A general model on the simulation of the measurement-device independent quantum key distribution

Qin Wang\textsuperscript{1} and Xiang-Bin Wang\textsuperscript{2,3,*}

\textsuperscript{1}Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

\textsuperscript{2}Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China and

\textsuperscript{3}Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan, China

Abstract

PACS number(s): 42.50.Ct, 78.67.Hc, 78.47.D-

We present a general model on the simulation of the measurement-device independent quantum key distribution (MDI-QKD). It can be used to predict experimental observations of a MDI-QKD with linear channel loss, simulating corresponding values for the gains, the error rates in different basis, and also the final key rates. Our model can be applicable to the MDI-QKDs with whatever convex source states or using whatever coding schemes. Therefore, it is useful in characterizing and evaluating the performance of any MDI-QKD protocols, making it a valuable tool in studying the quantum key distributions.

\textsuperscript{*}Electronic address: xbwang@mail.tsinghua.edu.cn
I. INTRODUCTION

There has been a long history between the attacks and the anti-attacks in the development of quantum key distributions (QKD) since the idea of BB84 (Bennett-Brassard 1984) protocol was put forward, due to the conflictions between the ”in-principle” unconditional security and realistic implementations. Till today, there have been many different proposals for the secure QKD with realistic setups, such as the decoy-state method [3–14] which can rescue the QKD with imperfect single-photon sources [15, 16], while the device-independent quantum key distribution [17, 18] and the recently proposed measurement-device independent quantum key distribution (MDI-QKD) [19, 20] can further relieve the QKD even when the detectors are controlled by the eavesdropper [21]. Most interestingly, the MDI-QKD is not only immune to any detector attacks, but also able to generate a significant key rate with existing technologies. Moreover, its security can still be maintained with imperfect single-photon sources [19, 22–27], and the effects of coding errors have also been studied [23, 28].

In developing practical QKDs, one important question is how to evaluate the performance of a proposal before really implementing it, since it is not realistic to experimentally test everything. Therefore, it is crucially important to make a thorough theoretical study and numerical simulation to predict the experimental results. In principle, it allows to use different kinds of sources in a decoy state MDI-QKD [22, 23]. Before experimentally testing all of them, one can choose to give a theoretical comparison with a reasonable model. In traditional decoy state methods [4–6], the models for calculation are relatively simple. However, for MDI-QKDs, it is not a simple job except for the special case of using weak coherent states. So far, there have been proposals with different sources, e.g., the heralded single-photon source (HSPS) etc [8, 9, 22]. And it has been shown that such a source can promise a longer secure distance than the weak coherent state. Nevertheless, it is unknown whether there are other sources which can present even better performance. Therefore, a general model on simulating the performance of arbitrary source states will be highly desirable. Here in this manuscript we solve the problem.

For simplicity, we assume a linear lossy channel in our model. Note that the security does not depend on the condition of linear loss at all. We only use this model to predict: what values the gains and error rates would possibly be observed if one did the experiment in the
FIG. 1: (Color online) A schematic of the experimental setup for the collective measurements at the UTP. BS: beam-splitter; PBS: polarization beam-splitter; D1 - D4: single-photon detector; 1, 2: input port for photons.

normal case when there is no eavesdropper. Given these values, one can then calculate the low bound of the yield and the upper bound of the phase flip-error rates for single-photon pairs. The major goal here is to simulate the values of gains and error rates of different states in normal situations. Of course, they can be replaced with the observed values in real implementations.

The paper is arranged as follows: In Sec. II we present the general model for the gains and error rates in a MDI-QKD, describing the detailed calculation processes. In Sec. III we proceed corresponding numerical simulations, comparing the different behaviors of MDI-QKDs when using different source states. Finally, discussions and summaries are given out in Sec. IV.
II. THE GENERAL MODEL ON MDI-QKD

A. Setups and definitions

Consider the schematic setup in Fig. 1 [19], there are three parties, the users-Alice and Bob, and the un-trusted third party (UTP)-Charlie. Alice and Bob send their polarized photon pulses to the UTP who will take collective measurement on the pulse-pairs. The collective measurement results at the UTP determine the successful events. They are two-fold click of detectors (1,4), (2,3), (1,2) or (3,4). The gain of any (two-pulse) source is determined by the number of successful events from the source. There are 4 detectors at the UTP, we assume each of them has the same dark count rate $d$, and the same detection efficiency $\xi$.

In such a case, we can simplify our model by attributing the limited detection efficiency to the channel loss. Say, if the actual channel transmittance from Alice to Charlie is $\eta_1$, we shall assume perfect detection efficiency for Charlie’s detectors with channel transmittance of $\eta_1\xi$. Each detector will detect one of the 4 different modes, say $a_H^+, a_V^+, b_H^+, b_V^+$ in creation operator. For simplicity, we denote them by $c_i^+$, i.e., $c_1^+ = a_H^+, c_2^+ = a_V^+, c_3^+ = b_H^+, c_4^+ = b_V^+$. In such a way, detector $D_i$ corresponds to mode $i$ exactly. To calculate the gains that would-be observed for different source states in the linear lossy channel, we need to model the probabilities of different successful events conditional on different states. Let’s first postulate some definitions before further study.

Definition 1: event $(i, j)$. We define event $(i, j)$ as the event that both detector $i$ and detector $j$ click while other detectors do not click. Obviously, each $i, j$ must be from numbers $\{1, 2, 3, 4\}$ and $i \neq j$. For simplicity, we request $i < j$ throughout this paper.

Definition 2: Output states and conditional probabilities of each events: notations $\rho_{out}$: the output state of the beam-splitter. $|l_i, l_j\rangle = |l_i l_j\rangle$: the beam-splitter’s specific output state of $l_i$ photon in mode $i$, $l_j$ photon in mode $j$, and no photon in any other mode. Explicitly, $|l_i l_j\rangle = \frac{1}{\sqrt{l_i!l_j!}} c_i^{l_i} c_j^{l_j} |0\rangle$. $P(ij|l_i, l_j)$ and $P(ij|\rho_{out})$: the probability that event $(i, j)$ happens conditional on that the beam-splitter’s output state is $|l_i l_j\rangle$ and $\rho_{out}$, respectively. Hereafter, we omit the comma between $l_i$ and $l_j$, i.e., we use $|l_i l_j\rangle$ for $|l_i, l_j\rangle$, and $P(ij|l_i l_j)$ for $P(ij|l_i, l_j)$.

Definition 3: Events’ probability conditional on the beam-splitter’s input state: $p_{ij}^{\alpha\beta}(k_1, k_2) = p_{ij}^{\alpha\beta}(k_1 k_2)$. We denote $p_{ij}^{\alpha\beta}(k_1, k_2)$ as the probability of event $(i, j)$ conditional on that there are $k_1$ photons of polarization $\alpha$ for mode $a$ and $k_2$ photons of polarization $\beta$. 


for mode \( b \) as the input state of the beam-splitter. Hereafter, we omit the comma between \( k_1 \) and \( k_2 \). \( \alpha \) or \( \beta \) indicate the photon polarization. Explicitly, \( \alpha \) or \( \beta \) can be \( H, V, +, − \) for polarizations of horizontal, vertical, \( \pi/4 \) and \( 3\pi/4 \), respectively. To indicate the corresponding polarization state, we simply put each of these symbols inside a ket.

Definition 4: Events’ probability conditional on the two-pulse state of Alice and Bob’s source: \( q_{ij}^{\alpha\beta}(\rho_A \otimes \rho_B) \). It is the probability that event \((i, j)\) happens conditional on that Alice sends out photon-number state \( \rho_A \) with polarization \( \alpha \) and Bob sends out photon number state \( \rho_B \) with polarization \( \beta \). Sometimes we simply use \( q_{ij}^{\alpha,\beta} \) for simplicity.

B. Elementary formulas and outline for the model

Given the definitions above, we now formulate various conditional probabilities. We start with the probability of event \((i, j)\) conditional on the output state \(|l_i l_j\rangle\).

\[
P(ij|l_i l_j) = \begin{cases} 
(1 - d)^2, & \text{if } l_i > 0, l_j > 0 \\
 d(1 - d)^2, & \text{if } l_i \cdot l_j = 0 \text{ and } l_i + l_j > 0 \\
 d^2(1 - d)^2, & \text{if } l_i = l_j = 0 
\end{cases}
\]

(1)

Here the detection efficiency does not appear because we put shall this into the channel loss and hence we assume perfect detection efficiency. The factor \((1 - d)^2\) comes from the fact that we request detectors other than \( i, j \) not to click. Also, the probability for event \((i, j)\) is 0 if any mode other than \( i, j \) is not vacuum. Given these, we can now calculate probability distribution of the various two fold events given arbitrary input states of the beam-splitter. Therefore, for any output state of the beam-splitter \( \rho_{out} \), the probability that event \((i, j)\) happens is

\[
P(ij|\rho_{out}) = \sum_{l_i, l_j} P(ij|l_i l_j) \langle l_i l_j|\rho_{out}|l_i l_j\rangle
\]

(2)

Based on this important formula, we can calculate the probability of event \((i, j)\) for any input state by this formula. For the purpose, we only need to formulate \( \rho_{out} \). Therefore, given the source state of the two pulses \( \rho_A \otimes \rho_B \), we can use the following procedure to calculate the probability of event \((i, j)\), \( p_{ij}(\rho_A \otimes \rho_B)\):

i) Using the linear channel loss model to calculate the two-pulse state when arriving at the beam-splitter. Explicitly, if the channel transmittance is \( \eta \), any state \(|n\rangle\langle n|\) is changed into

\[
|n\rangle\langle n| \rightarrow \sum C_n^k \eta^k (1 - \eta)^n-k |k\rangle\langle k|.
\]

(3)
ii) Using the transformation: 
\[ a_{H,V}^\dagger \rightarrow \frac{1}{\sqrt{2}}(a_{H,V}^\dagger + b_{H,V}^\dagger); \quad b_{H,V}^\dagger = \frac{1}{\sqrt{2}}(a_{H,V}^\dagger - b_{H,V}^\dagger) \]
to calculate the output state of the beam-splitter, \( \rho_{\text{out}} \).

iii) Using Eq.(2) to calculate the probability of event \((i,j)\). According to the protocol, we shall only be interested in the probabilities of successful events, \((1,2)\), \((3,4)\), \((1,4)\) and \((2,3)\).

Below we will describe the detailed calculation processes in Z basis and X basis individually.

In Z basis, all successful events correspond to correct bit values when Alice and Bob send out orthogonal polarizations, and they correspond to wrong bit values when Alice and Bob send out the same polarizations. The observed gain in Z basis for photon-number state \( \rho_A \otimes \rho_B \) is,

\[ S_Z^{\rho_A \otimes \rho_B} = \frac{1}{4} \sum_{(i,j) \in \text{Suc}} [q_{ij}^{HV}(\rho_A \otimes \rho_B) + q_{ij}^{VH}(\rho_A \otimes \rho_B) + q_{ij}^{HH}(\rho_A \otimes \rho_B) + q_{ij}^{VV}(\rho_A \otimes \rho_B)] \]  

and the set \( \text{Suc} = \{(1,2), (3,4), (1,4), (2,3)\} \). Here, as defined in Definition 4, \( q_{ij}^{\alpha\beta}(\rho_A \otimes \rho_B) \) represents the probability of event \((i,j)\) whenever Alice sends her photon number state \( \rho_A \) with polarization \( \alpha \) and Bob sends his photon number state \( \rho_B \) with polarization \( \beta \). For simplicity, we shall omit \( \rho_A \otimes \rho_B \) in brackets or in subscripts if there is no confusion.

Meantime, the successful events caused by the same polarizations will be counted as wrong bits. These will contribute to the bit-flip rate by:

\[ \tilde{E}^Z = \frac{\sum_{(i,j) \in \text{Suc}} [q_{ij}^{++} + q_{ij}^{--}]}{4S_Z^Z} \]  

In X basis, we should be careful that the situation is different from in Z basis, since now the successful events correspond to correct bits include two parts: 1) Alice and Bob send out the same polarizations \((++\) or \(--\)), and Charlie detects \( \Phi^+ \) ((1,2) or (3,4) events happen); 2) Alice and Bob send out orthogonal polarizations \((+-\) or \(--+\)), and Charlie detects \( \Psi^- \) ((1,4) or (2,3) events happen). And the left successful events belong to wrong bits. Therefore, we have

\[ S_X = \frac{1}{4} \sum_{(i,j) \in \text{Suc}} [q_{ij}^{++} + q_{ij}^{--} + q_{ij}^{+-} + q_{ij}^{-+}] \]  

and

\[ \tilde{E}^X = \frac{\sum_{(i,j) \in (14),(23)} [q_{ij}^{++} + q_{ij}^{--}] + \sum_{(i,j) \in (12),(34)} [q_{ij}^{+-} + q_{ij}^{-+}]}{4S_X^X} \]
Moreover, there are alignment errors which will cause a fraction \(E_d\) of states to be flipped. We then modify the error rate in different bases by

\[
E^Z = E_d \cdot (1 - 2\bar{E}^Z) + \bar{E}^Z
\]

and

\[
E^X = E_d \cdot (1 - 2\bar{E}^X) + \bar{E}^X
\]

Note that in the above two formulas above, we have considered this fact: before taking the alignment error into consideration, the successful events can be classified into two classes: one class has no error and the other class has an error rate of 50%, they are totally random bits. The second class takes a fraction of \(2E^Z\) (or \(2E^X\)) among all successful events. Alignment error does not change the error rate of the second class of events, since they are random bits only.

Given these, we can simulate the final key rate. In a model of numerical simulation, our goal is to deduce the probably would-be value for \(S^Z, S^X\) and \(E^Z, E^X\) in experiments. Given these, one can then calculate the yield of the single-photon pairs, \(s_{11}\), the bit-flip rates in \(Z\) basis and \(X\) basis, and hence the final key rate. Now everything is reduced to calculate all \(p^\alpha_\beta_{ij}\) above.

C. Conditional probabilities for beam-splitter’s incident state of \(k_1\) photons in mode \(a\) and \(k_2\) photons in mode \(b\)

We consider the case that there are \(k_1\) incident photons in mode \(a\) and \(k_2\) incident photons in mode \(b\) of the beam-splitter. Each incident pulse of the beam-splitter has its own polarization and is indicated by a subscript. In general, we consider the state

\[
|k_1\alpha\rangle|k_2\beta\rangle
\]

We shall consider the conditional probabilities for various successful events, i.e. \(p^\alpha_\beta_{ij}(k_1k_2)\). Since we only consider the incident state of \(k_1\) photons in mode \(a\) and \(k_2\) photons in mode \(b\), we shall simply use \(p^\alpha_\beta_{ij}\) for \(p^\alpha_\beta_{ij}(k_1k_2)\) in what follows.

i) in \(Z\) basis

First, we consider the following two-mode state

\[
|k_1\rangle_H|k_2\rangle_V = \frac{1}{\sqrt{k_1!k_2!}}a^{k_1\dagger}_{H}b^{k_2\dagger}_{V}|0\rangle
\]

\[
|k_1\rangle_H|k_2\rangle_V = \frac{1}{\sqrt{k_1!k_2!}}a^{k_1\dagger}_{H}b^{k_2\dagger}_{V}|0\rangle
\]

7
as the input state of the beam-splitter. After BS, the output state $|\psi\rangle$ is

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^{k_1+k_2} \frac{1}{\sqrt{k_1!k_2!}} (a_H^\dagger + b_H^\dagger)^{k_1}(a_V^\dagger - b_V^\dagger)^{k_2}|0\rangle$$  \hspace{1cm} (12)

Therefore

$$\langle l_1 l_2 | \rho_{out} | l_1 l_2 \rangle = (1/2)^{k_1+k_2} \delta_{k_1 l_1} \delta_{k_2 l_2}$$  \hspace{1cm} (13)

According to Eq. (2), the conditional probability for event (1,2) is

$$p_{12}^{HV} = P(12|\rho_{out}) = \sum_{l_1, l_2} P(12|l_1 l_2)(1/2)^{k_1+k_2} \delta_{k_1 l_1} \delta_{k_2 l_2} = (1/2)^{k_1+k_2} P(12|k_1 k_2)$$  \hspace{1cm} (14)

Similarly, we have

$$p_{34}^{HV} = (1/2)^{k_1+k_2} P(34|k_1 k_2)$$

$$p_{14}^{HV} = (1/2)^{k_1+k_2} P(14|k_1 k_2)$$

$$p_{23}^{HV} = (1/2)^{k_1+k_2} P(23|k_2 k_1)$$  \hspace{1cm} (15)

Note that here $P(ij|m_n)$ is just $P(ij|l_i = k_m, l_j = k_n)$ when $l_i = k_1$ as defined by our Definition 2 in previous section. For example, $P(23|k_2 k_1)$ is actually $P(23|l_2 = k_2, l_3 = k_1)$.

Similarly, if the beam-splitter’s input state is $|k_1\rangle_V |k_2\rangle_H$, i.e. $k_1$ vertical photons in mode $a$ and $k_2$ horizontal photons in mode $b$, we have

$$p_{12}^{VH} = (1/2)^{k_1+k_2} P(12|k_2 k_1)$$

$$p_{34}^{VH} = (1/2)^{k_1+k_2} P(34|k_2 k_1)$$

$$p_{14}^{VH} = (1/2)^{k_1+k_2} P(14|k_2 k_1)$$

$$p_{23}^{VH} = (1/2)^{k_1+k_2} P(23|k_1 k_2)$$  \hspace{1cm} (16)

Next we consider the following two-mode state

$$|k_1\rangle_H |k_2\rangle_H = \frac{1}{\sqrt{k_1!k_2!}} a_H^\dagger^{k_1} b_H^\dagger^{k_2} |0\rangle$$  \hspace{1cm} (17)

as the input state of the beam-splitter. After the beam-splitter, it changes into:

$$|\psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^{k_1+k_2} \frac{1}{\sqrt{k_1!k_2!}} (a_H^\dagger + b_H^\dagger)^{k_1}(a_V^\dagger - b_V^\dagger)^{k_2}|0\rangle$$  \hspace{1cm} (18)

We have the following uniform formula for probabilities of any successful events:

$$p_{ij}^{HH} = \begin{cases} 
\left(\frac{k_1+k_2}{k_1!k_2!}\right)^2 (1/2)^{k_1+k_2} P(ij|k_1+k_2, 0); & \text{for } i = 1, j = 2; \text{or } i = 3, j = 4 \\
\left(\frac{k_1+k_2}{k_1!k_2!}\right)^2 (1/2)^{k_1+k_2} P(ij|0, k_1+k_2); & \text{for } i = 1, j = 4; \text{or } i = 2, j = 3 
\end{cases}$$  \hspace{1cm} (19)
Similarly, when the beam-splitter’s input pulses are both vertical, we can find the value for $p_{ij}^{VV}$.

ii) in $X$ basis

We first consider the beam-splitter’s input state of $|k_1⟩_+|k_2⟩_-$, i.e., there are $k_1$ photon with $\pi/4$ polarization in mode $a$ and $k_2$ photons with $3\pi/4$ polarization in mode $b$. Note that $|±⟩ = \frac{1}{\sqrt{2}}(|H⟩ ± |V⟩)$. The output state of the beam-splitter is

$$|ψ⟩ = \frac{1}{2^{k_1+k_2}}(a_H^† + a_V^† + b_H^† + b_V^†)^{k_1}(a_H^† - a_V^† - b_H^† + b_V^†)^{k_2}|0⟩.$$  \hspace{1cm} (20)

We have

$$⟨l_i l_j|ψ⟩ = \frac{1}{2^{k_1+k_2}} \sum_{i=0}^{Δ_2} \sqrt{l_i!l_j!}C_{k_1}^s C_{k_2}^{l_i+s}(-1)^{k_2-l_i+s}δ_{l_i+l_j,k_1+k_2}$$ \hspace{1cm} (21)

where

$$Δ_1 = min\{l_i, k_1\}, \hspace{0.5cm} Δ_2 = l_i - min\{l_i, k_2\}$$  \hspace{1cm} (22)

and $min\{l_i, k_1(k_2)\}$ is the smaller one of $l_i$ and $k_1(k_2)$. Thus we can calculate the conditional probabilities by

$$p_{ij}^{+-} = \frac{k_{1+k_2}}{4^{k_1+k_2}k_1!k_2!} \sum_{i=0}^{Δ_1} \sum_{s=Δ_2} \sqrt{l_i!l_j!(k_1+k_2-l_i)!(k_1+k_2-l_j)!}C_{k_1}^s C_{k_2}^{l_i+s}(-1)^{l_i-s}P(ij|l_i, k_1+k_2-l_i)$$ \hspace{1cm} (23)

for $i = 1, j = 2$ and $i = 3, j = 4$; and

$$p_{ij}^{+-} = \frac{k_{1+k_2}}{4^{k_1+k_2}k_1!k_2!} \sum_{i=0}^{Δ_1} \sum_{s=Δ_2} \sqrt{l_i!(k_1+k_2-i)!}C_{k_1}^s C_{k_2}^{l_i+s}P(ij|l_i, k_1+k_2-l_i)$$ \hspace{1cm} (24)

for $i = 1, j = 4$ and $i = 2, j = 3$. Besides, it is easy to show

$$p_{ij}^{-+} = p_{ij}^{+-}$$ \hspace{1cm} (25)

If the polarization of incident pulses of the beam-splitter are both $\pi/4$, then the output state is

$$|ψ⟩ = \frac{1}{2^{k_1+k_2}}(a_H^† + a_V^† + b_H^† + b_V^†)^{k_1}(a_H^† + a_V^† - b_H^† - b_V^†)^{k_2}|0⟩.$$  \hspace{1cm} (26)

We find

$$p_{ij}^{++} = \frac{k_{1+k_2}}{4^{k_1+k_2}k_1!k_2!} \sum_{i=0}^{Δ_1} \sum_{s=Δ_2} \sqrt{l_i!(k_1+k_2-i)!}C_{k_1}^s C_{k_2}^{l_i+s}P(ij|l_i, k_1+k_2-l_i)$$ \hspace{1cm} (27)
for \( i = 1, j = 2 \) and \( i = 3, j = 4 \); and

\[
p^{++}_{ij} = \frac{1}{4k_1 + k_2} k_1^{k_1+k_2} \sum_{l_i=0}^{\frac{\Delta_1}{2}} \left| \sum_{s=\Delta_2} \sqrt{l_i!(k_1 + k_2 - l_i)!} C^{s}_{k_1} C^{d-s}_{k_2} (-1)^{l_i-s} \right|^2 P(ij|l_i, k_1 + k_2 - l_i) \quad (28)
\]

for \( i = 1, j = 4 \) and \( i = 2, j = 3 \). Also, we have

\[
p^{--}_{ij} = p^{++}_{ij} \quad (29)
\]

### D. Probabilities of events conditional on source states

In the above subsection, we have formulated the probabilities of various events conditional on a pure input state \( |k_1\rangle|k_2\rangle \). In fact, the results can be easily extended to the more general case when the beam-splitter’s input state is a mixed state. Say,

\[
\left( \sum_{k_1} f_{k_1} |k_1\rangle \langle k_1| \right) \otimes \left( \sum_{k_2} f_{k_2} |k_2\rangle \langle k_2| \right) \quad (30)
\]

Suppose the polarizations of mode \( a, b \) are \( \alpha, \beta \), respectively. We then have

\[
p^{\alpha\beta}_{ij} = \sum_{k_1, k_2} f_{k_1} f_{k_2} p^{\alpha\beta}_{ij} (k_1 k_2) \quad (31)
\]

where \( p^{\alpha\beta}_{ij} (k_1 k_2) \) is the same as defined in the previous subsection, for all possible polarizations \( (\alpha, \beta) = (H, V), (V, H), (H, H), (V, V), (+, -), (-, +), (+, +), (-, -) \). To formulate the probabilities conditional on any source states, we only need to relate the source state with the beam-splitter’s input state. Suppose the source state in photon-number space is \( \rho_A \otimes \rho_B \) and

\[
\rho_A = \sum_n a_n |n\rangle \langle n| \\
\rho_B = \sum_n b_n |n\rangle \langle n| \quad (32)
\]

After some loss channel, the state changes into the beam-splitter’s input state as Eq.(30). Suppose the transmittance for the channel between Alice (Bob) and UTP is \( \eta_A \) (\( \eta_B \)). Using the linear loss model of Eq. (3) we have

\[
f_{k_1} = \sum_{n \geq k_1} a_n \eta_A^{k_1} (1 - \eta_A)^{n-k_1} C^k_n \\
f_{k_2} = \sum_{n \geq k_2} b_n \eta_B^{k_2} (1 - \eta_B)^{n-k_2} C^k_n \quad (33)
\]

We now arrive at our major conclusion:
Major conclusion: Formulas of \( p_{ij}^{\alpha\beta}(k_1k_2) \) in the earlier subsection together with Eqs. (31-33) complete the model of probabilities of different events conditional on any source states, i.e., the gains. Using Eqs. (8,9), one can also model the observed error rates of any source states.

E. 3-intensity decoy-state MDI-QKD

Using the Major conclusion above, we can model the gains and the error rates with a 3-intensity decoy-state MDI-QKD method [22, 23]. We assume that Alice (Bob) has three intensities in their source states, denoted as 0, \( \mu_A, \mu'_A \) (0, \( \mu_B, \mu'_B \)). Denote \( \rho_x \) (\( \rho_y \)) as the density operator for source \( x \) (\( y \)) at Alice’s (Bob’s) side, and \( x \) (\( y \)) can take any value from 0, \( \mu_A, \mu'_A \) (0, \( \mu_B, \mu'_B \)).

\[
\rho_0 = |0\rangle\langle 0|; \rho_{\mu_A} = \sum_k a_k |k\rangle\langle k|; \rho_{\mu'_A} = \sum_k a'_k |k\rangle\langle k|; \rho_{\mu_B} = \sum_k b_k |k\rangle\langle k|; \rho_{\mu'_B} = \sum_k b'_k |k\rangle\langle k|
\]  

Then we have the expression for the low bound of the yield of single-photon pulse pairs

\[
Y_{11}^X \geq Y_{11}^{X,L} \equiv \frac{a'_{1}b_{1}^{2}(S_{\mu,\mu}^{X} - \tilde{S}_{0}^{X}) - a_{1}b_{2}(S_{\mu,\mu'}^{X} - \tilde{S}'_{0}^{X})}{a'_{1}a_{1}(b'_{2}b_{1} - b_{2}b'_{1})}
\]

and their upper bound of the phase flip-error rate

\[
e_{11}^{X} \leq e_{11}^{X,U} \equiv \frac{E_{\mu,\mu}S_{\mu,\mu}^{X} - E_{\mu,0}S_{\mu,0}^{X} - E_{0,\mu}S_{0,\mu}^{X} + E_{0,0}S_{0,0}^{X}}{Y_{11}^{X}}
\]

With the results above, now we can calculate the key rate with the formula [19, 22, 23]

\[
R \geq a'_{1}b_{1}Y_{11}^{Z}[1 - H(e_{11}^{X})] - S_{\mu',\mu'}^{Z}f(E_{\mu',\mu'}^{Z})H(E_{\mu',\mu'}^{Z})
\]

III. NUMERICAL SIMULATIONS

Using all the above correspondence, we can numerically simulate the gains and error rates of any source states. Taking as an example, we consider the source of a HSPS from parametric down-conversion processes [22]. It originally has a Poissonian photon number distribution when pumped by a continuous wave (CW) laser [29], written as:

\[
|\psi\rangle = \frac{x^n}{n!}e^{-x}
\]
where $x$ is the average intensity of the emission light. However, after chosen a proper gating time and triggered with a practical single photon detector, a sub-Poissonian distributed source state can be obtained, which can be expressed as:

$$
\rho = \left[ P_{\text{Cor}} d_i + (1 - P_{\text{Cor}}) e^{-x} \right] |0\rangle \langle 0| + \sum_{n=1}^{\infty} \left[ P_{\text{Cor}} e^{-x} \frac{x^{n-1}}{(n-1)!} + (1 - P_{\text{Cor}}) e^{-x} \frac{x^n}{n!} \right] |n\rangle \langle n| \tag{39}
$$

where $P_{\text{Cor}}$ is the correlation rate of photon pairs, i.e., the probability that we can predict the existence of a heralded photon when a heralding one was detected; $d_i$ is the dark count rate of the triggering detector.

In the following numerical simulations, for simplicity, we assume the UTP lies in the middle of Alice and Bob, and all triggering detectors (at Alice or Bob’s side) have the same detection efficiency (75%) and the same dark count rate ($10^{-6}$). We also assume all triggered detectors (at the UTP’s side) have the same detection efficiency (they are attributed into the channel loss), and the same dark count rate ($3 \times 10^{-6}$). Besides, we set the system misalignment probability to be 1.5%.

Fig. 2(a) and (b) each show the low bound of $Y_{11}$ (in X or Z basis) and the upper bound of $c_{11}^X$ changing with channel loss for different source states, i.e., the weak coherent sources (W), the poissonian heralded single photon sources (P) and the sub-poisonian heralded single photon sources (S). The solid line represents the result of using infinite number of decoy state method (W0), and the dashed or dotted lines (P1 or S1) are the results of using three-decoy state method.

Similar to Fig. 2(a) and (b), Fig. 3(a) and (b) each show corresponding values of the gains ($S_{\mu\mu'}^Z$) and the quantum bit-error rates (QBER) ($E_{\mu\mu'}^Z$) of signal pulses in Z basis for different source states. And Fig. 5 presents the final key rate changing with channel loss.

See from Fig. 4, we find that the sub-poisonian heralded single photon sources can generate the highest key rate at lower or moderate channel loss ($\leq 64$ dB). Because within this range, its signal state has a lower QBER than in the weak coherent sources, and a higher gain than in the poissonian heralded single photon sources as simulated in Fig. 3 (a) and (b). However, at larger channel loss ($\geq 64$ dB), the poissonian heralded single photon source shows better performance than the other two, this is mainly due to its much lower vacuum component which may play an essential role in the key distillation process when suffering from larger channel loss.
FIG. 2: (Color online) (a) The lower bound of $Y_{11}$ and (b) the upper bound of $e_{11}^X$ for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources [19], possonian heralded single photon sources [9] or sub-possonian heralded single photon sources [22], individually. X or Z represent in X or Z basis respectively. Here at each point, we set $\mu = 0.05$, and optimize the value for $\mu'$.

IV. CONCLUSIONS

In summary, we have presented a general model for simulating the gains, the error rates and the key rates for MDI-QKDs, which can be applicable to the schemes of using arbitrary convex source states and any coding methods. This facilitates the performance evaluation
FIG. 3: (Color online) (a) The gain and (b) the quantum error-bit rate in Z basis for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources, poissonian heralded single photon sources [9] or sub-poissonian heralded single photon sources [22], individually. Here at each point, we set $\mu = 0.05$, and optimize the value for $\mu'$.

of any MDI-QKD methods, and thus make it a valuable tool for devising high efficient QKD protocols and for studying long distance quantum communications.

V. ACKNOWLEDGMENTS

We gratefully acknowledge the financial support from the National High-Tech Program of China through Grants No. 2011AA010800 and No. 2011AA010803, the NSFC through
FIG. 4: (Color online) (a) The final key rate for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources, poissonian heralded single photon sources [9] or sub-poissonian heralded single photon sources [22], individually. Here at each point, we set $\mu = 0.05$, and optimize the value for $\mu'$. 

Grants No. 11274178, No. 11174177, No. 60725416 and No. 11311140250, and the 10000-Plan of Shandong province. The author-X. B. Wang thanks Y. H. Zhou and Z. W. Yu for useful discussion.

[1] C.H. Bennett, and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. 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, and H. Zbinden, Quantum cryptography. Rev. Mod. Phys. 74, 145 (2002); N. Gisin, and R. Thew, Quantum communication. Nature Photonics, 1, 165 (2006); M. Dusek, N. Lütkenhaus, M. Hendrych, Quantum Cryptography. Progress in Optics VVVX, edited by E. Wolf (Elsevier, 2006); V. Scarani, H. Bechmann-Pasquenucci, N.J. Cerf, M. Dusek, N. Lütkenhaus, and M Peev, The security of practical quantum key distribution.
Rev. Mod. Phys. 81, 1301 (2009).

[3] H. Inamori, N. Lütkenhaus, and D. Mayers, Unconditional Security of Practical Quantum Key Distribution. Eur. Phys. J. D, 41, 599 (2007), which appeared in the arXiv as quant-ph/0107017; D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect Devices. Quantum Inf. Comput. 4, 325 (2004).

[4] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. 91, 057901 (2003).

[5] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. Phys. Rev. Lett. 94, 230503 (2005); X. B. Wang, Decoy-state protocol for quantum cryptography with four different intensities of coherent light. Phys. Rev. A 72, 012322 (2005).

[6] H. K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution. Phys. Rev. Lett. 94, 230504 (2005); X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Practical decoy state for quantum key distribution. Phys. Rev. A 72, 012326 (2005).

[7] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion. Phys. Rev. Lett. 99, 180503 (2007).

[8] Q. Wang, X. B. Wang, and G. C. Guo, Practical decoy state method in quantum key distribution with heralded single photon source. Phys. Rev. A 75, 012312 (2007).

[9] Q. Wang, et al., Experimental Decoy-State Quantum Key Distribution with a Sub-Poissonian Heralded Single-Photon Source. Phys. Rev. Lett. 100, 090501 (2008).

[10] M. Hayashi, Practical evaluation of security for quantum key distribution. Phys. Rev. A 74, 022307 (2006); M. Hayashi, Upper bounds of eavesdropper performance in finite-length code with the decoy method. Phys. Rev. A 76, 012329 (2007).

[11] D. Rosenberg, et al., Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. Phys. Rev. Lett. 98, 010503 (2007); T. S. Manderbach, et al., Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. Phys. Rev. Lett. 98, 010504 (2007); C. Z. Peng, et al., Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding. Phys. Rev. Lett. 98, 010505 (2007); Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Unconditionally secure one-way quantum key distribution using decoy pulses. Appl. Phys. Lett. 90, 011118 (2007); Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Experimental Quantum Key Distribution with Decoy States. Phys. Rev. Lett. 96, 070502 (2006); Y. Zhao, R. Adve, and T. J. Lim, Improving Amplify-and-Forward Relay
Networks: Optimal Power Allocation versus Selection. Proceedings of IEEE International Symposium on Information Theory, Seattle, 2006, pp.2094-2098 (IEEE, New York).

[12] X. B. Wang, C. Z. Peng, J. Zhang, L. Yang, and J. W. Pan, General theory of decoy-state quantum cryptography with source errors. Phys. Rev. A 77, 042311 (2008); J. Z. Hu, and X. B. Wang, Reexamination of the decoy-state quantum key distribution with an unstable source. Phys. Rev. A 82, 012331 (2010).

[13] X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Quantum Information with Gaussian States. Phys. Rep. 448, 1 (2007).

[14] X. B. Wang, L. Yang, C. Z. Peng, and J. W. Pan, Decoy-state quantum key distribution with both source errors and statistical fluctuations. New J. Phys. 11, 075006 (2009).

[15] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Limitations on Practical Quantum Cryptography. Phys. Rev. Lett. 85, 1330 (2000); N. Lütkenhaus, Security against individual attacks for realistic quantum key distribution. Phys. Rev. A 61, 052304 (2000); N. Lütkenhaus, and M. Jahma, Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. New J. Phys. 4, 44 (2002).

[16] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states. Phys. Rev. A 51, 1863 (1995); H. P. Yuen, Quantum amplifiers, quantum duplicators, and quantum cryptography. Quantum Semiclass. Opt. 8, 939 (1996).

[17] D. Mayers, and A. Yao, Quantum Cryptography with Imperfect Apparatus. Proc. of the 39th Annual Symposium on Foundations of Computer Science (FOCS98) (IEEE Computer Society, Washington, DC, 1998), pp.503; A. Acin, et al., Device-Independent Security of Quantum Cryptography against Collective Attacks. Phys. Rev. Lett. 98, 230501 (2007); V. Scarani, and R. Renner, Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. Phys. Rev. Lett. 100, 200501 (2008); V. Scarani, and R. Renner, Security Bounds for Quantum Cryptography with Finite Resources. Proc. of TQC2008, (Springer Verlag, Berlin), pp.83-95 (2008).

[18] N. Gisin, S. Pironio, and N. Sangouard, Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. Phys. Rev. Lett. 105, 070501 (2010).

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

[20] S. L. Braunstein, and S. Pirandola, Side-Channel-Free Quantum Key Distribution. Phys. Rev.
Lett. 108, 130502 (2012).

[21] L. Lyderson, et al., Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photonics, 4, 686 (2010); I. Gerhardt, et al., Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Commu. 2, 349 (2011).

[22] Q. Wang, and X. B. Wang, An efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. [arXiv:1305.6480] accepted by Phys. Rev. A.

[23] X. B. Wang, Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. Phys. Rev. A 87, 012320 (2013).

[24] A. Rubenok, et al., Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. Phys. Rev. Lett. 111, 130501 (2013).

[25] Y. Liu, et al., Experimental Measurement-Device-Independent Quantum Key Distribution. Phys. Rev. Lett. 111, 130502 (2013).

[26] F. H. Xu, M. Curty, B. Qi, H. K. Lo, Long distance measurement-device-independent quantum key distribution with entangled photon sources. Appl. Phys. Lett. 103, 061101 (2013).

[27] M. Curty et al., Finite-key analysis for measurement-device-independent quantum key distribution. [arXiv:1307.1081v1].

[28] K. Tamaki, H. K. Lo, C. H. F. Fung, and B. Qi, Phase encoding schemes for measurement device independent quantum key distribution and basis-dependent flaw. Phys. Rev. A 85, 042307 (2012).

[29] During a spontaneous parametric down conversion (SPDC) process, if a pulsed pump laser is used, as long as the coherence time of the emission, $\Delta t_c$, is much longer than the duration of the pump pulse, $\Delta t$, i.e., $\Delta t_c \gg \Delta t$, (in practice easily obtained by using ultrafast (fs) pulse pump lasers), a single emission process will take place, giving an thermal photon number distribution. In contrast, when a continuous wave (CW) laser is used, as long as $\Delta t_c$ is much shorter than the gating period of the detector, a large number of independent SPDC processes will be present, each thermally distributed, but collectively resulting in a Poisson distribution. However, the "original" distribution can be altered by conditional gating. By choosing proper gating time and using an appropriate correlation rate, a sub-Poissonian distributed HSPS can be obtained as the result of postselections.