H. Cai, Y. Zhang, X. Hu, C. Jiang, W. Fan, et al., Physical Review Applied accepted (2020).

[57] W. Wang, F. Xu, and H.-K. Lo, Physical Review X 9, 041012 (2019).

[58] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang, Scientific Reports 8, 17634 (2018).

[59] H. Chau, arXiv preprint arXiv:2003.08549 (2020).

[60] H. Chernoff et al., The Annals of Mathematical Statistics 23, 493 (1952).