Passive scheme with a photon-number-resolving detector for decoy-state quantum key distribution with an untrusted source

Bingjie Xu, Xiang Peng,* and Hong Guo†
CREAM Group, State Key Laboratory of Advanced Optical Communication Systems and Networks (Peking University) and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, PR China
(Dated: February 1, 2010)

A passive scheme with a photon-number-resolving (PNR) detector and a beam splitter which are used to monitor the statistical characteristics of photon source, is proposed to verify the security of vacuum+weak decoy-state quantum key distribution system with an untrusted source. The practical imperfection due to statistical fluctuation and detection noise is considered in the passive-scheme analysis. The simulation results show that the scheme can work efficiently when the data size $N \geq 10^8$ and the dark-count rate of PNR detector is kept below 0.5 counts per pulse, which are realizable by current techniques. We also give an experimental example of PNR detector which is easily realized by a variable optical attenuator combined with a practical threshold detector.

PACS numbers: 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) provides a secure way of establishing correlated random data between two parties (Alice and Bob), while an eavesdropper (Eve) can not obtain any information on the data [1, 2]. The first QKD protocol, i.e., BB84 protocol [3], has been proven to be unconditionally secure [4, 5], even when the imperfect devices are implemented [6, 7]. Due to the channel loss and multi-photon states of the source, Eve can perform the so-called photon-number-splitting (PNS) attack [8], which limits the performance of practical QKD system [2, 7, 9]. Fortunately, the decoy state method was proposed to beat this attack and enhance the performance dramatically [10–12]. Note that the security analysis in [6, 7, 10–12] assumes a trusted QKD source whose characteristics Eve can not control or change. However, this assumption is not always valid in all QKD systems, such as commercial two-way "Plug & Play" system [13]. This QKD system demonstrates self-calibration and good optical visibility which achieves the low quantum bit error rate (QBER) [14]. In this setup, a bright laser source is sent from Bob to Alice, and then attenuated, encoded and sent back to Bob. In principle, Eve can change the source during the process when it is sent from Bob to Alice, and send her wanted source into Alice's side. Thus, the QKD source is an untrusted source whose photon statistics needs to be verified by Alice and Bob.

The qualitative security analysis of untrusted source was first given in [15]. Then rigorous security analysis for BB84 and decoy-state protocols was first given theoretically in [16], where the photon statistics of untrusted source was monitored with active scheme of a high speed optical random switch and a perfect intensity monitor after passing through a single-mode filter and a phase randomizer. Due to the impractical devices of active scheme, the passive scheme with a beam splitter and inefficient detector was first proposed and tested experimentally even though some practical issues, i.e., statistical fluctuation and detection noise, were not considered [17]. Recently, some techniques have been developed to resolve these issues, which makes the passive scheme more robustly applicable [18, 19].

Intuitively, if the performance of untrusted source infinitely approaches to that of trusted source, Alice needs quantum nondemolition (QND) measurement [20] to verify the photon number distribution (PND) of QKD source. However, it is hard to implement the QND measurement in practice. Fortunately, recent results for the vacuum+weak decoy state protocol with an untrusted source have rigorously proved that it is enough to monitor the lower and upper bounds of vacuum, one photon, and two photon states from Alice's side [21, 22]. In the following, a passive scheme with a beam splitter and a photon-number-resolving (PNR) detector which can discriminate vacuum, one photon, two photons and more than two photons, is proposed to monitor the parameters needed in [21, 22] with a confidence level. Some practical issues due to finite data size and random detection noise are included in the analysis. Especially, an experimental realization of PNR detector is analyzed.

II. KEY PARAMETERS IN SECURITY ANALYSIS

Generally, the secure key rate of BB84 protocol is [6, 7]

$$R = \frac{1}{2} Q \left\{ \Delta_1 [1 - H_2(e_1)] - H_2(E) \right\}, \tag{1}$$

where Q and E are, respectively, the count rate and QBER which are measured directly in QKD experiment, Δ_1 (e_1) is the fraction of counts (QBER) due to single photon state, and $H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary Shanon entropy.

In the security analysis of BB84 protocol, all the losses and errors are assumed from the single photon state [8], which

*Correspondence author: xiangpeng@pku.edu.cn.
†Correspondence author: hongguo@pku.edu.cn.

gives

$$\Delta_1 = \frac{Q - P_{multi}}{Q},\ e_1 = \frac{E}{\Delta_1}, \tag{2}$$

where P_{multi} is the probability for Alice to send out multiphoton states. The decoy-state method offers an effective way to estimate the lower (upper) bound of Δ_1 (e_1) compared to Eq. (2) [10–12]. In the vacuum+weak decoy-state protocol [23, 24], Alice randomly sends three kinds of sources: vacuum, decoy and signal, respectively. The quantum state of decoy (signal) source is $\rho_d = \sum_{n=0}^{\infty} a_n |n\rangle\langle n|$ ($\rho_s = \sum_{n=0}^{\infty} a'_n |n\rangle\langle n|$). It has been proved that [21, 22]

$$\Delta_1^s \geq \frac{a_1'^L \left(a_2'^L Q_d - a_2^U Q_s - a_2'^L a_0^U Q_0 + a_2^U a_0'^L Q_0\right)}{Q_s \left(a_1^U a_2'^L - a_1'^L a_2^U\right)}, \tag{3}$$

where Q_0, Q_d, and Q_s are the count rate of vacuum, decoy and signal source, respectively, and Δ_1^s is the fraction of counts due to single photon state of signal source. To calculate the lower bound of Δ_1^s, one needs to estimate the value of $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$, where the superscript $L(U)$ means lower (upper) bound. The secure key rate of signal source is

$$R^s = \frac{1}{2} Q_s \{\Delta_1^s [1 - H_2(e_1^s)] - H_2(E_s)\}, \tag{4}$$

where E_s is the QBER from the signal source and $e_1^s = E_s/\Delta_1^s$. For a QKD system with an untrusted source, the parameters $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$ need to be verified in practice. In the following, we present a general method to estimate these parameters experimentally.

III. THEORY OF ESTIMATION WITH PASSIVE SCHEME

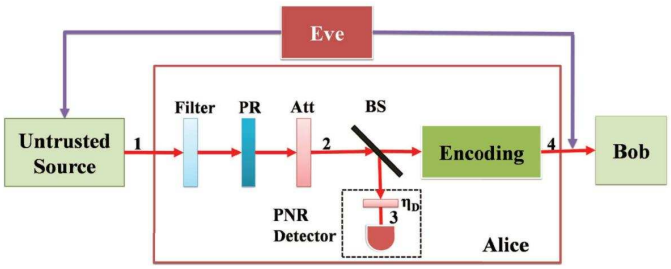


FIG. 1: The passive scheme for estimating the parameters $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$. The untrusted source prepared at P1 by Eve, where Pi means position i ($i = 1, 2, 3, 4$), passes through a low-bandwidth optical filter, a phase randomizer (PR), and an optical variable attenuator (Att) with the attenuation coefficient η_s (η_d) for the signal (decoy) source. Then, a beam splitter (BS) with transmittance η_{BS} is used to separate it into two beams: one goes to a photon-number-resolving (PNR) detector with efficiency η_D at P3, and the other is encoded and sent out of Alice's side at P4.

The experimental scheme for estimating the bounds $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$ is shown in Fig. 1, where a photon-number-resolving (PNR) detector to discriminate the photon number of $n = 0$, $n = 1$, $n = 2$, $n \geq 3$ is used. For simplicity, one can calibrate the setup to satisfy

$$\eta_{BS}\eta_D = 1 - \eta_{BS}, \tag{5}$$

where η_{BS} is the transmittance of the beam splitter and η_D is the detection efficiency of the PNR detector in Fig. 1. Clearly, based on Eq. (5), the PND at P4 is the same to that at P3, where Pi means position i ($i = 1, 2, 3, 4$) in Fig. 1.

A. PNR detector without detection noise

In the following, the PNR detector is assumed to be noiseless. Suppose $P^{s(d)}(n_4)$ denote the PND for signal (decoy) source at P4, and $D^{s(d)}(m)$ denote the PND for signal (decoy) source at P3. Clearly, one has

$$\begin{aligned} a_n &= P^d(n_4 = n) = D^d(m = n), \\ a'_n &= P^s(n_4 = n) = D^s(m = n), \end{aligned} \tag{6}$$

where $n = 0,\ 1,\ 2, \cdots$.

Suppose the total number of untrusted optical pulses is N, while the number of signal (decoy) pulses is $N^{s(d)}$, correspondingly. Let $k_m^{s(d)}$ denote the number of detected signal (decoy) pulses in the PNR detector which records m photoelectrons ($m = 0, 1, 2, \geq 3$). Using *random sampling theory* [25], $D^s(m) \in [k_m^s/N^s - \varepsilon', k_m^s/N^s + \varepsilon']$ with a confidence level $1 - 2\exp(-N^s\varepsilon'^2/2)$ for signal pulses, and $D^d(m) \in [k_m^d/N^d - \varepsilon, k_m^d/N^d + \varepsilon]$ with a confidence level $1 - 2\exp(-N^d\varepsilon^2/2)$ for decoy pulses can be estimated. Then, from Eq. (6), one gets

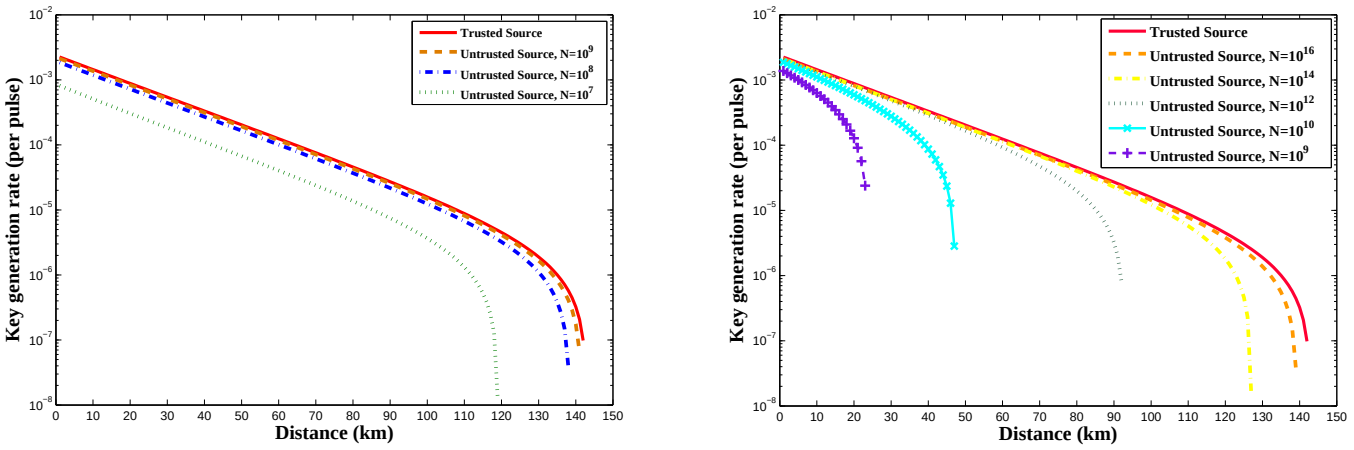
$$\begin{aligned} a'^L_m &= \frac{k_m^s}{N^s} - \varepsilon', \quad a'^U_m = \frac{k_m^s}{N^s} + \varepsilon', \\ a^L_m &= \frac{k_m^d}{N^d} - \varepsilon, \quad a^U_m = \frac{k_m^d}{N^d} + \varepsilon, \ (m = 0, 1, 2) \end{aligned} \tag{7}$$

with a confidence level $1 - 2\exp(-N^s\varepsilon'^2/2)$ for signal pulses and $1 - 2\exp(-N^d\varepsilon^2/2)$ for decoy pulses, respectively. Thus, after obtaining $k_m^{s(d)}$ by the PNR detector, one can estimate the value of $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$ with a quantitative confidence level.

TABLE I: The simulation parameters for Figs. 2 and 3.

η_D	η_{BS}	η_{Bob}	α	Y_0	e_{det}	e_0
0.15	0.87	0.045	0.21	1.7×10^{-6}	3.3%	0.5

For testing the effects of statistical fluctuation without considering the detection noise, we choose an untrusted source of Poissonian statistics to perform simulations based on the vacuum+weak decoy state protocol. Fig. (2a) shows the numerical simulation results for trusted source, and untrusted source with the passive scheme in Fig. 1, where a beam splitter and a noiseless PNR detector are used to verify the parameters



(a) (b)

FIG. 2: (color online) Simulation result of the vacuum+weak decoy state protocol for trusted and untrusted source: (a) with finite data size $N = 10^9, 10^8, 10^7$, respectively, based on the scheme in Fig. 1, where a beam splitter and a noiseless PNR detector which can discriminate vacuum, one-photon and two-photon states are used to verify the parameters $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$ with a confidence level $1 - 10^{-6}$; (b) with finite data size $N = 10^{16}, 10^{14}, 10^{12}, 10^{10}, 10^9$, respectively, based on the passive scheme in [18], where a beam splitter and noiseless PNA, are used to verify the lower bound of the probability of "untagged bits" with a confidence level $1 - 10^{-6}$, after which one can calculate the secure key rate by Eq. (A1) in Appendix A [16].

$\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$. Here, the average photon number (APN) of Poissonian source at P1 is 7.66×10^6. The attenuation η_s and η_d are set to be 5×10^{-7} and 1×10^{-7}, respectively, so that the APN for signal (decoy) state at P4 is $\mu_s = 0.5$ ($\mu_d = 0.1$). The photoelectron detection generated by PNR detector is simulated using Monte Carlo method, and $N = 10^7, 10^8$ and 10^9 of measurements are run. Other experimental parameters are cited from the GYS experiment [26] as shown in Table I, where η_{Bob} is the efficiency of Bob's detection, Y_0 is dark count rate of Bob's detector and e_{det} (e_0) is the probability that a photon (dark count) hit the erroneous detector in Bob's side. To compare the performance of the scheme in Fig. 1 with the passive scheme proposed in [18], where a beam splitter with transmittance η_{BS} and a noiseless photodiode with efficiency η_D are used to verify the lower bound of the probability of "untagged bits" (see Appendix A), Fig. (2b) shows the numerical simulation results for trusted source, and untrusted source with the scheme in [18]. All the experimental parameters are chosen to be the same to that of Fig. (2a).

B. PNR detector with additive detection noise

Given a PNR detector with an independent additive detection noise y, the detected photoelectron number m', and the photon number m at P3 satisfy

$$m' = m + y. \tag{8}$$

One can calculate the lower and upper bound of photon number distribution $D(m)$ ($m = 0, 1, 2$) at P3 based on the photoelectron distribution of $P(m')$ with a high confidence level, given that the distribution of the detection noise $N(y)$ is known by Alice.

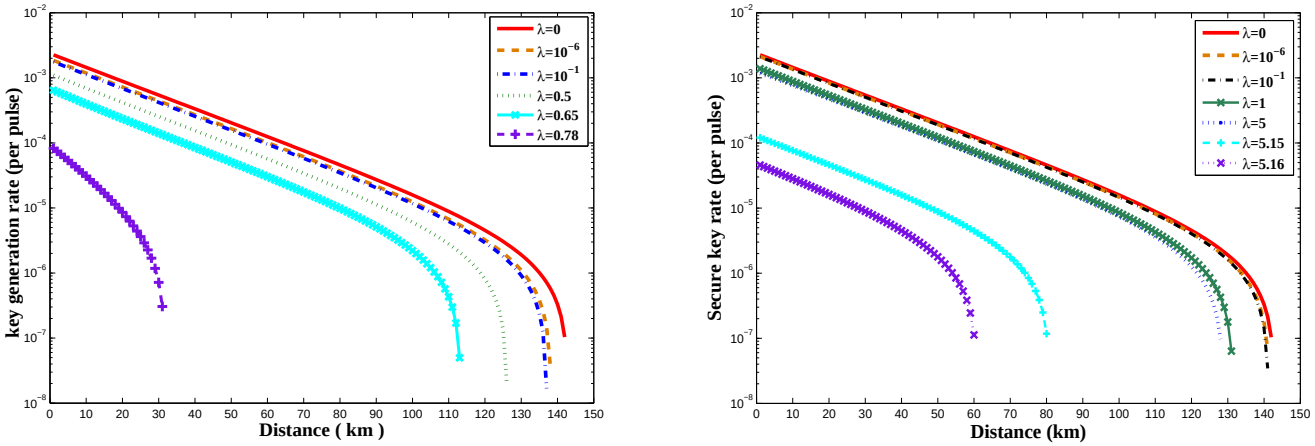
The dark count is the main kind of detection noise for the PNR detector such as time multiplexing detector (TMD) [27, 28], transition-edge sensor (TES) [29], or a threshold detector together with a variable attenuator [30, 31]. In case of independent Poisson statistics noise (e.g. dark counts), the probability of detecting m' photoelectrons is

$$P(m') = \sum_{d=0}^{m'} \frac{e^{-\lambda}\lambda^{m'-d}}{(m'-d)!} D(d), \tag{9}$$

where $N(y = d) = e^{-\lambda}\lambda^d/d!$ is the probability of that d dark counts occur in the PNR detector, and λ is the average dark-count rate of noise. Based on Eq. (9), one easily calculate

$$\begin{aligned} D(m=0) &= P(m'=0)e^{\lambda}, \\ D(m=1) &= P(m'=0)e^{\lambda}(-\lambda) + P(m'=1)e^{\lambda}, \\ D(m=2) &= P(m'=0)e^{\lambda}\frac{\lambda^2}{2} + P(m'=1)e^{\lambda}(-\lambda) \\ &\quad + P(m'=2)e^{\lambda}. \end{aligned} \tag{10}$$

Let $k_{m'}^{s(d)}$ denote the number of detected signal (decoy) pulses by Alice at P3, given that PNR detector records m' photoelectrons. Using *random sampling theory* [25], one has $P^s(m') \in [k_{m'}^s/N^s - \varepsilon', k_{m'}^s/N^s + \varepsilon']$ for signal source and $P^d(m') \in [k_{m'}^d/N^d - \varepsilon, k_{m'}^d/N^d + \varepsilon]$ for decoy source with a confidence level $1 - 2\exp(-N^s\varepsilon'^2/2)$ and $1 - 2\exp(-N^d\varepsilon^2/2)$,



(a) (b)

FIG. 3: (color online) Simulation result of the vacuum+weak decoy state protocol for untrusted source based on the scheme in Fig. 1 in two cases: (a) the data size is $N = 10^8$ and the APN of independent Poissonian detection noise of the PNR detector (efficiency: η_D) is $\lambda = 0, 10^{-6}, 10^{-1}, 0.5, 0.65, 0.78$, respectively; (b) the data size is $N = 10^8$ and the APN of independent Poissonian detection noise of the PNR detector (efficiency: η_D) is $\lambda = 0, 10^{-6}, 10^{-1}, 1, 5, 5.15, 5.16$, respectively. The experimental parameters are the same as Table I, and the confidence level of both cases is $1 - 10^{-6}$.

respectively. Combing Eqs. (6) and (10), one yields

$$
\begin{aligned}
a'_0 &\geq e^{\lambda}\left(\frac{k^s_{m'=0}}{N^s} - \varepsilon'\right) = {a'_0}^L,\\
a'_1 &\geq -\lambda e^{\lambda}\left(\frac{k^s_{m'=0}}{N^s} + \varepsilon'\right) + e^{\lambda}\left(\frac{k^s_{m'=1}}{N^s} - \varepsilon'\right) = {a'_1}^L,\\
a'_2 &\geq \frac{\lambda^2}{2}e^{\lambda}\left(\frac{k^s_{m'=0}}{N^s} - \varepsilon'\right) - \lambda e^{\lambda}\left(\frac{k^s_{m'=1}}{N^s} + \varepsilon'\right)\\
&\quad + e^{\lambda}\left(\frac{k^s_{m'=2}}{N^s} - \varepsilon'\right) = {a'_2}^L,\\
a_0 &\leq e^{\lambda}\left(\frac{k^d_{m'=0}}{N^s} + \varepsilon\right) = a^U_0,\\
a_1 &\leq -\lambda e^{\lambda}\left(\frac{k^d_{m'=0}}{N^s} - \varepsilon\right) + e^{\lambda}\left(\frac{k^d_{m'=1}}{N^s} + \varepsilon\right) = a^U_1,\\
a_2 &\leq \frac{\lambda^2}{2}e^{\lambda}\left(\frac{k^d_{m'=0}}{N^s} + \varepsilon\right) - \lambda e^{\lambda}\left(\frac{k^d_{m'=1}}{N^s} - \varepsilon\right)\\
&\quad + e^{\lambda}\left(\frac{k^d_{m'=2}}{N^s} + \varepsilon\right) = a^U_2.
\end{aligned}
\tag{11}
$$

For testing the effects of detection noise, we choose an untrusted source of Poissonian statistics to perform simulations based on the vacuum+weak decoy state protocol with the passive scheme in Fig. 1. The untrusted source is of Poissonian statistics with APN $\mu = 7.66 \times 10^6$ at P1, and the attenuation η_s and η_d are set to be 5×10^{-7} and 1×10^{-7}, respectively. The other experimental parameters are cited from Table I. The photoelectron detection and additive Poissonian noise of the PNR detector at P3 in Fig. 1 are simulated using Monte Carlo method, and $N = 10^8$ and 10^9 of measurements are run for Figs. (3a) and (3b), respectively.

More generally, when the random positive detection noise y with the probability $N(y)$ is known to Alice, one can still estimate the parameters $\{{a'_0}^L, a^U_0, {a'_1}^L, a^U_1, {a'_2}^L, a^U_2\}$ as shown in Appendix B.

IV. AN EXPERIMENTAL REALIZATION OF PNR DETECTOR

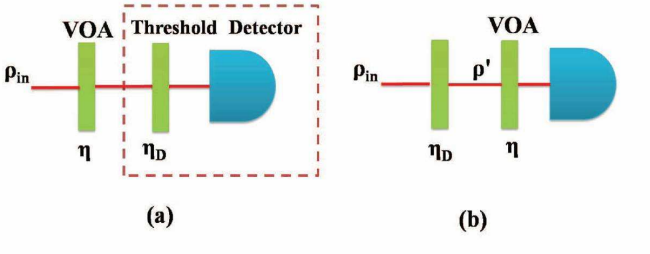


FIG. 4: (a) A threshold detector (modeled by an attenuator with transmittance η_D and an ideal threshold detector) combined with a variable optical attenuator (transmittance: η) can realize a PNR detector [31]. (b) An equivalent model to (a), which means the two models will produce the same PND at the ideal detector if given the same input source ρ_{in}.

The PNR detector can be realized by a variable optical attenuator (VOA) combined with a practical threshold detector (such as single-photon detector) as shown in Fig. 4(a) [31], which is equivalent to the model in Fig. 4(b). Suppose the state of input source is $\rho_{in} = \sum_{n=0}^{\infty} p_n |n\rangle\langle n|$. In Fig. 4(b), after

passing through an attenuator with efficient η_D, the state of the source becomes

$$\rho' = \sum_{n=0}^{\infty} p'_n |n\rangle\langle n|,$$

where $p'_n = \sum_{m=n}^{\infty} p_m \binom{m}{n} \eta_D^n (1-\eta_D)^{m-n}$. When Eq. (5) holds, one has

$$p'^{s}_n = a'_n,\ p'^{d}_n = a_n. \tag{12}$$

Then the source passes through the VOA with efficiency η, and the probability that the detector dose not click can be calculated as $p(\eta) = \sum_{n=0}^{\infty}(1-\eta)^n p'_n$ [31]. When we take the dark count of the threshold detector into account, it can be calculated as

$$p(\eta) = (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta)^n p'_n,$$

where the ϵ is the dark count rate of the detector. If Alice varies the transmittance of the VOA $\eta = \{\eta_1, \cdots, \eta_M\}$, she has a set of linear equations

$$p(\eta_i) = (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta_i)^n p'_n,\ (i = 1, \cdots, M). \tag{13}$$

When she employs an infinity number of possible transmittance $\eta \in [0,\ 1]$, she can always estimate any finite number of probabilities p'_n with arbitrary precision by solving Eqs. (13). However it is not necessary for our purpose where we mainly concern the probability of vacuum, one photon and two photon states. In this case, only three different transmittances $\eta = \{\eta_0,\ \eta_1,\ \eta_2\}$ are needed [31]. Then Alice has

$$\begin{aligned} p(\eta_0) &= (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta_0)^n p'_n, \\ p(\eta_1) &= (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta_1)^n p'_n, \\ p(\eta_2) &= (1-\epsilon)\sum_{n=0}^{\infty}(1-\eta_2)^n p'_n. \end{aligned} \tag{14}$$

One can choose $\eta_0 = 1$ so that

$$p(\eta_0 = 1) = (1-\epsilon)p'_0. \tag{15}$$

Then one has

$$\begin{aligned} \frac{p(\eta_1)}{1-\epsilon} &\geq p'_0 + (1-\eta_1)p'_1, \\ \frac{p(\eta_1)}{1-\epsilon} &\leq p'_0 + (1-\eta_1)p'_1 + (1-\eta'_1)^2(1-p'_0-p'_1), \end{aligned}$$

from which the upper and lower bounds for p'_1 can be calculated as

$$\begin{aligned} p'_1 &\leq \frac{p(\eta_1) - p(\eta_0)}{(1-\epsilon)(1-\eta_1)} = \overline{p'_1}, \\ p'_1 &\geq \frac{p(\eta_1) - p(\eta_0)[1-(1-\eta_1)^2] - (1-\epsilon)(1-\eta_1)^2}{(1-\epsilon)[1-\eta_1-(1-\eta_1)^2]} \\ &= \underline{p'_1}. \end{aligned} \tag{16}$$

In a similar way, one has

$$\begin{aligned} \frac{p(\eta_2)}{1-\epsilon} &\geq p'_0 + (1-\eta_2)p'_1 + (1-\eta_2)^2 p'_2 \\ &\geq p'_0 + (1-\eta_2)\underline{p'_1} + (1-\eta_2)^2 p'_2 \\ \frac{p(\eta_1)}{1-\epsilon} &\leq p'_0 + (1-\eta_2)p'_1 + (1-\eta_2)^2 p'_2 \\ &\quad + (1-\eta_2)^3(p'_3 + p'_4 + p'_5 + \cdots) \\ &\leq [1-(1-\eta_2)^3]p'_0 + [1-\eta_2-(1-\eta_2)^3]\overline{p'_1} \\ &\quad + [(1-\eta_2)^2 - (1-\eta_2)^3]p'_2 - (1-\eta_2)^3, \end{aligned}$$

from which the upper and lower bounds for p'_2 can be estimated as

$$\begin{aligned} p'_2 &\leq \frac{p(\eta_2) - p(\eta_0) - (1-\epsilon)(1-\eta_2)\underline{p'_1}}{(1-\epsilon)(1-\eta_2)^2} = \overline{p'_2} \\ p'_2 &\geq \frac{p(\eta_2) - [1-(1-\eta_2)^3]p(\eta_0) - (1-\varepsilon)[1-\eta_2-(1-\eta_2)^3]\overline{p'_1} - (1-\varepsilon)(1-\eta_2)^3}{(1-\varepsilon)[(1-\eta_2)^2 - (1-\eta_2)^3]} = \underline{p'_2}. \end{aligned} \tag{17}$$

In conclusion, based on the recorded data $\{p(\eta_0),\ p(\eta_1),\ p(\eta_2)\}$, Alice can estimated the parameters $\{a'^{L}_0,\ a^{U}_0,\ a'^{L}_1,\ a^{U}_1,\ a'^{L}_2,\ a^{U}_2\}$ as in Eqs. (12) and (15-17). The scheme in Fig. (4) can be easily realized with current technology. As for the effect of statistical fluctuation, one can use the *Ran-*

dom Sampling Theory as before to consider the fluctuation of the $\{p(\eta_0),\ p(\eta_1),\ p(\eta_2)\}$ with a confidence level so that we still can bound $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$.

V. DISCUSSION AND CONCLUSION

The results in Fig. 2 show that: (i) the performance of QKD system with untrusted source is very close to that of trusted source, when the source is monitored efficiently and the data size is large enough; (ii) finite data size has negative effect on the secure key rate; (iii) the method in [18] is more sensitive to statistical fluctuation and needs a larger data size than our method.

In the passive scheme proposed in [18] (see Fig. 5 in Appendix A), Alice uses a threshold detection to monitor the frequency of "untagged bits" in untrusted source, from which the lower bound of the probability of "untagged bits" can be estimated with a confidence level . When the confidence level is set to be constant (e.g. $1-10^{-6}$), the estimation resolution ε for the probability of "untagged bits" is only decided by the data size N (ignoring the effect of detection noise), where the confidence level is $1-2\exp(-N\varepsilon^2/4)$ [18]. However, the secure key rate in [18] is quite sensitive to the estimation resolution ε, and will reduce greatly when ε increases (see Fig. 6 in Appendix A). When the data size N decrease, the resolution ε has to increase to keep the constant confidence level, and thus the key rate will reduce greatly.

While in the scheme shown in Fig. 1, Alice uses a PNR detector to monitor the counts of vacuum, one-photon, and two-photon states for signal and decoy source, respectively. Because of the low intensity of the output pulses at P4 (e.g. $\mu_s = 0.5$, $\mu_d = 0.1$), the vacuum, one-photon, and two-photon pulses are dominant in pulses, and Alice can gain most of the information about the statistics of the untrusted source at P4 based on the recorded data at P3. In our scheme, six parameters are monitored, and more information is gained than the scheme in [18]. Mathematically, formulas shown by Eqs. 3-(4) are not so sensitive to the estimation resolution of $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$ compared to that in [18], so that it does not require a very large data size to work efficiently as shown in Fig. (2a). When the data size $N \geq 10^8$, the performance of the scheme is very close to that of trusted source. In asymptotic case where Alice sends infinitely long bit sequence ($N \sim \infty$), the performance will be the same to that of trusted source as shown in Appendix C, which means this passive method will not reduce the efficiency of the system without eavesdropping.

The results in Fig. 3 show that: (i) given a PNR detector with the same dark count rate, the performance of a system with untrusted source will be better when the data size increase; (ii) given the same data size, the performance of a system with untrusted source will reduce when the dark count rate increase. Performance of the scheme in Fig. 1 is quite sensitive to the detection noise of the PNR detector. It is shown that when the data size $N \geq 10^8$ and dark count rate of the PNR detector $\lambda \leq 0.5$ which are realizable by current techniques [27–30], this scheme can still work efficiently.

In conclusion, we propose an experimental scheme to verify the key parameters needed in [21, 22] with a quantitative confidence level. The practical issues due to detection noise and finite data size fluctuation are concerned. The simulation results show that our scheme can work efficiently.

Acknowledgments

This work is supported by the Key Project of National Natural Science Foundation of China (Grant No. 60837004) and National Hi-Tech Research and Development (863) Program.

Appendix A: Passive scheme method in [18]

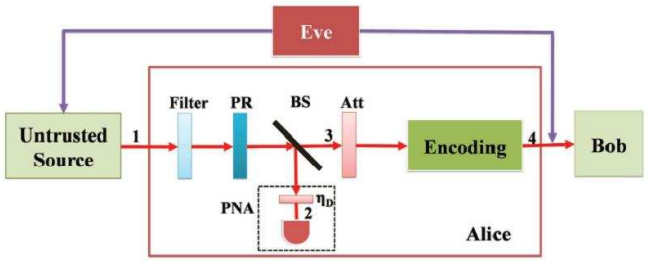


FIG. 5: (color online) The model of the passive scheme in [17–19]. The untrusted source prepared by Eve passes through a low-bandwidth optical filter, and a phase randomizer (PR). Then, a beam splitter (BS) with transmittance η_{BS} is used to separate it into two beams: one goes to a photon-number-analyzer (PNA) with efficiency η_D, and the other is attenuated with an attenuator (Att) with efficiency $\eta_{s(d)}$ for signal (decoy) state and encoded before it is sent out of Alice's side.

The passive method in [18] is shown in Fig. 5, where a beam splitter and a photon number analyzer (PNA) are used to record the frequency of "untagged bits" experimentally. Define the pulses with photon number $M \in [M_{\min}, M_{\max}]$ at position 3 in Fig. 4 as "untagged bits". For simplicity, one can set $\eta_{BS}\eta_D = 1-\eta_{BS}$.

Assume that N pulses are sent from Alice to Bob. Alice and Bob do not know which bits are untagged. Let $N_{untagged}$ denote the number of detected pulses by the PNA given that the recorded photoelectron number at position 2 belongs to $[M_{\min}, M_{\max}]$, and $\Delta = N_{untagged}/N$. From the recorded data in PNA, one can estimate that at least $(1-\Delta-\varepsilon)N$ pulses are "untagged bits" with a confidence $1-2\exp(-N\varepsilon^2/4)$ where ε is a small positive parameter [18].

Alice can measure the overall gain $Q_{s(d)}$ and QBER $E_{s(d)}$ for signal (decoy) pulses, respectively, while she doesn't known the gain and QBER for "untagged bits". The upper and lower bounds of the gain of "untagged bits" for signal (decoy) source can be estimated as

$$\overline{Q_{s(d)}} = \frac{Q_{s(d)}}{1-\Delta-\varepsilon},\ \underline{Q_{s(d)}} = \max\left\{0, \frac{Q_{s(d)}-\Delta-\varepsilon}{1-\Delta-\varepsilon}\right\}.$$

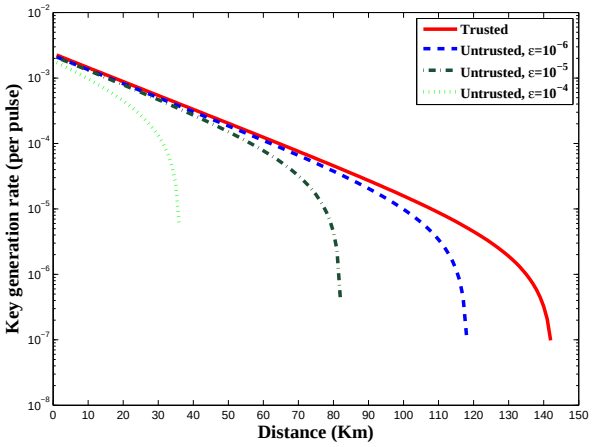


FIG. 6: (color online) Simulation result of the vacuum+weak decoy state protocol for trusted and untrusted source with different estimation resolution $\varepsilon = 10^{-6}$, 10^{-5}, 10^{-4}, respectively. Based on the passive shown in Fig. 4, a beam splitter and a noiseless PNA are used to verify the lower bound of the probability of untagged bits. Experimental parameters are cited from Table I.

The upper and lower bound for the QBER of "untagged bits" can be estimated as

$$\overline{Q_s E_s} = \frac{Q_s E_s}{1-\Delta-\varepsilon},\ \underline{Q_s E_s} = \max\left\{0, \frac{Q_s E_s - \Delta - \varepsilon}{1-\Delta-\varepsilon}\right\},$$

for signal states, and

$$\overline{Q_d E_d} = \frac{Q_d E_d}{1-\Delta-\varepsilon},\ \underline{Q_d E_d} = \max\left\{0, \frac{Q_d E_d - \Delta - \varepsilon}{1-\Delta-\varepsilon}\right\},$$

for decoy states. For untagged bits, one can show that the upper and lower bounds of the probability that the output photon number at position 4 is n for signal (decoy) pulses are:

$$\overline{P_n^{s(d)}} = \begin{cases} (1-\eta_{s(d)})^{M_{\min}} & n=0, \\ \binom{M_{\max}}{n}\eta_{s(d)}^n (1-\eta_{s(d)})^{M_{\max}-n} & 1 \le n \le M_{\max}, \\ 0 & n > M_{\max}, \end{cases}$$

$$\underline{P_n^{s(d)}} = \begin{cases} (1-\eta_{s(d)})^{M_{\max}} & n=0, \\ \binom{M_{\min}}{n}\eta_{s(d)}^n (1-\eta_{s(d)})^{M_{\min}-n} & 1 \le n \le M_{\min}, \\ 0 & n > M_{\min}, \end{cases}$$

under condition that $M_{\max}\eta_{s(d)} < 1$.

When the lower bounds of the probability of "untagged bits" is known by Alice, the secure key rate for vacuum+weak decoy state protocol with untrusted source is [16]

$$R = \frac{1}{2}\left\{-Q_s H_2(E_s) + (1-\Delta-\varepsilon)\underline{Q_1^s}[1-H_2(\overline{e_1^s})]\right\}, \quad \text{(A1)}$$

where

$$\underline{Q_1^s} = \frac{\underline{P_1^s}}{\overline{P_1^d}\underline{P_2^s} - \underline{P_1^s}\overline{P_2^d}} \times \left\{\underline{Q_d P_2^s} - \overline{Q_s}\,\overline{P_2^d} + \underline{P_0^s}\,\overline{P_2^d} Q_0 - \overline{P_0^d}\underline{P_2^s} Q_0 - \frac{(M_{\max}-M_{\min})(1-\eta_d)^{M_{\max}-M_{\min}-1}\underline{P_2^s}}{[M_{\min}+1]!}\right\},$$

and

$$\overline{e_1^s} = \frac{\overline{E_s Q_s} - \underline{P_0^s E_0 Q_0}}{\underline{Q_1^s}},$$

under some condition.

For testing the effects of ε onto the secure key rate, we choose an untrusted source of Poissonian statistics to perform the simulations based on the vacuum+weak decoy state protocol.Suppose the untrusted source is of Poissonian with APN 7.66×10^6 at position 1 of Fig. 4. Set $\eta_s = 5 \times 10^{-7}$, and $\eta_d = 1 \times 10^{-7}$. The other experimental parameters are chosen to be same as Table I. The values of $M_{\max}$ and $M_{\min}$ are chosen to be constant. The results in Fig. 5 show that the final key rate is very sensitive to the value of ε.

Suppose Alice has a noiseless PNA, and the estimation confidence level is set to be constant

$$1 - 2\exp^{-N\varepsilon^2/4} = 1 - 10^{-6}. \quad \text{(A2)}$$

The estimation resolution ε for the probability of "untagged bits" is only decided by the data size N. When the data size N decrease, the resolution ε has to increase to keep the constant confidence level, and thus the key rate will reduce greatly as has been shown in Fig. 2(b).

Appendix B: General positive detection noise

Generally, when the random positive detection noise y with the probability $N(y)$ is known to Alice where $N(y<0)=0$, one has

$$\begin{aligned} P(m'=0) &= N(y=0)D(m=0), \\ P(m'=1) &= N(y=0)D(m=1) + N(y=1)D(m=0), \\ P(m'=2) &= N(y=0)D(m=2) + N(y=1)D(m=1) \\ &\quad + N(y=2)D(m=0). \end{aligned} \quad \text{(B1)}$$

Thus, combine the results in Eqs. (6) and (B1), one has

$$
\begin{aligned}
a_0' &\geq \frac{k^s_{m'=0}/N^s - \varepsilon'}{N(y=0)}, \\
a_1' &\geq \frac{\left(k^s_{m'=1}/N^s - \varepsilon'\right)N(y=0) - \left(k^s_{m'=0}/N^s + \varepsilon'\right)N(y=1)}{N^2(y=0)}, \\
a_2' &\geq \frac{k^s_{m'=2}/N^s - \varepsilon'}{N(y=0)} - \frac{k^s_{m'=1}/N^s + \varepsilon'}{N^2(y=0)}N(y=1) \\
&\quad + \frac{k^s_{m'=0}/N^s - \varepsilon'}{N^3(y=0)}N^2(y=1) - \frac{k^s_{m'=0}/N^s + \varepsilon'}{N^2(y=0)}N(y=2), \\
a_0 &\leq \frac{k^d_{m'=0}/N^d + \varepsilon}{N(y=0)}, \\
a_1 &\leq \frac{\left(k^d_{m'=1}/N^d + \varepsilon\right)N(y=0) - \left(k^d_{m'=0}/N^d - \varepsilon\right)N(y=1)}{N^2(y=0)}, \\
a_2 &\leq \frac{k^d_{m'=2}/N^d + \varepsilon}{N(y=0)} - \frac{k^d_{m'=1}/N^d - \varepsilon}{N^2(y=0)}N(y=1) \\
&\quad + \frac{k^d_{m'=0}/N^d + \varepsilon}{N^3(y=0)}N^2(y=1) - \frac{k^d_{m'=0}/N^d - \varepsilon}{N^2(y=0)}N(y=2). \quad \text{(B2)}
\end{aligned}
$$

Therefor, once the distribution of the noise is known, the secure key rate can be estimated given the bounds of $\{a_0'^L, a_0^U, a_1'^L, a_1^U, a_2'^L, a_2^U\}$.

Appendix C: Asymptotic case of method in [21]

In the asymptotic case, Alice sends infinitely long bit sequence ($N \sim \infty$). Therefore we can consider ε, $\varepsilon' \sim 0$ in Eqs. (7), (11) or (B2) while still have confidence level to be 1. Suppose the untrusted source is Poissonian with APN $\mu_{s(d)}$ for signal (decoy) pulses at P4, then one has

$$
\begin{aligned}
&a_0^U = \exp(-\mu_d),\ a_1^U = \mu_d \exp(-\mu_d),\ a_2^U = \mu_d^2/2 \exp(-\mu_d), \\
&a_0'^U = \exp(-\mu_s),\ a_1'^U = \mu_s \exp(-\mu_s),\ a_2'^U = \mu_s^2/2 \exp(-\mu_s).
\end{aligned}
$$

Then one can estimate

$$
\begin{aligned}
Q_1^s = Q_s\Delta_1^s &\geq \frac{a_1'^L\left(a_2'^L Q_d - a_2^U Q_s - a_2'^L a_0^U Q_0 + a_2^U a_0'^L Q_0\right)}{a_1^U a_2'^L - a_1'^L a_2^U} \\
&= \frac{\mu_s}{\mu_s^2 - \mu_s\mu_d}\left(Q_d e^{-\mu_d} - Q_s e^{-\mu_s}\frac{\mu_d^2}{\mu_s^2} - \frac{\mu_s^2 - \mu_d^2}{\mu_s^2}Q_0\right),
\end{aligned}
$$

which is exactly the same to the case of trusted source (see Eq. (35) in [24]).

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, Bangalore, India, 1984).
[4] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[7] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004)
[8] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[9] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[10] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[11] H. K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[12] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[13] www.idquantique.com.
[14] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, New J. Phys. **4**, 41 (2002).
[15] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[16] Y. Zhao, B. Qi, and H. K. Lo, Phys. Rev. A **77**, 052327 (2008).
[17] X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, Opt. Lett. **33**, 2077 (2008).
[18] Y. Zhao, B. Qi, H. K. Lo, and L. Qian, arXiv: quant-ph/0905.4225 (2009).
[19] X. Peng, B. Xu, and H. Guo, arXiv: quant-ph/0908.1461 (2009).
[20] M. O. Scully and M. S. Zubairy, *Quantum Optics* (Cambridge, 1997).
[21] X. B. Wang, C. Z. Peng, J. Zhang, L. Yang and J. W. Pan, Phys. Rev. A **77**, 042311 (2008).
[22] X. B. Wang, L. Yang, C. Z. Peng, and J. W. Pan, New J. Phys. **11**, 075006 (2009).
[23] X. B. Wang, Phys. Rev. A **72**, 012322 (2005).
[24] X. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005).
[25] J. V. Uspensky, *Intruduction to mathematical probability* (McGraw-Hill, 1937).
[26] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[27] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, and I. A. Walmsley, Opt. Lett. **28**, 2387 (2003).
[28] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, J. Mod. Opt. **51**, 1499 (2004).
[29] D. Rosenberg, A. E. Lita, A. J. Miller,and S. W. Nam, Phys. Rev. A **71**, 061803 (2005).
[30] G. Zambra, A. Andreoni, M. Bondani, M. Gramegna, M. Genovese, G. Brida, A. Rossi, and M. G. A. Paris, Phys. Rev. Lett. **95**, 063602 (2005).
[31] T. Moroder, M. Curty, and N. Lütkenhaus, New J. Phys. **11**, 045008 (2009).