Improved statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method

Zong-Wen Yu\textsuperscript{1,2}, Yi-Heng Zhou\textsuperscript{1,3}, and Xiang-Bin Wang\textsuperscript{1,3,4}\textsuperscript{*}

\textsuperscript{1}State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, Peoples Republic of China
\textsuperscript{2}Data Communication Science and Technology Research Institute, Beijing 1000841, China
\textsuperscript{3}Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China
\textsuperscript{4}Shandong Academy of Information and Communication Technology, Jinan 250101, Peoples Republic of China

We present an improved statistical fluctuation analysis for measurement device independent quantum key distribution with three-intensity decoy-state method. After introducing some relations among different fluctuation ratios, we reanalysis the effect of statistical fluctuations and obtain more tight estimations. Based on this, we find that the key rate is improved by about 97% than the result given by Xu., et al. (Phys. Rev. A 89, 052333) in the case of data-size $10^{12}$ for the distance 50km.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) is one of the most successful applications of quantum information processing. QKD can provide unconditional security based on the laws of quantum physics\textsuperscript{1,2}. However, owing to the imperfections in real-life implementations of QKD, a large gap between its theory and practice remains unfiled. Security for real set-ups of QKD\textsuperscript{1,2} has become a major problem in this area recent years. The security loopholes for practical set-ups are mainly due to the imperfect single-photon source and the limited efficiency of the detectors. Fortunately, by using the decoy-state method\textsuperscript{3-13}, it has been shown that the unconditional security of QKD can still be assured with an imperfect single-photon source\textsuperscript{14,15}.

Besides the source imperfection, the defect in the detectors is another threaten to the security\textsuperscript{16}. To patch up this, several approaches have been proposed. One is the device independent QKD (DI-QKD)\textsuperscript{17}. This technique does not require detailed knowledge of how QKD devices work and can be proved secure.

Recently, an idea of measurement device independent QKD (MDI-QKD)\textsuperscript{18,19} was proposed based on the idea of entanglement swapping\textsuperscript{18,19}. The key idea of MDI-QKD is that both legitimate users, Alice and Bob, are senders. Neither Alice nor Bob performs any measurement, but only send out quantum signals to the un-trusted third party (UTP), who is supposed to perform a Bell state measurement. After Alice and Bob send out signals, they wait for UTP’s announcement of weather he has obtained a successful event after detection, and proceed to the standard postprocessing of their sifted data. The only assumption needed in MDI-QKD is that the preparation of the quantum signal sources by Alice and Bob. By using the decoy-state method, Alice and Bob can use imperfect single-photon sources\textsuperscript{19,21}. Hence, MDI-QKD can remove all detector side-channel attacks and is also practical for current technology. Owing to this, it has attracted a lot of scientific attention. So far, the decoy-state MDI-QKD has been studied by a number of scientists both experimentally\textsuperscript{22-24} and theoretically\textsuperscript{21,22,23}.

As is well known, in any real experiment, we have to consider the effect of statistical fluctuations caused by a finite-size key. Such an analysis is crucial to ensure the security of MDI-QKD in practice set-ups. In precious works, the methods of standard error analysis is most commonly used\textsuperscript{25-36}. M. Curty et al. present a rigorous finite-key analysis with Chernoff bound in Ref.\textsuperscript{30}. In all these works, the relations among the statistical fluctuation ratios are not considered sufficiently. Actually, as shown in this paper, the statistical ratios are interdependent from each other with a given security bound. By using these relations among the statistical fluctuation ratios, we present an improved statistical fluctuation analysis. Based on this, we obtain the more tight bounds of $Z_{11}$ and $X_{11}$ which lead to a higher key rate.

Here in this work, we first show some crude analytical methods with explicit formulas to estimate the lower bounds of $s_{11}$ and the upper bounds of $e_{11}$. In the third section, we present an improved statistical fluctuation analysis by introducing relations among the fluctuation ratios. The article is ended with a concluding remark.

II. THREE-INTENSITY DECOY-STATE METHOD FOR MDI-QKD

In the MDI-QKD protocol, each time a pulse-pair (two-pulse state) is sent to the relay for detection. The relay is controlled by an UTP. The UTP will announce whether the pulse-pair has caused a successful event. Those bits corresponding to successful events will be post-selected.


\*Email Address: xbwang@mail.tsinghua.edu.cn
and further processed for the final key. Since the imperfect single-photon sources can only be used in real set-ups, we need the decoy-state method for security in practice.

In the three-intensity decoy-state protocol, we assume Alice (Bob) has three different sources in each bases, say $o_A, x_A, y_A$ ($o_B, x_B, y_B$) which can only emit three different states $\rho_{oA} = |0\rangle\langle 0|$, $\rho_{x_A}^\omega, \rho_{y_A}^\omega$ ($\rho_{oB} = |0\rangle\langle 0|$, $\rho_{x_B}^\omega, \rho_{y_B}^\omega$) respectively, where $\omega = X$ for $X$ basis and $\omega = Z$ for $Z$ basis. In photon number space, suppose
\[
\rho_{x_A}^\omega = \sum_k a_k^\omega |k\rangle \langle k|, \quad \rho_{y_A}^\omega = \sum_k a_k^\omega |k\rangle \langle k|, \quad (1)
\]
\[
\rho_{x_B} = \sum_k b_k^\omega |k\rangle \langle k|, \quad \rho_{y_B}^\omega = \sum_k b_k^\omega |k\rangle \langle k|, \quad (2)
\]
We shall consider the decoy-state method in each basis separately. For simplicity, we shall omit the superscripts $\omega$ of $\rho_{x_A}, \rho_{y_A}$ and $\rho_{x_B}, \rho_{y_B}$ in what follows of this article provided that the omission does not cause any confusion. We request the states above satisfy the following very important condition
\[
mn a_k' \geq a_k \geq a_1, \quad b_k' \geq b_k \geq b_1, \quad (3)
\]
for $k \geq 2$. The imperfect sources used in practice such as the coherent state source, the heralded source out of the parametric-down conversion, satisfy the above restrictions. Given a specific type of source, the above listed different states have different averaged photon numbers (intensities), therefore the states can be obtained by controlling the light intensities. At each time, Alice will randomly choose source $\rho_{lA}$ with probability $p_{lA}$ and $\omega$ basis with probability $p_{\omega|l}$ for $l = o, x, y$. Similarly, Bob will randomly choose source $\rho_{lB}$ with probability $p_{lB}$ and $\omega$ basis with probability $p_{\omega|l}$ for $r = o, x, y$. The pulse from Alice and the pulse from Bob form a pulse pair and are sent to UTP. We regard equivalently that each time a two-pulse source is selected and a pulse pair (one pulse from Alice, one pulse from Bob) is emitted. For postprocessing, Alice and Bob evaluate the data sent in two bases separately. The $Z$-basis is used for key generations, while the $X$-basis is used for testing against tampering and the purpose of quantifying the amount of privacy amplification needed. Here, we use the capital letters $Z(X)$ for the bases and the lowercase letters $o, x, y$ for the different sources. Here and after, we omit the subscripts $A$ and $B$ without causing any ambiguity.

In order to calculate the secret final key rate of this protocol, we need the lower bound of the yield $s_{11}^l$ and the upper bound of the error rate $e_{11}$.

### A. Asymptotic case

As shown in Ref. [20], we denote $l r$ as the two-pulse source when Alice uses source $l$ and Bob uses $r$, and $l, r$ can take $o, x, y$. For example, two-pulse source $o y$ denote the case when Alice use vacuum source $\rho_o$ and Bob uses the signal source $\rho_y$. There are 9 two-pulse sources $l r$ in each bases of the three-intensity decoy-state method. We also denote $S_{1r}$ as the yield of two-pulse source $l r$. $S_{1r}$ are observed values and will be regarded as known values here. However, the yields $s_{1r}^l$ for the two-pulses states $|m\rangle \langle m| \otimes |n\rangle \langle n|$ out of source $l r$ cannot be directly observed. In the asymptotic case, we assume that $s_{1r}^l$ for all $l r$ are the same and we can denote all of them by $s_{11}$, i.e.
\[
s_{1r}^l = s_{1r}^l = s_{11}. \quad (4)
\]
Given this, we can formulate the very important unknown variable $s_{11}$ by using constraints
\[
S_{1r} = \sum_{m,n} c_{mn}^l s_{11}. \quad (5)
\]
if the state for the two-pulse source $l r$ is
\[
\rho_{1r} = \sum_{m,n} c_{mn}^l |m\rangle \langle m| \otimes |n\rangle \langle n|. \quad (6)
\]
In Refs. [20, 31], we presented some explicit formulas for the practical decoy-state implementation through using part of the above constraints. Explicitly, we rewrite these formulas into its equivalent forms that are shown in Appendix A.

### B. Non-asymptotic case

In any real experiment, the total pulses sent by Alice and Bob are finite. So the number of sifted keys is always finite. In order to extract the secure final key, we have to consider the effect of statistical fluctuations caused by the finite-size key. This is to say, yields of the same two-pulse state out of different sources are different, i.e.,
\[
s_{1r}^l \neq s_{1r}^l. \quad (7)
\]
In such a case, there are too many variants $\{s_{1r}^l\}$. To obtain the lower bound value for $s_{11}$ and upper bound value for $e_{11}$, one can implement the idea of Ref. [13]. Define $\hat{s}_{11}$ as the mean value of yield of state $|m n\rangle$ produced by all sources used in the decoy-state method,
\[
\hat{s}_{11} = \sum_{l r} p_{lr} c_{mn}^l s_{1r}^l. \quad (8)
\]
Based on this, we can also define quantity
\[
\hat{S}_{1r} = \sum_{m,n=0} c_{mn}^l s_{mn}^l. \quad (9)
\]
Replacing $S_{1r}$ by $\hat{S}_{1r}$ in Eq. (5), we obtain formulate the lower bound of $\hat{s}_{11}$. Note that even though $S_{1r}$ are known
values directly observed in an experiment, \( \hat{S}_{tr} \) are not. However, given the values \( S_{tr} \) and \( N_{tr} \), we have

\[
\hat{S}_{tr} = S_{tr} (1 + \delta_{tr}).
\]

With a probability larger than \( 1 - \epsilon \), \( \delta_{tr} \) is in the range of

\[
|\delta_{tr}| \leq n_\delta \sqrt{1/N_{tr} S_{tr}}.
\]

In a Ref. [13], \( n_\delta \) is set to be 10. Here in this paper we shall set

\[
n_\delta = 5.3
\]

which corresponds to \( \epsilon = 10^{-7} \) [31] in our numerical simulation, so as to make a fair comparison with [30]. Therefore, we can formulate the lower bound value of \( s_{11} \) by \( S_{tr} \). Similarly, one can also calculate the averaged value of \( e_{11}^X \) by \( T_{tr} \), with \( T_{tr} = \sum_{m,n=0}^\infty c_{tr}^{\omega} s_{mn} c_{mn}^{\omega} \) being the error yields. Details of all these can be seen in Appendix B. In the calculation, previous work [30] used the worst-case values for each individual \( \delta_{tr} \) in Eqs. (9,10).

Here in this work, instead of using this simple worst-case calculation, we propose a more efficient method to treat the statistical fluctuations in the decoy-state MDAQKD. In our method, we don't have to consider the fluctuation of each quantities separately. For example, in estimating the quantity \( e_{11}^X \) in Eq. (11), in a symmetric protocol where \( a_0 = b_0 \), we need to calculate bound of \( T_{0x} + T_{x0} \). The simple worst-case result would calculate the worst-case fluctuation for \( T_{0x} \) and \( T_{x0} \) separately. However, we can treat this more efficiently by considering the statistical fluctuations jointly. Say, we regard sources \( S_{0x} \) and \( S_{x0} \) as one source \( 0x \) which emits state \( \frac{1}{\sqrt{2}} (\rho_{ox} + \rho_{xo}) \). For such a source, the error yield \( T_{0x} + T_{x0} = 2T_{0x} \). We then only need to consider the fluctuation for only one quantity \( T_{0x} \). This will improve the performance of the decoy-state protocol. In the next section we present a systematic study of this joint constraints in the statistical fluctuation.

III. IMPROVED STATISTICAL FLUCTUATION ANALYSIS

In order to estimate the lower bound of \( s_{11}^Z \) and the upper bound of \( e_{11}^X \), we need the values of yields \( S_{tr} \) and error yields \( T_{tr} \) \( \{l, r = o, x, y \} \) for this 3-intensity decoy-state protocol, which can be observed in experiment. On the other hand, in any real experiment, we have to consider the effect of statistical fluctuation caused by a finite-size key. As discussed above, we need introduce the fluctuation ratios \( \delta_{tr} \) and \( \tau_{tr} \) to obtain the values of yields \( \hat{S}_{tr} \) and error yields \( \hat{T}_{tr} \) with its observed values \( S_{tr} \) and \( T_{tr} \). With a given security bound, we can bound the fluctuation ratios \( \delta_{tr}^\omega \) and \( \tau_{tr}^X \), such as the relations presented in Eq. (13) and Eq. (14). In all previous works, the relations among these fluctuation ratios have not been considered sufficiently. In this section, we will introduce some relations among these ratios firstly. With these relations, we show the improved formulas to estimate the lower bound of \( s_{11}^Z \) and the upper bound of \( e_{11}^X \) which can help us to extract the secret final key with a higher rate.

A. Relations among the fluctuation ratios

When we do the statistical fluctuation analysis, we need to choose a proper security bound firstly. With a given definite security bound, we can bound the fluctuation ratios \( \delta_{tr}^\omega \) and \( \tau_{tr}^X \) by Eq. (13) and Eq. (14) respectively. In order to obtain the relations among these fluctuation ratios, we need to reconsider the grouping of the successful events announced by UTP.

For the sake of clarity, we consider the relation between \( \delta_{tr}^\omega \) and \( \delta_{tr}^{l,r} \) firstly. As defined above, we know that \( \delta_{tr}^\omega \) and \( \delta_{tr}^{l,r} \) are the fluctuation ratios for the observed yields \( S_{tr}^l \) and \( S_{tr}^r \) respectively. These two observable are corresponding to the successful events with source pairs \( \{(l_1, r_1), (l_2, r_2)\} \). If we group all the successful events of these two types together, and denote \( J_2 = \{(l_1, r_1), (l_2, r_2)\} \), the value of the yield is

\[
\hat{S}_{J_2} = S_{J_2}^l (1 + \delta_{J_2}^l),
\]

where \( \delta_{J_2}^l \) is the fluctuation ratio for the observable \( S_{J_2}^l \). Similarly, the ratio \( \delta_{J_2}^r \) possesses the following property with the given definite security bound

\[
|\delta_{J_2}^r| \leq \sqrt{N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r} \leq \delta_{J_2}^r.
\]

In this relation, \( N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r \) is the number of successful events announced by UTP when Alice and Bob use source pairs in \( J_2 \) in the \( \omega \) basis. Reconsidering the definition of \( S_{J_2}^l \), we know that

\[
N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r = (N_{J_2}^l + N_{J_2}^r) S_{J_2}^l.
\]

Now we take into account the mean values. The above relation can be written into

\[
N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r = (N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r) (1 + \delta_{J_2}^l).
\]

Then we can find out the relations between these two ratios \( \delta_{J_2}^l \) and \( \delta_{J_2}^r \)

\[
|N_{J_2}^l S_{J_2}^l \delta_{J_2}^l + N_{J_2}^r S_{J_2}^r \delta_{J_2}^r| \leq n_\delta \sqrt{|N_{J_2}^l S_{J_2}^l + N_{J_2}^r S_{J_2}^r|}.
\]

where Eq. (13) has been used.

Generally, we can group the successful events of any source pairs together. In order to see more clearly, we
define the set $J_{ab} = \{(l, r)|l, r = o, x, y\}$ to collect all the source pairs chosen by Alice and Bob in the three-intensity decoy-state protocol. Furthermore, we define

$$J_m = \{J_m = \{(l_1, r_1), \cdots , (l_m, r_m)|J_m \subset J_{ab}\}\},$$

(16) to collect all subsets $J_m$ of $J_{ab}$, where $J_m$ contains $m$ different source pairs in it. For example, $J_1 = \{\{(l_1, r_1)\}|l_1, r_1 = o, x, y\}$ which collects all subsets of $J_{ab}$ with only one source pair in each element, $J_2 = \{\{(l_1, r_1), (l_2, r_2)\}|l_1, r_1, l_2, r_2 = o, x, y; (l_1, r_1) \neq (l_2, r_2)\}$ which collects all subsets of $J_{ab}$ with two different source pairs in each element, and $J_3 = \{J_{ab}\}$ which contains the set $J_{ab}$ as its sole element. With these preparations, we can write all the relations among the ratios $\delta_{lr}$ into

$$\left| \sum_{(l, r) \in J_m} N_{lr}^o S_{lr}^o \delta_{lr}^o \right| \leq n_\delta \sqrt{\sum_{(l, r) \in J_m} N_{lr}^o S_{lr}^o},$$

(17) for all $J_m \in J_m$, $m = 1, 2, \cdots , 8$ and

$$\sum_{(l, r) \in J_{ab}} N_{lr}^o S_{lr}^o \delta_{lr}^o = 0.$$  

(18)

The last equation is deduced from the fact that

$$\sum_{(l, r) \in J_{ab}} N_{lr}^o S_{lr}^o = \sum_{(l, r) \in J_{ab}} N_{lr}^o S_{lr}^o.$$  

Specially, if we set $m = 1$, then the relations presented in Eq. (17) is just the bounds for each fluctuation ratios $\delta_{lr}$ which has been shown in Eq. (13). If we set $m = 2$, then the relations presented in Eq. (17) is just the relations between any two ratios $\delta_{lr_1}$ and $\delta_{lr_2}$ which has been shown in Eq. (16).

It should be note that there are 9 fluctuation ratios $\delta_{lr}$ in Eq. (10) for this 3-intensity protocol in $\omega$ basis. In Eq. (17) and Eq. (18), there are $\sum_{l=2}^9 C_l^9 = 2^9 - 9 - 1 = 502$ joint constraints for these 9 ratios. It is a hard work to obtain an explicit formula to estimate the lower bound of $s_{11}$ from Eq. (10) with all these constraints. In the next subsection, we will present some explicit formulas to lower bound $s_{11}$ and upper bound $\bar{s}_{11}$ with an efficient method by introducing some more generalized constraints. Though in our formulas we have not used all constraints, our formulas can give a key rate almost exactly the same with the one fully using all these constraints.

Similarly, all the relations among the fluctuation ratios $\tau_{lr}$ can be written into

$$\left| \sum_{(l, r) \in J_m} N_{lr}^X T_{lr}^X \tau_{lr}^X \right| \leq n_\tau \sqrt{\sum_{(l, r) \in J_m} N_{lr}^X T_{lr}^X},$$

(19) for all $J_m \in J_m$, $m = 1, 2, \cdots , 8$ and

$$\sum_{(l, r) \in J_{ab}} N_{lr}^X T_{lr}^X \tau_{lr}^X = 0.$$  

(20)

Specially, if we set $m = 1$, then the relations presented in Eq. (19) is just the bounds for each fluctuation ratios $\tau_{lr}^X$ which has been shown in Eq. (14).

B. Improved statistical fluctuation analysis

Practically, in order to extract the secret final key, we need to consider the statistical fluctuation caused by a finite-size key. Such an analysis is crucial to ensure the security of MDI-QKD in real setups. As concluded in previous works [25 27 31 32], comparing with the asymptotic result, the final key rate will be evidently decreased in a reasonable data-size in the situation with finite-size key, such as $N_t = 10^{12}$. So it is very important to introduce some more efficient methods to realanalys the finite-size effect. As discussed previously, in statistical analysis, the fluctuation ratios should be used, such as $\delta_{lr}$ and $\tau_{lr}$ defined in Eq (11) and Eq (12) respectively. The lower and upper bounds of these ratios can be fixed with a given security bound. Besides the bound relations for these ratios, we have shown some other relations among them without changing the security bound. In all previous works [25 27 31 32], the relations among these ratios have not been considered sufficiently. Here in this subsection, we make some improved statistical analysis with the relations presented above.

We consider the estimation of lower bound of $s_{11}$ firstly. As is defined in Eq. (10), the mean values $\bar{s}_{11}^\omega$ is the function of fluctuation ratio $\delta_{lr}^\omega$. Replacing $\bar{s}_{11}^\omega$ by its expectation values $\hat{s}_{11}^\omega$ in Eq. (15), we get a function about ratios $\delta_{lr}^\omega$

$$s_{11}^{\omega, f_a} = \min\{s_{11}^{\omega, f_a}, s_{11}^{\omega, f_b}\},$$

(21)

where

$$s_{11}^{\omega, f_a} = s_{11}^{\omega, a} + (S_{+}^{\omega, f_a} - S_{-}^{\omega, f_a})/(a_{11}^{\omega, f_a} b_{12}^{\omega, f_a}),$$

(22)

$$s_{11}^{\omega, f_b} = s_{11}^{\omega, b} + (S_{+}^{\omega, f_b} - S_{-}^{\omega, f_b})/(b_{11}^{\omega, f_b} b_{12}^{\omega, f_b}),$$

(23)

with

$$S_{+}^{\omega, f_a} = a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_b} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_b} S_{+}^{\omega, f_b},$$

$$S_{+}^{\omega, f_b} = a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_b} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_b} S_{+}^{\omega, f_b},$$

$$S_{-}^{\omega, f_a} = a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_a} b_{12}^{\omega, f_a} S_{+}^{\omega, f_b} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_a} S_{+}^{\omega, f_a} + a_{11}^{\omega, f_b} b_{12}^{\omega, f_b} S_{+}^{\omega, f_b},$$

and $s_{11}^{\omega, a}, s_{11}^{\omega, b}$ being constant factors which are defined in Eq. (13).

In order to obtain the proper estimation of the lower bound of $s_{11}^{\omega}$ from this function $s_{11}^{\omega, f}$, we need to find out the worst case under the constraints about the ratios $\delta_{lr}^\omega$. That is to say, we need minimize the function $s_{11}^{\omega, f_a}$ of variables $\delta_{lr}^\omega$ under the constraints shown in Eqs. (17-18). Actually, some constraints can be abandoned in minimizing $s_{11}^{\omega, f_a}$. Taking $s_{11}^{\omega, f_a}$ as example, we can see that the signs in front of $S_{+}^{\omega, f_a}$ and $S_{-}^{\omega, f_a}$ are different. So we can
treat the variables in $S^o_{++,+}$ and $S^o_{++,f}$ separately. That is to say, equivalently, the minimization of $s^{o,v}_{11}$ can be divided into two simple problems which are the minimization of $S^o_{++,+}$ and the maximization of $S^o_{++,f}$. In minimizing $S^o_{++,+}$, we only need consider the constraints among variables $\delta_{ox}$, $\delta_{oy}$ and $\delta_{oz}$. Similarly, in maximizing $S^o_{++,f}$, we only need consider the constraints among variables $\delta_{yy}$ and $\delta_{zo}$. These optimization problems can be solved by using the linear programming (LP) method. In Appendix C we show the improved LP method with our joint constraints for the statistical fluctuation ratios above.

In the above subsection, we introduce some relations among these fluctuation ratios by regrouping the successful events. Actually, by taking partial successful events of each group randomly, we can generalize these relations. That is to say, the relation in Eq. (17) can be generalized into

$$
\sum_{(l,r) \in J_m} \lambda_{lr}^o N_{lr}^o S_{lr}^o \delta_{lr}^o \leq n_\delta \sqrt{\sum_{(l,r) \in J_m} \lambda_{lr}^o N_{lr}^o S_{lr}^o},
$$

(24)

where $\lambda_{lr}^o \leq 1$. With these generalized relations, we can find out some explicit formulas to estimate the bounds.

Firstly, we commit ourself to derive an explicit formula to estimate the minimization of $S^o_{++,f}$. In the function $S^o_{++,f}$, there are 4 variables $\delta_{ox}$, $\delta_{oy}$, $\delta_{oz}$ and $\delta_{zo}$. In order to obtain a reasonable value, we need rewrite $S^o_{++,f}$ into its equivalent form. For convenience, we use nature numbers 1, 2, 3, 4 to indicate these 4 different subscripts $xx$, $oy$, $yo$ and $oo$ with decreasing coefficients of variables $\delta_{rr}^o$ in $S^o_{++,f}$. That is to say, if $a_1^l b_1^l S_{xx}^o \geq a_1 b_2 a_2 b_2^f S_{yy}^o \geq a_1 b_2 a_2^f b_2 b_2^o S_{yo}^o \geq (a_1^l b_2 a_2^f b_2^o) S_{oo}^o$, we use nature numbers 1, 2, 3, 4 to indicate $xx$, $oy$, $yo$ and $oo$ respectively. With these preparations, we can rewrite $S^o_{++,f}$ into the following form

$$
S^o_{++,f} = \frac{4}{j=1} \prod_{k=1}^{j} h_{j}^{(k)} \sum_{k=j}^{4} \lambda_{k}^o N_{k}^o S_{k}^o \delta_{k}^o \leq \frac{4}{j=1} I_j,
$$

(25)

where $\lambda_{j}^o = 1$, and

$$
\lambda_{k}^o = \min(1, h_{k}^{(j)} / h_{j}^{(j)}), \quad h_{k}^{(j+1)} = h_{k}^{(j)} / h_{j}^{(j)} - \lambda_{k}^o,
$$

(26)

for $j = 1, 2, 3, 4$, $k = j + 1, \cdots, 4$, with $h_{1}^{(1)} = a_1^l b_1^l N_{xx}^o, h_{2}^{(2)} = a_1 b_2 a_2^f N_{yy}^o, h_{3}^{(3)} = a_1 b_2 a_2 b_2^o S_{yo}^o, h_{4}^{(4)} = (a_1^l b_2 a_2 b_2^o) S_{oo}^o$, when $a_1^l b_1^l S_{xx}^o \geq a_1 b_2 a_2^f b_2^o S_{yy}^o \geq a_1 b_2 a_2 b_2^o S_{yy}^o \geq a_1 b_2 a_2^f b_2^o S_{oo}^o$. Furthermore, in the above equation, we always rearrange the subscript number with increasing order to make sure that $h_{k}^{(j)} N_{k}^o S_{k}^o \leq h_{k}^{(k-1)} N_{k}^o S_{k}^o$ when $k_1 < k_2$.

According to the generalized constraints presented in Eq. (24), we obtain that

$$
I_j \geq -n_\delta \prod_{k=1}^{j} h_{j}^{(k)} \sqrt{\sum_{k=j}^{4} \lambda_{k}^o N_{k}^o S_{k}^o},
$$

Then the minimum of $S^o_{++,f}$ can be estimate by using the following explicit formula

$$
S^o_{++,f} \geq -n_\delta \prod_{j=1}^{4} h_{j}^{(j)} \sqrt{\sum_{k=j}^{4} \lambda_{k}^o N_{k}^o S_{k}^o} \leq S^o_{++,f},
$$

(27)

Similarly, we can estimate the maximum of $S^o_{++,f}$ by the following explicit formula

$$
S^o_{++,f} \leq n_\delta \prod_{j=1}^{3} h_{j}^{(j)} \sqrt{\sum_{k=j}^{3} \lambda_{k}^o N_{k}^o S_{k}^o} \leq S^o_{++,f},
$$

(28)

where $\lambda_{k}^o$ and $h_{k}^{(j)}$ are defined in Eq. (20) with initial values $h_{1}^{(1)} = a_1^l b_2/N_{yy}^o, h_{2}^{(2)} = a_1 b_2^f a_2^f/N_{xx}^o, h_{3}^{(3)} = a_1 b_2 b_2^o/N_{xx}^o$, when $a_1^l b_1^l S_{xx}^o \geq a_1 b_2^f a_2^f S_{yy}^o \geq a_1 b_2 b_2^o S_{yy}^o \geq (a_1^l b_2 b_2^o) S_{oo}^o$.

In the same way, we can estimation the minimum of $S^o_{++,f}$ and the maximum of $S^o_{++,f}$ by using the following explicit formulas

$$
S^o_{++,f} = -n_\delta \prod_{j=1}^{4} h_{j}^{(j)} \sqrt{\sum_{k=j}^{4} \lambda_{k}^o N_{k}^o S_{k}^o},
$$

(29)

$$
S^o_{++,f} = n_\delta \prod_{j=1}^{3} h_{j}^{(j)} \sqrt{\sum_{k=j}^{3} \lambda_{k}^o N_{k}^o S_{k}^o},
$$

(30)

where $\lambda_{k}^o$ and $h_{k}^{(j)}$ are defined in Eq. (20) with initial values $h_{1}^{(1)} = b_1^l a_2/N_{yy}^o, h_{2}^{(2)} = b_1^l a_2^f a_2^o/N_{xx}^o, h_{3}^{(3)} = b_1^l a_2 b_2^o/N_{xx}^o$, when $b_1^l a_2 S_{yy}^o \geq b_1^l a_2^f a_2^o S_{yy}^o \geq b_1^l a_2^f b_2^o S_{yy}^o \geq (b_1^l a_2^f b_2^o) S_{oo}^o$.

Similar to the definition of $S^o_{++,f}$, in the above definition of $S^o_{++,f}$ and $S^o_{++,f}$, with Eqs. (28) and (30), we always rearrange the subscript number with increasing order to make sure that $h_{k}^{(j)} N_{k}^o S_{k}^o \leq h_{k}^{(k-1)} N_{k}^o S_{k}^o$ when $k_1 < k_2$.

With these preparations, we obtain a lower bound of $s^{o,v}_{11}$ with explicit formula as follows

$$
\hat{\omega}_{11}^{v,f} = \min(\hat{\omega}_{11}^{v,f}, \hat{\omega}_{11}^{v,f}),
$$

(31)

where

$$
\hat{\omega}_{11}^{v,f} = \hat{\omega}_{11}^{v,a} + (\hat{\omega}_{11}^{v,f} - \hat{\omega}_{11}^{v,a})/(a_1^1 b_1^1 b_1^1),
$$

$$
\hat{\omega}_{11}^{v,f} = \hat{\omega}_{11}^{v,b} + (\hat{\omega}_{11}^{v,f} - \hat{\omega}_{11}^{v,b})/(b_1^1 b_1^1 b_1^1),
$$

with $\hat{\omega}_{11}^{v,a}$ and $\hat{\omega}_{11}^{v,b}$ being defined in Eq. (22), $\hat{\omega}_{11}^{v,f}$, $\hat{\omega}_{11}^{v,f}$ and $\hat{\omega}_{11}^{v,f}$ being defined in Eq. (27), Eq. (28), Eq. (29) and Eq. (30) respectively.
Besides the lower bound $s_{o}^{f_1}$, we can obtain another lower bound of $s_{e}^{f_1}$ with explicit formula as follows

$$s_{o}^{f_2} = \frac{s_{o}^{f_1}}{1 + \frac{S_{+}^{o} - S_{-}^{o}}{a_1 b_1 a_1 b_1}},$$  \quad (32)$$

where $s_{o}^{f_1}$ is a constant factor defined by Eq. (A3) and $S_{+}^{o}, S_{-}^{o}$ can be analytically obtained with the same method for $S_{+}^{o}, S_{-}^{o}$. Explicitly, we have

$$S_{+}^{o} = -n_0 \sum_{j=1}^{4} \prod_{k=1}^{j} h_j^{(j)} \sum_{k=j}^{4} \lambda_k^{(j)} N_k^{o} S_0^{o},$$  \quad (33)$$

where $\lambda_k^{(j)}$ and $h_k^{(j)}$ are defined in Eq. (26) with initial values $h_1^{(1)} = g_{xx}/N^{o}_{xx}, h_2^{(1)} = g_{yy}/N^{o}_{yy}, h_3^{(1)} = g_{yx}/N^{o}_{yx}, h_4^{(1)} = g_{oz}/N^{o}_{oz}$, when $g_{xx}S_{0}^{xx} \geq g_{yy}S_{0}^{yy} \geq g_{yx}S_{0}^{yx} \geq g_{oz}S_{0}^{oz}$.

$$S_{-}^{o} = n_0 \sum_{j=1}^{4} \prod_{k=1}^{j} h_j^{(j)} \sum_{k=j}^{4} \lambda_k^{(j)} N_k^{o} S_0^{o},$$  \quad (34)$$

where $\lambda_k^{(j)}$ and $h_k^{(j)}$ are defined in Eq. (26) with initial values $h_1^{(1)} = g_{yy}/N^{o}_{yy}, h_2^{(1)} = g_{yx}/N^{o}_{yx}, h_3^{(1)} = g_{ox}/N^{o}_{ox}, h_4^{(1)} = g_{zo}/N^{o}_{zo}$, when $g_{yx}S_{0}^{yx} \geq g_{ox}S_{0}^{ox} \geq g_{zo}S_{0}^{zo} \geq g_{oz}S_{0}^{oz}$. Similar to the definition of $S_{+}^{o}, S_{-}^{o}$, in the above definitions of $S_{+}^{o}, S_{-}^{o}$ and $S_{+}^{o}, S_{-}^{o}$ with Eqs. (33,34), we always rearrange the subscript number with increasing order to make sure that $h_k^{(j)}N_k^{o}S_0^{o} \geq h_k^{(j)}N_k^{o}S_0^{o}$ when $k_1 < k_2$.

In Appendix A, we shall first reduce those 502 constraints to only 11 or even less. Based on this, we can estimate the lower bound of $s_{e}^{f_1}$ and the upper bound of $e_{e}^{f_1}$ efficiently through linear programming.

IV. NUMERICAL SIMULATION

In this section, we will present some numerical simulations to compare the results obtained with the improved methods and the traditional methods. Without losing the generality, we focus on the symmetric case where the two channel transmissions from Alice to UTP and from Bob to UTP are equal. We also assume that the UTP’s detectors are identical, i.e., they have the same dark count rates and detection efficiencies, and their detection efficiencies do not depend on the incoming signals. We shall estimate what values would be probably observed for the yields and error yields in the normal cases by the linear models as in []. For fair comparison, we use the same experimental parameters used in Ref. [36] for our numerical simulation, which are mostly from the long-distance QKD experiment reported in [35]. The values of these parameters are listed in Table [3]. With this, the yields $S_{0}^{xy}$ and error yields $E_{0}^{xy}$ can be calculated [35] with coherent states with intensities $\mu_x, \mu_y$. The density matrix of the coherent state with intensity $\mu$ can be written into $\rho = \sum_k \frac{c_k^{*}}{\sqrt{\mu}} |k\rangle \langle k|$. Using these values, we can estimate the lower bounds of $s_{e}^{f_1}$ and the upper bounds of $e_{e}^{f_1}$ with different methods presented in the above sections. With these preparations, we can calculate the final secret key rate with the following formula [14]

$$R = a'_{1} b'_{1} a_{1}^{Z} [1 - H(e_{1}^{X})] - f_{e}S_{0}^{Z}H(E_{0}^{Z}),$$  \quad (39)$$

where $S_{0}^{Z}$ and $E_{0}^{Z}$ denote, respectively, the yield and error rate in the $Z$-basis when both Alice and Bob use $p_{y_{a}}$ and $p_{y_{b}}$; $f_{e}$ is the efficiency factor of the error correction
method used; $s_{11}^Y$ and $e_{11}^X$ are the yield and error rate when both Alice and Bob send single-photon states.

To make a fair comparison, we need to find out the full parameter optimizations for different methods [36]. Here we also use the well-known local search algorithm. In this algorithm, we need to optimize the one-variable nonlinear function in each step for the local search.

We consider the three-intensity protocol in the case of data-size $N_t = 10^{12}$. The optimal parameters and the practical key rate per pulse for the distance 50km (standard fiber), with the statistical fluctuations, are shown in Table 1. The result presented in Ref. [36] is shown in the 2nd column. In the 3rd column, we show the optimal parameters after a full parameter optimization by using the traditional analytical method with Eq.(B9) and Eq.(B10). The 4th column is the optimal parameters obtained with explicit formulas Eq.(35) and Eq.(36). Comparing with the result given by Xu et al[36], our improved result raises the key rate $R$ by 97%.

| Parameter | Ref. [36] | Traditional | Improved |
|-----------|-----------|-------------|----------|
| $\rho_y$  | 0.25      | 0.396       | 0.401    |
| $\rho_x$  | 0.05      | 0.056       | 0.055    |
| $\rho_o$  | $1.0 \times 10^{-6}$ | 0       | 0        |
| $p_y$     | 0.58      | 0.646       | 0.681    |
| $p_x$     | 0.30      | 0.256       | 0.243    |
| $pX|y$    | 0.03      | 0.024       | 0.013    |
| $pX|x$    | 0.71      | 0.737       | 0.709    |
| $pX|o$    | 0.83      | 1.000       | 1.000    |
| $R$       | $1.68 \times 10^{-6}$ | $2.59 \times 10^{-6}$ | $3.31 \times 10^{-6}$ |

TABLE II: Comparison of parameters at 100km (standard fiber) for 3-intensity protocol with statistical fluctuation analysis in the case of data-size $N_t = 10^{12}$. The 2nd column is the optimal parameters after a full parameter optimization with explicit formulas Eq.(35) and Eq.(36). The 3rd column is the optimal parameters obtained with explicit formulas Eq.(35) and Eq.(36). Comparing with the result given by Xu et al[36], our improved result raises the key rate $R$ by 97%.

| Parameter | Traditional | Improved I | Improved II |
|-----------|-------------|------------|-------------|
| $\rho_y$  | 0.269       | 0.275      | 0.275       |
| $\rho_x$  | 0.067       | 0.068      | 0.068       |
| $p_y$     | 0.336       | 0.404      | 0.404       |
| $p_x$     | 0.477       | 0.447      | 0.447       |
| $pX|y$    | 0.132       | 0.084      | 0.084       |
| $pX|x$    | 0.742       | 0.719      | 0.720       |
| $R$       | $1.00 \times 10^{-8}$ | $2.46 \times 10^{-8}$ | $2.46 \times 10^{-8}$ |

TABLE III: Comparison of parameters at 100km (standard fiber) for 3-intensity protocol with statistical fluctuation analysis in the case of data-size $N_t = 10^{12}$. The 2nd column is the optimal parameters after a full parameter optimization with explicit formulas Eq.(35) and Eq.(36). The 3rd column is the optimal parameters obtained with explicit formulas Eq.(35) and Eq.(36). The 4th column is the optimal parameters obtained by our improved linear programming method with our constraints shown in appendix C. We can see that our new full parameter optimization can improve the key rate $R$ by 146%. Our improved results by formulas are almost the same with our LP method which has fully used all constraints of fluctuation ratios.

V. CONCLUSION

In real set-ups of MDL-QKD, we have to consider the effect of statistical fluctuations caused by the finite-size key. In the statistical analysis, we need to introduce the fluctuation ratios. With import the relations among
the following formula to estimate the lower bound of these fluctuation ratios, we obtain the improved statistical analysis with explicit formulas. According to the numerical simulations. The results obtained with our improved methods are significantly better than the results obtained with the traditional methods. In our study, we have taken the same intensities in both bases. The result can be further improved by taking different intensity values in different bases and taking the decoy-state method in only one basis as pointed out in \[32\]. This will be reported elsewhere.

Appendix A: Explicit formulas in the asymptotic case

In Ref. \[20\], Wang presented the first explicit formula for the practical decoy-state implementation through using part of the above constraints. Explicitly, we can use the following formula to estimate the lower bound of \(\hat{s}_{11}^\omega\),

\[
\hat{s}_{11}^\omega = \min\{\hat{s}_{11}^{\omega,a}, \hat{s}_{11}^{\omega,b}\},
\]

where

\[
\hat{s}_{11}^{\omega,a} = \frac{\hat{S}_{+} - \hat{S}_{-}^{\omega,a}}{a_1 b'_1 b_{12}}, \quad \hat{s}_{11}^{\omega,b} = \frac{\hat{S}_{+}^{\omega,b} - \hat{S}_{-}^{\omega,b}}{b_1 b'_1 a_{12}},
\]

with

\[
\hat{S}_{+} = a_1'b'_2 S_{xx}^\omega + a_1 b_2 a_0' S_{yy}^\omega + a_1 b_2 b_0' S_{00}^\omega + (a_1'b'_2 a_0 - a_1 b_2 a_0') S_{00}^\omega,
\]

\[
\hat{S}_{-} = a_1 b_2 S_{00}^\omega + a_1'b_2 a_0' S_{xx}^\omega + a_1 b_2 b_0' S_{xy}^\omega,
\]

\[
\hat{S}_{+}^{\omega,b} = b_1 a_2 S_{xx}^\omega + b_1 a_2 a_0' S_{yy}^\omega + b_1 a_2 b_0' S_{00}^\omega,
\]

\[
\hat{S}_{-}^{\omega,b} = b_1 a_2 S_{00}^\omega + b_1 a_2 a_0' S_{xy}^\omega + b_1 a_2 b_0' S_{xx}^\omega,
\]

and \(\hat{a}_{12} = a_1 a'_2 - a_1' a_2, \hat{b}_{12} = b_1 b'_2 - b'_1 b_2\). In the calculation, we have used the fact that the values \(S_{0r}^\omega\) and \(S_{r0}^\omega\) are equal to the observable \(S_{0r}\) and \(S_{r0}\) respectively in the asymptotic case.

Besides this formula, we also present some other methods to estimate the lower bounds of \(s_{11}^\omega\) for this three-intensity protocol \[31\]. Explicitly, the lower bound of \(s_{11}^\omega\) can be estimated by the following explicit formula

\[
\hat{s}_{11}^{\omega,2} = \frac{\hat{S}_{+}^{\omega,2} - \hat{S}_{-}^{\omega,2}}{a_1 b_1 a_{12} b_{12}},
\]

where

\[
\hat{S}_{+}^{\omega,2} = g_{xx} S_{xx}^{\omega} + g_{xy} S_{xy}^\omega + g_{0y} S_{yx}^\omega + g_{00} S_{00}^\omega,
\]

\[
\hat{S}_{-}^{\omega,2} = g_{xy} S_{xy}^\omega + g_{yx} S_{yx}^\omega + g_{0x} S_{ox}^\omega + g_{0y} S_{oy}^\omega,
\]

with

\[
g_{xx} = a_1 a'_2 b_1 b'_2 - a_1' a_2 b'_1 b_2, \quad g_{xy} = b_1 b_2 \hat{a}_{12},
\]

\[
g_{yx} = a_1 a'_2 \hat{b}_{12}, \quad g_{0y} = a_0 g_{xy}, \quad g_{0x} = b_0 g_{yx},
\]

\[
g_{00} = a_0 b_0 g_{xx} - a_0 b'_2 g_{xy} - a'_0 b_2 g_{yx} = a_0 b_2 \hat{a}_{12} \hat{b}_{01} + b_0 a_1 \hat{a}_{02} \hat{b}_{12},
\]

\[
g_{0x} = a_0 g_{xx} - a_0 g_{yx} = a_0 \hat{a}_{12} \hat{b}_{12} + a_0 b'_1 b_2 \hat{a}_{12},
\]

\[
g_{0y} = b_0 g_{xx} - b_0 g_{xy} = b_0 a_1' b_2 b_2 + b_2 \hat{a}_{1} \hat{b}_{01},
\]

and \(\hat{a}_{02} = a_0 a'_2 - a_0' a_2, \hat{a}_{12} = a_1 a'_2 - a_1' a_2, \hat{b}_{01} = b_0 b'_1 - b'_0 b_1, \hat{b}_{12} = b_1 b'_2 - b'_1 b_2\). With the condition presented in Eq. \[3\], we can easily prove that \(f_{lr} \geq 0\) for all \(l, r = 0, x, y\).

As presented in Ref. \[31\], we know that the lower bound \(\hat{s}_{11}^{\omega,2}\) is always better than \(\hat{s}_{11}^{\omega,2}\) in the asymptotic case. Whereas, in the non-asymptotic case, we need re-analysis the relation between them. Actually, the priority of \(\hat{s}_{11}^{\omega,2}\) will disappear in the case of reasonable data-size for a long enough key distribution distance.

Besides the lower bound of \(s_{11}^\omega\), we can estimate the upper bound of \(e_{11}^X\) with the following explicit formula

\[
\bar{e}_{11}^X = (\bar{T}_+^X - \bar{T}_-^X) / (a_1 b_1 \hat{s}_{11}^X),
\]

where

\[
\bar{T}_+^X = T_{xx}^X + a_0 b_0 T_{00}^X, \quad \bar{T}_-^X = a_0 T_{xx}^X + b_0 T_{00}^X,
\]

and \(\bar{s}_{11}^X\) is the lower bound of \(s_{11}\) in X-basis which can be estimated by using Eq. \[A3\].
Appendix B: Explicit formulas in the non-asymptotic case

Consider yields \( \hat{S}_l^\omega \) and error yields \( \hat{T}_l^X \) with the observed values \( S_l^\omega \) and \( T_l^X \) respectively by introducing the fluctuation ratios \( \delta_l^\omega \) and \( \tau_l^X \),

\[
\begin{align*}
\hat{S}_l^\omega &= S_l^\omega (1 + \delta_l^\omega), \\
\hat{T}_l^X &= T_l^X (1 + \tau_l^X),
\end{align*}
\]

(B1)

(B2)

for all \( l, r = o, x, y \). If we use the standard error analysis method, the fluctuation ratios \( \delta_l^\omega \) and \( \tau_l^X \) are bounded by

\[
|\delta_l^\omega| \leq \frac{n_{\delta}}{\sqrt{N_l^\omega S_l^\omega}} \triangleq \tilde{\delta}_l^\omega, \quad (B3)
\]

\[
|\tau_l^X| \leq \frac{n_\tau}{\sqrt{N_l^X T_l^X}} \triangleq \tilde{\tau}_l^X, \quad (B4)
\]

respectively, where \( N_l^\omega \) is the number of pulses sent out by Alice and Bob when they use sources \( \rho_{lA} \) and \( \rho_{lr} \) in the \( \omega \) basis respectively, \( n_{\delta} \) and \( n_\tau \) are the number of standard deviations one chooses for statistical fluctuation analysis with the given security bound. With these notations, we know that \( N_l^\omega S_l^\omega \) is the number of successful event announced by UTP when Alice and Bob use sources \( \rho_{lA} \) and \( \rho_{rb} \) in the \( \omega \) basis, and \( N_l^X T_l^X \) is the corresponding error count in the \( X \) basis.

In order to get a reasonable lower bound of \( s_{11}^\omega \) in the non-asymptotic case, we reconsider the explicit formulas Eq. (A11) firstly. As discussed above, in the non-asymptotic case, the observed values are different from its mean values. So we need to replace \( S_l^\omega \) by its expectation values \( \hat{S}_l^\omega \) defined in Eq. (11). Then the formula turns into a function of the fluctuation ratios \( \delta_l^\omega \).

In security proof, we assume that Eve can do anything except to violate rules of the nature. In order to obtain a reasonable estimation of the lower bound of \( s_{11}^\omega \), we should find out the worst case under the constraints about \( \delta_l^\omega \) given by Eq. (13). Considering the restrictions in Eq. (13), we know that the fluctuation ratios \( \delta_l^\omega \) are independent from each other. So the worst case can be obtained by taking the worst value for each terms. Explicitly, we have

\[
s_{11}^{\omega,1} = \min(s_{11}^{\omega,a}, s_{11}^{\omega,b}), \quad (B5)
\]

where

\[
s_{11}^{\omega,a} = \frac{S_{11}^{\omega,a} - S_{11}^a}{a_1 b_1 a_2 b_2}, \quad s_{11}^{\omega,b} = \frac{S_{11}^{\omega,b} - S_{11}^b}{b_1 a_1 b_2 a_2}, \quad (B6)
\]

with

\[
S_{11}^{\omega,a} = a_1 b_1^2 S_{11}^{x,x} + a_1 b_2 a_1^2 S_{11}^{y,y} + a_1 b_2^2 S_{11}^{z,z} + (a_1^2 b_1 b_2 - a_1 b_2 a_1 b_2) S_{11}^{\omega,\omega},
\]

\[
S_{11}^{\omega,b} = a_1 b_1 a_2^2 S_{11}^{x,x} + a_2 b_1^2 S_{11}^{y,y} + a_2 b_1 a_2 b_2 S_{11}^{z,z} + (a_1 a_2 b_1 b_2 - a_1 b_2 a_1 b_2) S_{11}^{\omega,\omega},
\]

\[
S_{11}^{\omega,a} = b_1 a_1^2 S_{11}^{x,x} + b_1 a_2 a_1 b_2 S_{11}^{y,y} + b_1 a_2 b_1 S_{11}^{z,z} + (b_1^2 a_1 b_2 a_2 - b_1 a_2 b_1 a_2) S_{11}^{\omega,\omega},
\]

\[
S_{11}^{\omega,b} = b_1 a_2 a_1 b_2 S_{11}^{x,x} + b_1 a_2 b_1 S_{11}^{y,y} + b_1 a_2 b_1 b_2 S_{11}^{z,z} + (b_1^2 a_2 b_1 a_2 - b_1 a_2 b_1 b_2) S_{11}^{\omega,\omega},
\]

and

\[
S_{11}^\omega = S_{11}^\omega (1 - \tilde{\delta}_l^\omega), \quad \tilde{S}_l^\omega = S_{11}^\omega (1 + \tilde{\delta}_l^\omega). \quad (B7)
\]

In the above equations, \( \tilde{\delta}_l^\omega \) is the upper bound of the fluctuation ratio \( \delta_l^\omega \) that is given by Eq. (13).

Besides this lower bound, we can also obtain the other one from Eq. (A13) by the same way. Explicitly, we have

\[
\tilde{S}_1^{\omega,2} = \frac{S_1^{\omega,2} - S_1^{\omega,2}}{a_1 b_1 a_2 b_2}, \quad (B8)
\]

where

\[
S_{11}^{\omega,2} = g_{xx} S_{11}^{x,x} + g_{yy} S_{11}^{y,y} + g_{zz} S_{11}^{z,z} + g_{\omega,\omega} S_{11}^{\omega,\omega},
\]

\[
S_{11}^{\omega,2} = g_{yy} S_{11}^{y,y} + g_{zz} S_{11}^{z,z} + g_{\omega,\omega} S_{11}^{\omega,\omega},
\]

with \( g_{\omega,\omega} \) being defined in the above subsection, \( \tilde{S}_1^\omega \) and \( \tilde{S}_1^{\omega,2} \) being given in Eq. (B7).

In Ref. [31], we have shown that the lower bound \( \tilde{S}_1^{\omega,1} \) is always better than \( \tilde{S}_1^{\omega,1} \) with the same experimental parameters in the asymptotic case. However, in the non-asymptotic case, the lower bound \( \tilde{S}_1^{\omega,1} \) can be better than \( \tilde{S}_1^{\omega,2} \) in the case of reasonable data-size for a long enough key distribution distance. So we should choose the bigger one. Explicitly, we define the new lower bound of \( s_{11}^\omega \) for this 3-intensity protocol as follows

\[
s_{11}^{\omega,1} = \max(s_{11}^{\omega,1}, s_{11}^{\omega,2}), \quad (B9)
\]

where \( s_{11}^{\omega,1} \) and \( s_{11}^{\omega,2} \) are defined in Eq. (B5) and Eq. (B8) respectively.

Similarly, in this 3-intensity decoy-state MDI-QKD protocol, we can use the following explicit formula to estimate the upper bound of \( \epsilon_{11}^X \)

\[
\epsilon_{11}^X = (T_{+}^X - T_{-}^X) / (a_1 b_1 \tilde{S}_1^{X}), \quad (B10)
\]

where

\[
\tilde{T}_{+}^X = \tilde{T}_{+}^X + a_0 b_0 \tilde{T}_{+}^X, \quad \tilde{T}_{-}^X = a_0 \tilde{T}_{-}^X + b_0 \tilde{T}_{-}^X \quad (B11)
\]

with \( \tilde{S}_1^{X} \) being the lower bound of \( s_{11} \) in \( X \)-basis which can be estimated by using Eq. (13) and

\[
\tilde{T}_{+}^X = T_{+}^X (1 - \tilde{T}_{-}^X), \quad \tilde{T}_{-}^X = T_{-}^X (1 + \tilde{T}_{-}^X) \quad (B12)
\]

In the above equations, \( \tilde{T}_{+}^X \) is the upper bound of the fluctuation ratio \( \tau_l^X \) that has been defined in Eq. (B4).
Appendix C: Improved results with linear programming

As was shown in [30], the existing linear programming (LP) method with the worst-case treatment [25] will only produce a very limited key rate and secure distance. It has a better performance when full optimization is taken. Here we consider both full optimization and our joint constraints. As shown in previously, the estimations of the lower bound of $s_{11}^+$ and the upper bound of $e_{11}^-$ can be obtained by solving some linear programming problems. As discussed in subsection 11A these are 502 constraints about ratios $\delta_{\omega, x}$. Though we can solve this problem with LP method directly, but it will spend too much time. To make it more efficiently, we shall first reduce those 502 constraints to only 11 or even fewer equivalent constraints.

Firstly, we consider the minimization of $S_{+}^{\omega, f_0}$ which is defined in Eq. (22). The function $S_{+}^{\omega, f_0}$ only contains the variables $\delta_{\omega, x}$, $\delta_{\omega, y}$, $\delta_{\omega, o}$ and $\delta_{\omega, oo}$. In order to minimize $S_{+}^{\omega, f_0}$, we can solve the LP problem with minimizing the objective function $S_{+}^{\omega, f_0}$ under the constraints presented in Eq. (17) with $J_m \in J_+^{\omega}$, where $J_+^{\omega} = \{ (m, r_m) \} | J_m \subset \{(l_x, r_x), (l_y, r_y), (l_o, r_o) \}$.

In this LP problem, there are only 11 constraints.

Similarly, the minimum value of $S_{+}^{\omega, f_0}$ can be obtained by minimizing the objective function $S_{+}^{\omega, f_0}$ under the constraints in Eq. (17) with $J_m \in J_+^{o}$. The maximum values of $S_{+}^{\omega, f_0}$ and $S_{+}^{\omega, f_0}$ can be obtained by maximizing $S_{+}^{\omega, f_0}$ and $S_{+}^{\omega, f_0}$ under the constraints presented in Eq. (17) with $J_m \in J_+^{\omega}$, respectively, where $J_+^{\omega} = \{ (m, r_m) \} | J_m \subset \{(l_x, r_x), (l_y, r_y), (l_o, r_o) \}$. There are only 4 constraints in these two LP problems. With these solutions, taking the maximum value of $S_{+}^{\omega, f_0}$ and the minimum value of $S_{+}^{\omega, f_0}$ into Eq. (22) and taking the maximum value of $S_{+}^{\omega, f_0}$ and the minimum value of $S_{+}^{\omega, f_0}$ into Eq. (23), we obtain the first estimation of the lower bound of $s_{11}^+$ with Eq. (21).

Besides the above estimation, we can find out another lower bound of $s_{11}^+$ corresponding to the explicit formula given by Eq. (22). In this case, we need minimize $S_{+}^{\omega, f_2}$ under the constraints shown in Eq. (17) with $J_m \in J_+^{\omega}$, and maximize $S_{+}^{\omega, f_2}$ under the constraints in Eq. (17) with $J_m \in J_+^{\omega}$, where $J_+^{\omega} = \{ (m, r_m) \} | J_m \subset \{(l_x, r_x), (l_y, r_y), (l_o, r_o) \}$.

Finally, in order to upper bound $e_{11}^-$, we need maximize $T_{-}^{x}$ under the constraints shown in Eq. (19) with $J_m \in J_+^{\omega}$, and minimize $S_{-}^{\omega, f_2}$ under the constraints shown in Eq. (19) with $J_m \in J_+^{\omega}$, where $J_+^{\omega} = \{ (m, r_m) \} | J_m \subset \{(l_x, r_x), (l_o, r_o) \}$ and $J_+^{\omega} = \{ (m, r_m) \} | J_m \subset \{(l_o, r_o) \}$. In these two LP problems, there is only one joint constraint.

[1] C.H. Bennett and G. Brassard, in Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175-179.

[2] N. Gisin, G. Ribordy, W. Tittel, et al., Rev. Mod. Phys. 74, 145 (2002); N. Gisin and R. Thew, Nature Photonics, 1, 165 (2006); M. Dusek, N. Lütkenhaus, M. Hendrych, in Progress in Optics XVII, edited by E. Wolf (Elsevier, 2006); V. Scarani, H. Bechmann-Pasquon, N.J. Cerf, et al., Rev. Mod. Phys. 81, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, European Physical Journal D, 41, 599 (2007), which appeared in the arXiv as quant-ph/0107017; D. Gottesman, H.K. Lo, N. Lütkenhaus, et al., Quantum Inf. Comput. 4, 325 (2004).

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

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

[6] X.-B. Wang, Phys. Rev. A 72, 012322 (2005).

[7] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94, 230504 (2005); X. Ma, B. Qi, Y. Zhao, et al., Phys. Rev. A 72, 012326 (2005).

[8] Y. Adachi, T. Yamamoto, M. Koashi, et al., Phys. Rev. Lett. 99, 180503 (2007).

[9] M. Hayashi, Phys. Rev. A 74, 022307 (2006); Ibid 76, 012329 (2007).

[10] D. Rosenberg, J.W. Harrington, P.R. Rice, et al., Phys. Rev. Lett. 98, 010503 (2007); T. Schmitt-Manderbach, H. Weier, M. Kürst, et al., Phys. Rev. Lett. 98, 010504 (2007); C.-Z. Peng, J. Zhang, D. Yang, et al. Phys. Rev. Lett. 98, 010505 (2007); Z.-L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. 90, 011118 (2007); Y. Zhao, B. Qi, X. Ma, et al., Phys. Rev. Lett. 96, 070502 (2006); Y. Zhao, B. Qi, X. Ma, et al., in Proceedings of IEEE International Symposium on Information Theory, Seattle (IEEE, New York, 2006), pp. 2094–2098.

[11] X.-B. Wang, C.-Z. Peng, J. Zhang, et al. Phys. Rev. A 77, 042311 (2008); J.-Z. Hu and X.-B. Wang, Phys. Rev. A 82, 012331(2010).

[12] X.-B. Wang, T. Hiroshima, A. Tomita, et al., Physics Reports 448, 1(2007).

[13] X.-B. Wang, L. Yang, C.-Z. Peng, et al., New J. Phys. 11, 075006 (2009).

[14] G. Brassard, N. Lütkenhaus, T. Mor, et al., Phys. Rev. Lett. 85, 1330 (2000); N. Lütkenhaus, Phys. Rev. A 61, 052304 (2000); N. Lütkenhaus and M. Jähne, New J. Phys. 4, 44 (2002).

[15] B. Huttner, N. Imoto, N. Gisin, et al., Phys. Rev. A 51, 1863 (1995); H.P. Yuen, Quantum Semiclass. Opt. 8, 939 (1996).

[16] L. Lydersen, V. Makarov, and J. Skaar, Nature Photonics, 4, 868(2010); I. Gerhardt, L. Mai, A. Lamata-Linares, et al., Nature Comm. 2, 349 (2011).

[17] D. Mayers and A.C.-C. Yao, in Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS98) (IEEE Computer Society, Washington, DC, 1998), p. 503; A. Acín, N. Brunner, N. Gisin, et al., Phys. Rev. Lett. 98, 230501 (2007); V. Scarani, and R. Ren-
[18] S.L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett., **108**, 130503 (2012), K. Tamaki, H.-K. Lo, C.-H. F. Fung, et al., Phys. Rev. A, **85**, 042307 (2012).

[20] X.-B. Wang, Phys. Rev. A **87**, 012320 (2013).

[21] Phys. Rev. A 72, 049908 (2013)(Erratum of Ref.[20]).

[22] A. Rubenok, J. A. Slater, P. Chan, et al., 1304.2463v1.

[23] P. Chan, J. A. Slater, I. Lucio-Martinez, et al., arXiv:1204.0738v1.

[24] Y. Liu, T.-Y. Chen, L.-J. Wang, et al., arXiv:1209.6178v1.

[25] X. Ma, C.-H. Fred Fung, and M. Razavi, Phys. Rev. A **86**, 052305 (2012).

[26] S.-H. Sun, M. Gao, C.-Y. Li, et al., Phys. Rev. A **87**, 052329 (2013).

[27] S.-H. Sun, M. Gao, C.-Y. Li, et al., Phys. Rev. Phys. Rev. A **88**, 019905 (2013) (Erratum of Ref.[20]).

[28] Q. Wang and X.-B. Wang, Phys. Rev. A, **88**, 052332 (2013).

[29] F. Xu, M. Curty, B. Qi, et al., Appl. Phys. Lett. 103, 061101 (2013).

[30] M. Curty, F. Xu, W. Cui, et al., [arXiv:1307.1081v1].

[31] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Phys. Rev. A **88**, 062339 (2013).

[32] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, arXiv: 1309.0471v1.

[33] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, arXiv: 1309.5886v1.

[34] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Phys. Rev. A **89**, 052325 (2014).

[35] Q. Wang, and X.-B. Wang, *Scientific Reports*, 4, 4612(2014).

[36] F. Xu, H. Xu, and H.-K. Lo, Phys. Rev. A **89**, 052333 (2014).

[37] R.H. Byrd, J.C. Gilbert, and J. Nocedal, Mathematical Programming, 89(1), 149-185 (2000). R.A. Waltz, J.L. Morales, J. Nocedal, and D. Orban, Mathematical Programming, 107(3), 391-408 (2006).

[38] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, et al., Nat. Phys. 3, 481 (2007).