SCIENTIFIC REPORTS

OPEN

SUBJECT AREAS:
QUANTUM OPTICS
QUANTUM INFORMATION

Received
28 November 2013

Accepted
28 February 2014

Published
14 April 2014

Correspondence and requests for materials should be addressed to X.-B.W. (xbwang@mail.tsinghua.edu.cn)

Simulating of the measurement-device independent quantum key distribution with phase randomized general sources

Qin Wang[1] & Xiang-Bin Wang[2,3]

[1]Institute of Signal Processing and Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China, [2]Department of Physics and State Key Laboratory of Low Dimensional Quantum Physics, Tsinghua University, Beijing 100084, China, [3]Jinan Institute of Quantum Technology, Shandong Academy of Information Technology, Jinan, China.

We present a model on the simulation of the measurement-device independent quantum key distribution (MDI-QKD) with phase randomized general sources. 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 arbitrary probabilistic mixture of different photon states or using any coding schemes. Therefore, it is useful in characterizing and evaluating the performance of the MDI-QKD protocol, making it a valuable tool in studying the quantum key distributions.

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[1–5]) 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[6–27] which can rescue the QKD with imperfect single-photon sources[28–32], while the device-independent quantum key distribution[33–37] and the recently proposed measurement-device independent quantum key distribution (MDI-QKD)[38,39] can further relieve the QKD even when the detectors are controlled by the eavesdropper[40,41]. 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[38,42–49].

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 an important job to make a 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[42,43]. Before experimentally testing all of them, one can choose to give a theoretical comparison with a reasonable model. In the traditional decoy state methods[8–12], the simulation model with linear channel loss is relatively simple. For example, given a source state, it is easy to calculate the state after transmission, and further estimate the gains and error rates possibly being observed in an experiment. However, for MDI-QKDs, it is not a simple job except for the special case of using weak coherent states, because both sides send out pulses and the successful events and errors are defined differently. So far, there have been proposals with different sources, e.g., the heralded single-photon source (HSPS) *etc*[14,15,42]. 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 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.

The general model on MDI-QKD

A. Setups and definitions. Consider the schematic setup in Fig. 1[38], 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 ξ. 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 η_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 $a_H^\dagger$, $a_V^\dagger$, $b_H^\dagger$, $b_V^\dagger$ in creation operator. For simplicity, we denote them by $c_i^\dagger$, i.e., $c_1^\dagger = a_H^\dagger$, $c_2^\dagger = a_V^\dagger$, $c_3^\dagger = b_H^\dagger$, $c_4^\dagger = b_V^\dagger$. 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* ρ_{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, $|l_i l_j\rangle = \frac{1}{\sqrt{l_i! l_j!}} c_i^{\dagger l_i} c_j^{\dagger l_j} |0\rangle$. $P(ij|l_i, l_j)$ 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 ρ_{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 α for mode a and k_2 photons of polarization β for mode b as the input state of the beam-splitter. Hereafter, we omit the comma between k_1 and k_2. α or β indicate the photon polarization. Explicitly, α or β 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 ρ_A with polarization α and Bob sends out photon number state ρ_B with polarization β. 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 $|l_i l_j\rangle$.

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

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 ρ_{out}, the probability that event (i, j) happens is

$$P(ij|\rho_{out}) = \sum_{l_i, l_j} P(ij|l_i l_j) \langle l_i l_i|\rho_{out}|l_i l_j\rangle \quad (2)$$

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 ρ_{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 η, any state $|n\rangle\langle n|$ is changed into

$$|n\rangle\langle n| \to \sum C_n^k \eta^k (1-\eta)^{n-k} |k\rangle\langle k|. \quad (3)$$

ii) Using the transformation: $a_{H,V}^\dagger \to \frac{1}{\sqrt{2}}\left(a_{H,V}^\dagger + b_{H,V}^\dagger\right)$; $b_{H,V}^\dagger \to \frac{1}{\sqrt{2}}\left(a_{H,V}^\dagger - b_{H,V}^\dagger\right)$. to calculate the output state of the beam-splitter, ρ_{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,

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

and the set 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 ρ_A with polarization

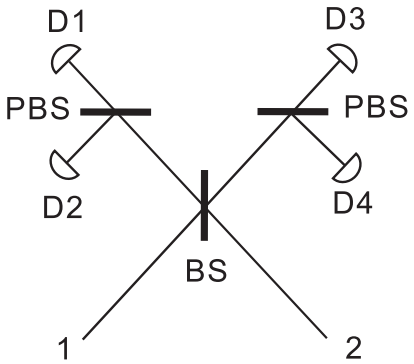

Figure 1 | A schematic of the experimental setup for the collective measurements at the UTP. BS: beam-splitter; PBS: polarization beam-splitter; D1 - D4: single-photon detector; 1, 2: input port for photons. Incident and output lights at the left side of BS are mode a, lights at the right side of BS are mode b.

α and Bob sends his photon number state ρ_B with polarization β. 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:

$$\tilde{E}^Z = \frac{\sum_{(i,j)\in Suc}\left[q_{ij}^{HH} + q_{ij}^{VV}\right]}{4S^Z} \tag{5}$$

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 Φ^+ ((1,2) or (3,4) events happen); 2) Alice and Bob send out orthogonal polarizations ($+-$ or $-+$), and Charlie detects Ψ^- ((1,4) or (2,3) events happen). And the left successful events belong to wrong bits. Therefore, we have

$$S^X = \frac{1}{4}\sum_{(i,j)\in Suc}\left[q_{ij}^{+-} + q_{ij}^{-+} + q_{ij}^{++} + q_{ij}^{--}\right] \tag{6}$$

and

$$\tilde{E}^X = \frac{\sum_{(i,j)\in(14),(23)}\left[q_{ij}^{++} + q_{ij}^{--}\right] + \sum_{(i,j)\in(12),(34)}\left[q_{ij}^{+-} + q_{ij}^{-+}\right]}{4S^X} \tag{7}$$

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

$$E^Z = E_d\cdot\left(1-2\tilde{E}^Z\right) + \tilde{E}^Z \tag{8}$$

and

$$E^X = E_d\cdot\left(1-2\tilde{E}^X\right) + \tilde{E}^X \tag{9}$$

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. 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 $p_{ij}^{\alpha\beta}$ 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

$$|k_1\rangle_\alpha|k_2\rangle_\beta \tag{10}$$

We shall consider the conditional probabilities for various successful events, i.e. $p_{ij}^{\alpha\beta}(k_1k_2)$. 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 $p_{ij}^{\alpha\beta}$ for $p_{ij}^{\alpha\beta}(k_1k_2)$ in what follows.

i) in Z basis

First, we consider the following two-mode state

$$|k_1\rangle_H|k_2\rangle_V = \frac{1}{\sqrt{k_1!k_2!}}a_H^{\dagger k_1}b_V^{\dagger k_2}|0\rangle \tag{11}$$

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

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

Therefore

$$\langle l_1l_2|\rho_{out}|l_1l_2\rangle = (1/2)^{k_1+k_2}\delta_{k_1l_1}\delta_{k_2l_2} \tag{13}$$

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

$$\begin{aligned} p_{12}^{HV} &= P(12|\rho_{out}) = \sum_{l_1,l_2}P(12|l_1l_2)(1/2)^{k_1+k_2}\delta_{k_1l_1}\delta_{k_2l_2} \\ &= (1/2)^{k_1+k_2}P(12|k_1k_2) \end{aligned} \tag{14}$$

Similarly, we have

$$\begin{aligned} p_{34}^{HV} &= (1/2)^{k_1+k_2}P(34|k_1k_2) \\ p_{14}^{HV} &= (1/2)^{k_1+k_2}P(14|k_1k_2) \\ p_{23}^{HV} &= (1/2)^{k_1+k_2}P(23|k_2k_1) \end{aligned} \tag{15}$$

Note that here $P(ij|k_mk_n)$ is just $P(ij|l_i = k_m, l_j = k_n)$ when $l_1 = k_1$ as defined by our Definition 2 in previous section. For example, $P(23|k_2k_1)$ 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

$$\begin{aligned} p_{12}^{VH} &= (1/2)^{k_1+k_2}P(12|k_2k_1) \\ p_{34}^{VH} &= (1/2)^{k_1+k_2}P(34|k_2k_1) \\ p_{14}^{VH} &= (1/2)^{k_1+k_2}P(14|k_2k_1) \\ p_{23}^{VH} &= (1/2)^{k_1+k_2}P(23|k_1k_2) \end{aligned} \tag{16}$$

Next we consider the following two-mode state

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

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

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

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

$$p_{ij}^{HH} = \begin{cases} \frac{(k_1+k_2)!}{k_1!k_2!}(1/2)^{k_1+k_2}P(ij|k_1+k_2,0); \text{ for } i=1,\ j=2; \text{ or } i=3,\ j=4 \\ \frac{(k_1+k_2)!}{k_1!k_2!}(1/2)^{k_1+k_2}P(ij|0,k_1+k_2); \text{ for } i=1,\ j=4; \text{ or } i=2,\ j=3 \end{cases} \tag{19}$$

Similarly, when the beam-splitter's input pulses are both vertical, we can find the value for p_{ij}^{VV}.

ii) X basis

We first consider the beam-splitter's input state of $|k_1\rangle_+|k_2\rangle_-$, 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 $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$. The output state of the beam-splitter is

$$\begin{aligned} |\psi\rangle = &\frac{1}{2^{k_1+k_2}\sqrt{k_1!k_2!}}\left(a_H^\dagger + a_V^\dagger + b_H^\dagger + b_V^\dagger\right)^{k_1} \\ &\left(a_H^\dagger - a_V^\dagger - b_H^\dagger + b_V^\dagger\right)^{k_2}|0\rangle \end{aligned} \tag{20}$$

We have

$$\langle l_i l_j|\psi\rangle = \frac{1}{2^{k_1+k_2}\sqrt{k_1!k_2!}} \sum_{s=\Delta_2}^{\Delta_1} \sqrt{l_i! l_j!} C_{k_1}^{s} C_{k_2}^{l_i-s} (-1)^{k_2-l_i+s} \delta_{l_i+l_j,k_1+k_2} \tag{21}$$

where

$$\Delta_1 = min\{l_i, k_1\}, \quad \Delta_2 = l_i - min\{l_i, k_2\} \tag{22}$$

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

$$p_{ij}^{+-} = \sum_{l_i=0}^{k_1+k_2} \left|\langle l_i l_j|\psi\rangle\right|^2$$

Hence

$$p_{ij}^{+-} = \frac{1}{4^{k_1+k_2} k_1! k_2!} \sum_{l_i=0}^{k_1+k_2} \left| \sum_{s=\Delta_2}^{\Delta_1} \sqrt{l_i!(k_1+k_2-l_i)!} C_{k_1}^{s} C_{k_2}^{l_i-s} (-1)^{l_i-s} \right|^2 P(ij|l_i, k_1+k_2-l_i) \tag{23}$$

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

$$p_{ij}^{+-} = \frac{1}{4^{k_1+k_2} k_1! k_2!} \sum_{l_i=0}^{k_1+k_2} \left| \sum_{s=\Delta_2}^{\Delta_1} \sqrt{l_i!(k_1+k_2-l_i)!} C_{k_1}^{s} C_{k_2}^{l_i-s} \right|^2 P(ij|l_i, k_1+k_2-l_i) \tag{24}$$

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

$$p_{ij}^{-+} = p_{ij}^{+-} \tag{25}$$

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

$$|\psi\rangle = \frac{1}{2^{k_1+k_2}\sqrt{k_1!k_2!}} \left(a_H^\dagger + a_V^\dagger + b_H^\dagger + b_V^\dagger\right)^{k_1} \left(a_H^\dagger + a_V^\dagger - b_H^\dagger - b_V^\dagger\right)^{k_2} |0\rangle. \tag{26}$$

We find

$$p_{ij}^{++} = \frac{1}{4^{k_1+k_2} k_1! k_2!} \sum_{l_i=0}^{k_1+k_2} \left| \sum_{s=\Delta_2}^{\Delta_1} \sqrt{l_i!(k_1+k_2-l_i)!} C_{k_1}^{s} C_{k_2}^{l_i-s} \right|^2 P(ij|l_i, k_1+k_2-l_i) \tag{27}$$

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

$$p_{ij}^{++} = \frac{1}{4^{k_1+k_2} k_1! k_2!} \sum_{l_i=0}^{k_1+k_2} \left| \sum_{s=\Delta_2}^{\Delta_1} \sqrt{l_i!(k_1+k_2-l_i)!} C_{k_1}^{s} C_{k_2}^{l_i-s} (-1)^{l_i-s} \right|^2 P(ij|l_i, k_1+k_2-l_i) \tag{28}$$

for $i = 1, j = 4$ and $i = 2, j = 3$. Also, we have

$$p_{ij}^{--} = p_{ij}^{++} \tag{29}$$

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,

$$\left(\sum_{k_1} f_{k1} |k_1\rangle\langle k_1|\right) \otimes \left(\sum_{k_2} f_{k2} |k_2\rangle\langle k_2|\right) \tag{30}$$

Suppose the polarizations of mode a, b are α, β, respectively. We then have

$$p_{ij}^{\alpha\beta} = \sum_{k_1,k_2} f_{k_1} f_{k_2} p_{ij}^{\alpha\beta}(k_1 k_2) \tag{31}$$

where $p_{ij}^{\alpha\beta}(k_1 k_2)$ 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

$$\rho_A = \sum\nolimits_n a_n |n\rangle\langle n| \qquad \rho_B = \sum\nolimits_n b_n |n\rangle\langle n| \tag{32}$$

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 η_A (η_B). Using the linear loss model of Eq. (3) we have

$$f_{k_1} = \sum\nolimits_{n \geq k_1} a_n \eta_A^{k_1} (1-\eta_A)^{n-k_1} C_n^{k_1} \qquad f_{k_2} = \sum\nolimits_{n \geq k_2} b_n \eta_B^{k_2} (1-\eta_B)^{n-k_2} C_n^{k_2} \tag{33}$$

We now arrive at our major conclusion:

Major conclusion: Formulas of $p_{ij}^{\alpha\beta}(k_1 k_2)$ 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[42,43]. We assume that Alice (Bob) has three intensities in their source states, denoted as 0, μ_A, $\mu'_A(0, \mu_B, \mu'_B)$. Denote ρ_x (ρ_y) as the density operator for source x (y) at Alice's (Bob's) side, and x (y) can take any value from 0, μ_A, $\mu'_A(0, \mu_B, \mu'_B)$.

$$\rho_0 = |0\rangle\langle 0|; \rho_{\mu_A} = \sum_k a_k |k\rangle\langle k|; \ \rho_{\mu'_A} = \sum_k a'_k |k\rangle\langle k|; \quad \rho_{\mu_B} = \sum_k b_k |k\rangle\langle k|; \ \rho_{\mu'_B} = \sum_k b'_k |k\rangle\langle k| \tag{34}$$

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

$$Y_{11}^X \geq Y_{11}^{X,L} \equiv \frac{a'_1 b'_2 \left(S_{\mu,\mu}^X - \tilde{S}_0^X\right) - a_1 b_2 \left(S_{\mu',\mu'}^X - \tilde{S}_0'^X\right)}{a'_1 a_1 (b'_2 b_1 - b_2 b'_1)} \tag{35}$$

and their upper bound of the phase flip-error rate

$$e_{11}^X \leq e_{11}^{X,U} \equiv \frac{E_{\mu,\mu}^X S_{\mu,\mu}^X - E_{\mu,0}^X S_{\mu,0}^X - E_{0,\mu}^X S_{0,\mu}^X + E_{0,0}^X S_{0,0}^X}{Y_{11}^X} \tag{36}$$

With the results above, now we can calculate the key rate with the formula[38,42,43]

$$R \geq a'_1 b'_1 Y_{11}^z \left[1 - H\left(e_{11}^X\right)\right] - S_{\mu'\mu'}^Z f\left(E_{\mu'\mu'}^Z\right) H\left(E_{\mu'\mu'}^Z\right) \tag{37}$$

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[42]. It originally has a Poissonian photon number distribution

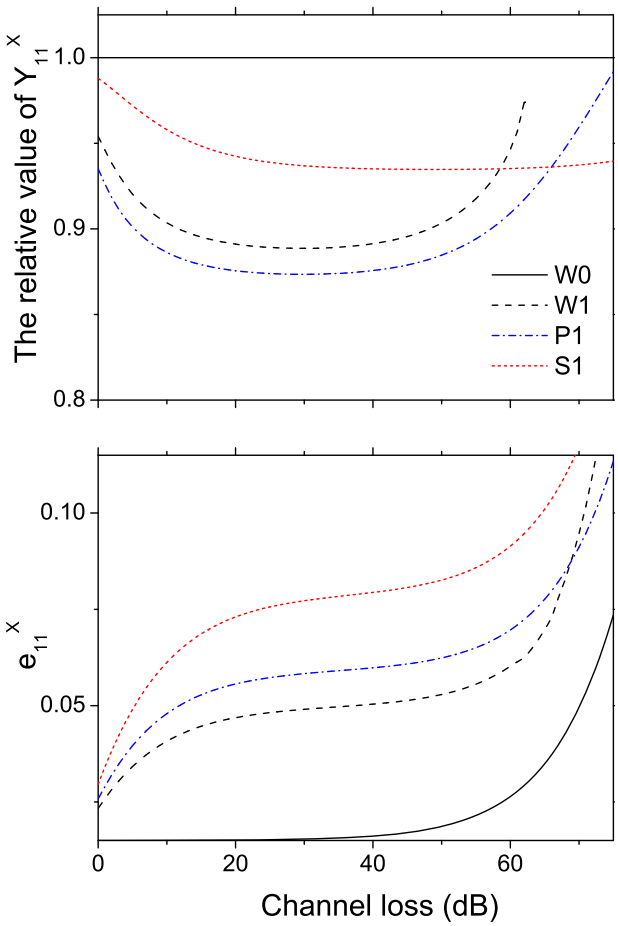

Figure 2 | (a) The relative lower bound of Y_{11}^X and (b) the upper bound of e_{11}^X for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources[38], possonian heralded single photon sources[15] or sub-possonian heralded single photon sources[42], individually. Here the superscript X represents in X basis, and at each point, we set $\mu = 0.05$, and optimize the value for μ'.

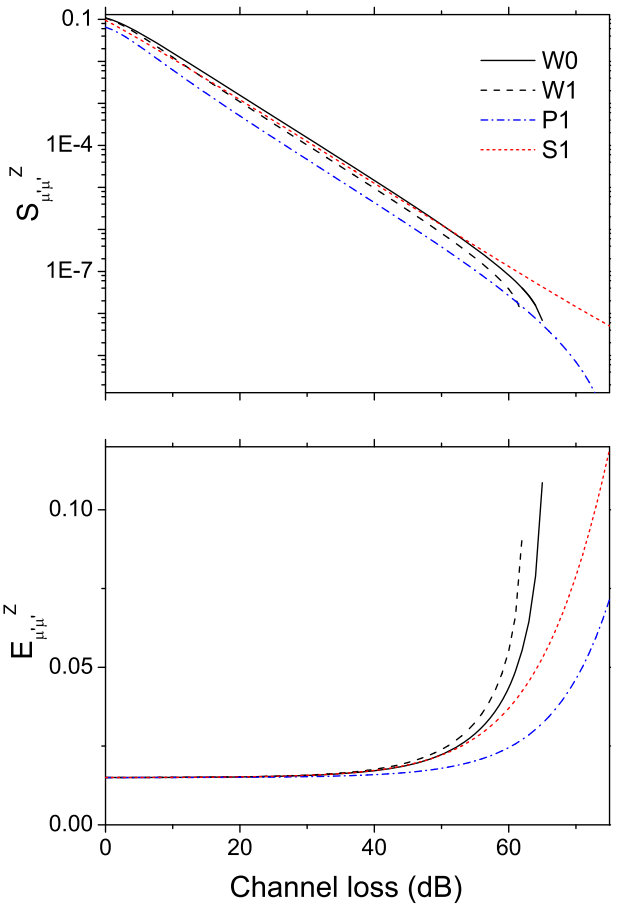

Figure 3 | (a) The gain and (b) the quantum error-bit rate of the signal pulses in Z basis for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources, possonian heralded single photon sources[15] or sub-possonian heralded single photon sources[42], individually. Here at each point, we set $\mu = 0.05$, and optimize the value for μ'.

when pumped by a continuous wave (CW) laser[42], written as:

$$|\psi\rangle = \frac{x^n}{n!}e^{-x} \tag{38}$$

where x is the 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:

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

where $\mathrm{P}^{\mathrm{Cor}}$ 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

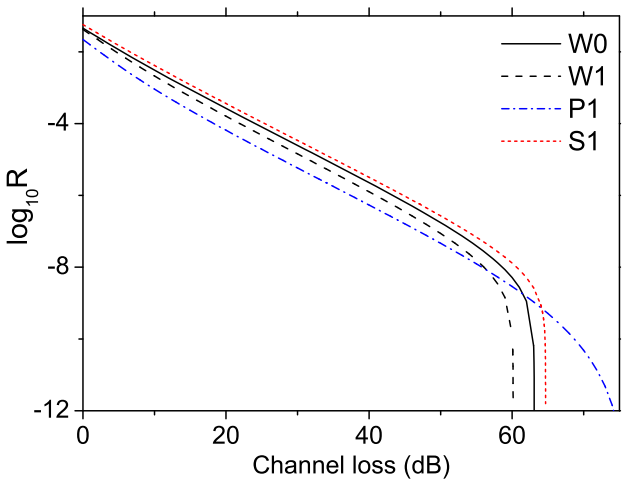

Figure 4 | (a) The final key rate for different photon sources. The solid lines (W0) represent the results of using infinite-decoy state method, and the dashed or dotted lines (W1, P1 or S1) represent using three-decoy state method. Besides, W, P or S each corresponds to the scheme of using weak coherent sources, possonian heralded single photon sources[15] or sub-possonian heralded single photon sources[42], individually. Here at each point, we set $\mu = 0.05$, and optimize the value for μ'.

count rate (3×10^{-6}). Besides, we set reasonable value for the system misalignment probability $E_d = 1.5\%$, and for the correlation rate of photon pairs $P^{Cor} = 0.4$[15].

Fig. 2(a) and (b) each shows the relative low bound of Y_{11}^X and the upper bound of e_{11}^X changing with channel loss for different source states, i.e., the weak coherent sources (W), the possonian heralded single photon sources (P) and the sub-possonian 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 (W1, 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 shows corresponding values of the gains ($S_{\mu'\mu'}^Z$) and the quantum bit-error rates (QBER) ($E_{\mu'\mu'}^Z$) of the signal pulses in Z basis for different source states. And Fig. 4 presents the final key rate changing with channel loss.

See from Fig. 4, we find that the sub-possonian heralded single photon sources can generate the highest key rate at lower or moderate channel loss (≤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 possonian heralded single photon sources as simulated in Fig. 3 (a) and (b). However, at larger channel loss (≥64 dB), the possonian 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 lager channel loss.

Conclusions

In summary, we have presented a 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 probabilistic mixture of different photon states or using any coding methods. This facilitates the performance evaluation of the MDI-QKD with phase randomized general sources, and thus makes it a valuable tool for devising high efficient QKD protocols and for studying long distance quantum communications.

1. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing* [175–179] (IEEE, New York, 1984).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).
3. Gisin, N. & Thew, R. Quantum communication. *Nat. Photon.* **1**, 165 (2007).
4. Dusek, M., Lütkenhaus, N., Hendrych, M. Quantum Cryptography. *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, 2006).
5. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
6. Inamori, H., Lütkenhaus, N. & Mayers, D. Unconditional Security of Practical Quantum Key Distribution. *Eur. Phys. J. D* **41**, 599 (2007).
7. Gottesman, D., Lo, H. K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect Devices. *Quantum Inf. Comput.* **4**, 325 (2004).
8. Hwang, W. Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
9. Wang, X. B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
10. Wang, X. B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **72**, 012322 (2005).
11. Lo, H. K., Ma, X & Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
12. Ma, X., Qi, B., Zhao, Y. & Lo, H. K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **72**, 012326 (2005).
13. Adachi, Y., Yamamoto, T., Koashi, M. & Imoto, N. Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion. *Phys. Rev. Lett.* **99**, 180503 (2007).
14. Wang, Q., Wang, X. B. & Guo, G. C. Practical decoy state method in quantum key distribution with heralded single photon source. *Phys. Rev. A* **75**, 012312 (2007).
15. Wang, Q. *et al.* Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source. *Phys. Rev. Lett.* **100**, 090501 (2008).
16. Hayashi, M. Practical evaluation of security for quantum key distribution. *Phys. Rev. A* **74**, 022307 (2006).
17. Hayashi, M. Upper bounds of eavesdroppers performances in finite-length code with the decoy method. *Phys. Rev. A* **76**, 012329 (2007).
18. Rosenberg, D. *et al.* Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. *Phys. Rev. Lett.* **98**, 010503 (2007).
19. Manderbach, T. S. *et al.* Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. *Phys. Rev. Lett.* **98**, 010504 (2007).
20. Peng, C. Z. *et al.* Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding. *Phys. Rev. Lett.* **98**, 010505 (2007).
21. Yuan, Z. L., Sharpe, A. W. & Shields, A. J. Unconditionally secure one-way quantum key distribution using decoy pulses. *Appl. Phys. Lett.* **90**, 011118 (2007).
22. Zhao, Y., Qi, B., Ma, X., Lo, H. K. & Qian, L. Experimental Quantum Key Distribution with Decoy States. *Phys. Rev. Lett.* **96**, 070502 (2006).
23. Zhao, Y., Adve, R. & Lim, T. J. Improving Amplify-and Forward Relay Networks: Optimal Power Allocation versus Selection. *Proceedings of IEEE International Symposium on Information Theory* [2094–2098] (IEEE, Seattle, New York, 2006).
24. Wang, X. B., Peng, C. Z., Zhang, J., Yang, L. & Pan, J. W. General theory of decoy-state quantum cryptography with source errors. *Phys. Rev. A* **77**, 042311 (2008).
25. Hu, J. Z. & Wang, X. B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A* **82**, 012331 (2010).
26. Wang, X. B., Hiroshima, T., Tomita, A. & Hayashi, M. Quantum Information with Gaussian States. *Phys. Rep.* **448**, 1 (2007).
27. Wang, X. B., Yang, L., Peng, C. Z. & Pan, J. W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **11**, 075006 (2009).
28. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **85**, 1330 (2000).
29. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000).
30. Lütkenhaus, N. & Jahma, M. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New J. Phys.* **4**, 44 (2002).
31. Huttner, B., Imoto, N., Gisin, N. & Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **51**, 1863 (1995).
32. Yuen, H. P. Quantum amplifiers, quantum duplicators, and quantum cryptography. *Quantum Semiclassic. Opt.* **8**, 939 (1996).
33. Mayers, D. & Yao, A. Quantum Cryptography with Imperfect Apparatus. *Proc. of the 39th Annual Symposium on Foundations of Computer Science (FOCS98)* [503–509] (IEEE Computer Society, Washington, DC, 1998).
34. Acin, A. *et al.* Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **98**, 230501 (2007).
35. Scarani, V. & Renner, R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.* **100**, 200501 (2008).
36. Scarani, V. & Renner, R. Security Bounds for Quantum Cryptography with Finite Resources. *Proc. of TQC2008* [83–95] (Springer Verlag, Berlin, 2008).
37. Gisin, N., Pironio, S. & Sangouard, N. Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. *Phys. Rev. Lett.* **105**, 070501 (2010).
38. Lo, H. K., Curty, M. & Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
39. Braunstein, S. L. & Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).
40. Lyderson, L. *et al.* Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **4**, 686 (2010).
41. Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2**, 349 (2011).
42. Wang, Q. & Wang, X. B. An efficient implementation of the decoy-state measurement-device-independent quantum key distribution with heralded single-photon sources. *Phys. Rev. A* **88**, 052332 (2013).
43. Wang, X. B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
44. Rubenok, A. *et al.* Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).
45. Liu, Y. *et al.* Experimental Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **111**, 130502 (2013).
46. Xu, F. H., Curty, M., Qi, B. & Lo, H. K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Appl. Phys. Lett.* **103**, 061101 (2013).
47. Curty, M. *et al.* Finite-key analysis for measurement-device-independent quantum key distribution. arXiv:1307.1081v1 (2013).
48. Tamaki, K., Lo, H. K., Fung, C. H. F. & Qi, B. Phase encoding schemes for measurement device independent quantum key distribution and basis-dependent flaw. *Phys. Rev. A* **85**, 042307 (2012).
49. Ma, X., Fung, C. H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

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

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.

Author contributions

Both authors derived the formulas, wrote the manuscript and reviewed the papers. Q.W. wrote the source code for numerical simulation, X.B.W. analyzed the numerical results.

Additional information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wang, Q. & Wang, X.-B. Simulating of the measurement-device independent quantum key distribution with phase randomized general sources. *Sci. Rep.* **4**, 4612; DOI:10.1038/srep04612 (2014).