Quantum Information and Computation, Vol. 12, No. 7&8 (2012) 0630–0647
© Rinton Press

THE SECYRITY OF SARG04 PROTOCOL IN PLUG AND PLAY QKD SYSTEM WITH AN UNTRUSTED SOURCE

BINGJIE XU, XIANG PENG, and HONG GUO
State Key Laboratory of Advanced Optical Communication Systems and Networks
and Institute of Quantum Electronics, School of Electronics Engineering and Computer Science
Peking University, Beijing 100871, PR China

Received October 27, 2011
Revised April 1, 2012

The SARG04 protocol is one of the most frequently used protocol in commercial plug-and-play quantum key distribution (QKD) system, where an eavesdropper can completely control or change the photon number statistics of the QKD source. To ensure the security of SARG04 protocol in plug-and-play QKD system with an unknown and untrusted source, the bounds of a few statistical parameters of the source need to be monitored. An active or a passive source monitor schemes are proposed to verify these parameters. Furthermore, the practical issues due to statistical fluctuation and detection noise in the source monitoring process are quantitatively analyzed. Our simulation results show that the passive scheme can be efficiently applied to plug-and-play system with SARG04 protocol.

Keywords: Quantum Cryptography, Quantum Key Distribution, Practical Security Loophole, Untrusted Source Problem
Communicated by: S Braunstein & R Laflamme

1 Introduction

Quantum key distribution (QKD) provides a means of sharing a secret key between two parties (Alice and Bob) in the presence of an eavesdropper (Eve). The single-photon (e.g. BB84 [1] and SARG04 [2]), entanglement-based (e.g. E91 [3]) and continuous variable (e.g. GG02 [4]) QKD protocols have proved to be unconditionally secure under ideal (source, channel, detection and postprocessing) assumptions [5, 6, 7, 8, 9, 10, 11, 12]. In practical QKD systems, the security assumptions are not completely satisfied and security loopholes exist [13]. Real implementations of QKD may deviate from the ideal models in security proofs, such as laser with intensity fluctuation [14, 15], detectors with mismatched detection efficiency [16, 17, 18, 19, 20, 21], or detection blinding effect [22, 23, 24]. The unconditional security of practical QKD systems will be compromised, if these loopholes are not included in general security analysis or no counter measures are made. For instance, the ideal security proof for the BB84 protocol was given when a single-photon source was assumed [6], while highly attenuated laser source is often used in real experiment, where the source sometimes produces multi-photon states. Due to the channel loss and these multi-photon states, Eve can perform the photon-number-splitting (PNS) attack [25]. Lately, more general security analysis for the BB84 protocol with weak coherent laser source and semi-realistic models were given [7, 8].

Furthermore, several methods (such as decoy state [26, 27, 28, 29, 30, 31, 32] and SARG04 [2] protocols) have been proposed to fight against the multi-photon loophole.

The security loophole considered in this paper is the untrusted source problem [33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43]. In the standard security analysis of some protocols (such as BB84, decoy state, and SARG04 protocols), the photon number distribution (PND) of the QKD source is assumed to be fixed and known to Alice and Bob, which is defined as a trusted source. However, in a one-way QKD system, the intensity fluctuation from the laser source and the parameter fluctuation from the optical devices cause the assumption of the trusted source to fail [14, 15, 42]. More seriously in a two-way plug-and-play QKD system, Eve can even control or change the PND of the QKD source in principle, such that the source is unknown and untrusted [35]. To solve the untrusted source problem, the statistical characteristics of the QKD source need to be monitored in real experiment [36]. Many theoretical researches have been done on the security analysis for BB84 and decoy state protocols with an untrusted source [35, 37, 38, 39, 40, 41, 43], and the real-time source monitoring for both one-way and two-way systems have been demonstrated experimentally [36, 37, 42].

As is pointed out in [5], the SARG04 protocol is more robust than BB84 against the PNS attack, and has been applied in commercial plug-and-play QKD system [44]. However, this protocol also suffer from the untrusted source problem. In this paper, rigorous security analysis for the SARG04 protocol with an untrusted source is given, and the lower bound of secure key rate is devised if the ranges of a few statistical parameters of the untrusted source are known. Then, an active and a passive schemes are proposed to monitor these parameters. Furthermore, the practical issues of finite data size and detection noise are quantitatively analyzed.

2 Security analysis for the SARG04 Protocol with an untrusted source

The security key rate of the SARG04 protocol is [9]

$$R^{\mathrm{SARG04}}_{1+2-\mathrm{photon}} = -Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(Z_1|X_1)] + Q_2[1 - H_2(Z_2|X_2)], \tag{1}$$

where Q_μ and E_μ are the total count rate and quantum bit error rate (QBER) respectively, $Q_{1(2)}$ is the gain of the 1(2)-photon state, $Z_{1(2)}$ and $X_{1(2)}$ are random variables characterizing the phase and bit errors for the 1(2)-photon state respectively, $f(x)$ is the error correction efficiency, and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the Shannon entropy function. Suppose $p_{X1(2)}$ denote the probability that bit flip without phase flip occurs on 1(2)-photon state, $p_{Z1(2)}$ denote the probability that phase flip without bit flip occurs on 1(2)-photon state, and $p_{Y1(2)}$ denote the probability that both bit flip and phase flip occur on 1(2)-photon state. Let e_i (e_{pi}) denote the bit (phase) error rate for i-photon state, and $e_{1(2)} = p_{X1(2)} + p_{Y1(2)}, e_{p1(2)} = p_{Z1(2)} + p_{Y1(2)}$. For one-way postprocessing, it has been proved that [9],

$$\begin{aligned} &p_{X1} = e_1 - a,\ p_{Z1} = \frac{3}{2}e_1 - a,\ p_{Y1} = a,\\ &p_{X2} = e_2 - b,\ p_{Z2} \le xe_2 + g(x) - b,\ p_{Y2} = b, \end{aligned} \tag{2}$$

where $g(x) = [3 - 2x + (6 - 6\sqrt{2}x + 4x^2)^{1/2}]/6$, and $e_1/2 \le a \le e_1$, $0 \le b \le e_2$. Based on Eq. (2), one has $H_2(Z_1|X_1) \le H_2^{\max}(Z_1|X_1) = \max_a\{H_2(Z_1|X_1)\}$, and $H_2(Z_2|X_2) \le$

$H_2(Z_2) \leq H_2(e_{p2}^{opt})$ where $e_{p2}^{opt} = \max_x\{xe_2 + g(x)\}$. Then,

$$R_{1+2-\text{photon}}^{\text{SARG04}} \geq -Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2^{\max}(Z_1|X_1)] + Q_2[1 - H_2(e_{p2}^{opt})]. \qquad (3)$$

In order to calculate the final secure key rate, one needs a good estimation of $Q_{1(2)}$ and $e_{1(2)}$. There are a few methods to approach the target. One is proposed by GLLP [8], where all the losses and errors are assumed from the 1-photon and 2-photon states, and $Q_{1(2)}$ and $e_{1(2)}$ are overestimated. Another is the decoy state method [26, 27, 28, 29, 30, 31, 32], which can accurately estimate the parameters. Thus, we consider the SARG04 protocol combined with decoy state method [9]. A fundamental assumption in the decoy state protocol with a trusted source is $e_n = e_n^s = e_n^d$ and $Y_n = Y_n^s = Y_n^d$ [26], where Y_n is the yield of n-photon state and the superscript $s(d)$ means the signal (decoy) source. The optimal estimation, with applying infinite decoy states, converges to [9],

$$Y_n = \eta_n(\frac{e_{\text{det}}}{2} + \frac{1}{4}) + \frac{1}{2}(1 - \eta_n)Y_0, e_n = [\eta_n\frac{e_{\text{det}}}{2} + \frac{1}{4}(1 - \eta_n)Y_0]/Y_n, \qquad (4)$$

where η_n is the probability for n-photon state to arrive at Bob's detector, Y_0 is the dark count rate of Bob's detector, and e_{det} is the probability that a photon hit the erroneous detector in Bob's side. Then, one has $Q_{1(2)} = P_{1(2)}Y_{1(2)}$, where $P_{1(2)}$ is the probability for Alice to send out 1(2)-photon state in signal source, which is fixed and known to Alice and Bob with a trusted source.

However, the assumptions of $e_n^s = e_n^d$ and $Y_n^s = Y_n^d$ are broken if the source is untrusted [35, 34], and the results in Eq. (4) no longer hold. One needs new methods to estimate $Q_{1(2)}$ and $e_{1(2)}$ for QKD system with an untrusted source. Fortunately, the results in [35, 39] provide two new ways to estimate the bounds of Q_1 and e_1 for BB84 protocol combined with 3-intensity decoy state methods. However, in SARG04 protocol, both 1-photon and 2-photon states have positive contributions to the secure key rate and one needs a further estimation of Q_2 and e_2. We find that a modification of the method in [39] will fulfill this task. In the following, the lower bound of Q_2 is calculated for the SARG04 protocol combined with 4-intensity decoy state method in untrusted source scheme.

In a SARG04 protocol combined with 4-intensity decoy state method, Alice randomly sends four kinds of sources [30]: vacuum, decoy-1, decoy-2 and signal source, with probability p_0, p_1, p_2, and p', respectively. In the trusted source scheme, the source is controlled by Alice, and the quantum states of vacuum, decoy-1, decoy-2 and signal sources are expected to be $\rho_0 = |0\rangle\langle 0|$, $\rho_1 = \sum_{n=0}^{\infty} a_n |n\rangle\langle n|$, $\rho_2 = \sum_{n=0}^{\infty} b_n |n\rangle\langle n|$ and $\rho_s = \sum_{n=0}^{\infty} a'_n |n\rangle\langle n|$, respectively, where $\{a'_n,\ a_n,\ b_n\}$ are fixed and known. In the untrusted source scheme, the source is controlled and prepared by Eve (as shown in Fig. 1(a)), and $\{a'_n,\ a_n,\ b_n\}$ are unknown, which need to be monitored to estimate final secure key rate.

Suppose Alice sends M optical pulses to Bob totally. In a real experiment, one could observe the following parameters: N_s, $N_{d1(2)}$, and N_0 (the number of counts caused by signal, decoy-1(2), and vacuum sources, respectively). Then the count rates for signal, decoy-1(2), and vacuum sources are $Q_\mu = N_s/p'M$, $Q_{d1(2)} = N_{d1(2)}/p_{1(2)}M$, and $Y_0 = N_0/p_0M$, respectively. Denote the lower (upper) bound of $\{a'_n,\ a_n,\ b_n\}$ as $\{{a'_n}^{L(U)},\ a_n^{L(U)},\ b_n^{L(U)}\}$, which can be experimentally estimated by source monitor (see Section 3 for details) [43]. One can rigorously prove that (see Appendix A for details)

$$Q_1 \geq \frac{{a'_2}^L Q_\mu - a_2^U Q_{d1} - ({a'_2}^L a_0^U - {a'_0}^L a_2^U) Y_0}{{a'_2}^L a_1^U - {a'_1}^L a_2^U}, \tag{5}$$

$$Q_2 \geq \frac{{a'_3}^L Q_{d1} - a_3^U Q_\mu - ({a'_3}^L a_0^U - {a'_0}^L a_3^U) Y_0 - ({a'_3}^L a_1^U - {a'_1}^L a_3^U) \frac{Q_{d2} - b_0^L Y_0}{b_1^L}}{c({a'_3}^L a_2^U - {a'_2}^L a_3^U)}, \tag{6}$$

under conditions

$$\frac{{a'_k}^L}{a_k^U} \geq \frac{{a'_3}^L}{a_3^U} \geq \frac{{a'_2}^L}{a_2^U} \geq \frac{{a'_1}^L}{a_1^U}, \text{ (for all k} \geq 4), \tag{7}$$

$$c = 1 + \frac{a_3^U {a'_1}^L - {a'_3}^L a_1^U}{{a'_3}^L a_2^U - a_3^U {a'_2}^L} \frac{b_2^L}{b_1^L} > 0. \tag{8}$$

As in [9], we will compare the following two cases in the paper. When one consider the contribution from only 1-photon state for the SARG04 protocol, the final secure key rate is

$$R_{1-\text{photon}}^{\text{SARG04}} \geq -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2^{\max}(Z_1|X_1)]. \tag{9}$$

The parameters $\{{a'_0}^L,\ a_0^U,\ {a'_1}^L,\ a_1^U,\ {a'_2}^L,\ a_2^U\}$ need to be verified to estimate the gain of 1-photon state in Eq. (5), after which one has $e_1 \leq E_\mu Q_\mu / Q_1$. Then one can calculate the secure key rate as Eq. (9). This case is defined as **Case-1**. When one consider the contributions from both 1-photon and 2-photon states, the parameters $\{{a'_0}^L,\ b_0^L,\ a_0^U,\ {a'_1}^L,\ b_1^L,\ a_1^U,\ {a'_2}^L,\ b_2^L,\ a_2^U,\ {a'_3}^L,\ a_3^U\}$ need to be verified to estimate the gains of 1-photon and 2-photon states as in Eqs. (5) and (6). Then one can numerically choose the optimal values e_1 and e_2 under constrain $Q_\mu E_\mu \geq Q_1 e_1 + Q_2 e_2$ to lower bound the secure key rate in Eq. (3). This case is defined as **Case-2**. Note that the conditions in Eqs. (7) and (8) need to be verified experimentally. In the following, we propose an active and a passive source monitors to estimate these statistical parameters experimentally.

3 Active and Passive Source Monitors

The schematic diagram of a QKD system with an untrusted source is shown in Fig. 1(a), where the source is assumed to be completely controlled and prepared by Eve [35]. A source monitor is used to verify the statistical characteristics of the untrusted source in Alice's side. At least two schemes can realize the source monitor: an active scheme (shown in Fig. 1(b)) [35] and a passive scheme (shown in Fig. 1(c)) [36, 37, 38]. Suppose that $P_1(n)$ is the PND of the untrusted source at P1 (Pi means position i in Fig. 1), and $P_3(m, \eta)$ is the PND at P3 given that the attenuation coefficient of the variable optical attenuator (VOA) is η. Then $P_3(m, \eta)$ is a Bernoulli trasformation of $P_1(n)$ [36],

$$P_3(m, \eta) = \sum\nolimits_{n=m}^{\infty} P_1(n) \begin{pmatrix} n \\ m \end{pmatrix} \eta'^m (1 - \eta')^{n-m}, \tag{10}$$

where $\eta' = \eta$ for active scheme and $\eta' = \eta \times \eta_{BS}$ for passive scheme. Due to the definition of $\{a'_m, a_m, b_m\}$, one has

$$a'_m = P_3(m, \eta_s),\ a_m = P_3(m, \eta_{d1}),\ b_m = P_3(m, \eta_{d2}). \tag{11}$$

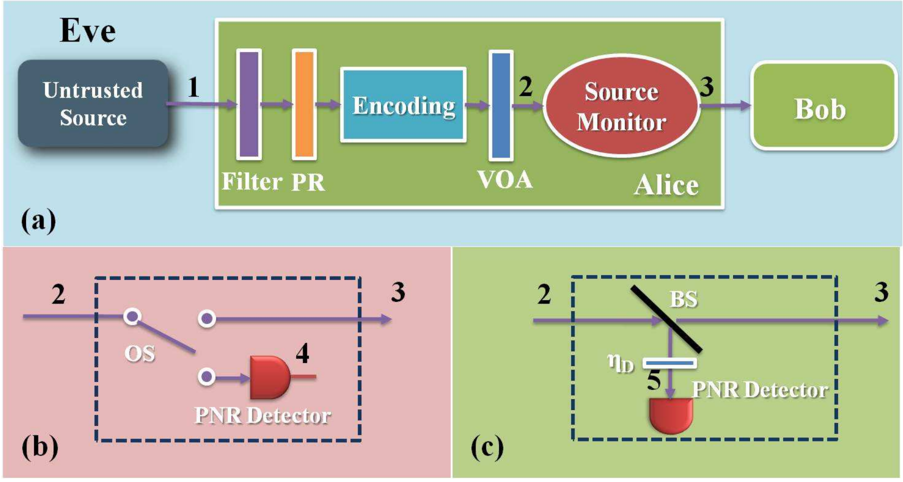

Fig. 1. (Color online) (a) Schematic diagram of the QKD system with an untrusted source. The untrusted source prepared at P1 by Eve, where Pi means position i ($i = 1, 2, 3, 4, 5$), passes through an optical filter, a phase randomizer (PR), an encoder and a variable optical attenuator (VOA) with attenuation coefficient $\eta = \eta_s$, η_{d1}, η_{d2}, and 0, for the signal, decoy-1, decoy-2, and vacuum source, respectively. Then, the source is sent into a source monitor at P2 to estimate the statistical parameters for security analysis, and sent out of Alice's side at P3. (b) Schematic diagram of an active source monitor. A high-speed active optical-switch (OS) randomly sends one half of the input optical pulses to a photon-number-resolving (PNR) detector at P4 for parameter estimation, and sends the other half to Bob for key generation. (c) Schematic diagram of a passive source monitor. The optical pulses are passively separated into two parts by a beam-splitter (BS) with transmittance η_{BS}: one goes to a PNR detector with efficiency η_D at P5, which is modeled by an attenuator with efficiency η_D combined with an ideal PNR detector, and the other is sent out of the source monitor.

A full security analysis procedure can be divided into four steps. **Step1:** Estimate the bounded statistical parameters of the untrusted source based on the measurement data of the monitor. **Step2:** Verify the conditions shown in Eqs. (7) and (8). **Step3:** Calculate the lower bound of Q_1 and Q_2 based on Eqs. (5) and (6). **Step4:** Estimate the secure key rate.

3.1 Active Source Monitor

In the active source monitor shown in Fig. 1(b), one half of the optical pulses are randomly sent to a photon-number-resolving (PNR) detector for parameters estimation, and the other half are sent to Bob for key generation [35]. In this subsection, the PNR detector is assumed to be noiseless and the detection efficiency is 1. Suppose $D(m, \eta)$ is the probability that m photoelectrons are recorded by the PNR detector given that the attenuation coefficient of the VOA is η, one has

$$D(m, \eta) = P_3(m, \eta), \ (m = 0, 1, 2, 3, \cdots). \tag{12}$$

Combining the results in Eqs. (11) and (12),

$$a'_m = D(m, \eta_s), a_m = D(m, \eta_{d1}), b_m = D(m, \eta_{d2}). \tag{13}$$

Clearly, one can bound the parameters $\{a'_m, a_m, b_m\}$ based on the recorded data $D(m, \eta)$. Then one can verify the conditions in Eqs. (7) and (8), and calculate the secure key rate.

3.2 Passive Source Monitor

As pointed out in [36, 37], it is challenging and inefficient to implement the active scheme. Then, a practical passive scheme is proposed and tested experimentally [36]. In the passive source monitor shown in Fig. 1(c), optical pulses are separated into two paths by a beam splitter (BS) with transmittance η_{BS}: one goes to a PNR detector with efficiency η_D, which is modeled by a BS with transmittance η_D and a perfect PNR detector, and the other is sent out of Alice's side. If the PNR detector is noiseless, the detected photoelectron distribution $F(m, \eta)$ at P5 will be the same to the PND $P_5(m, \eta)$ at P5,

$$F(m, \eta) = P_5(m, \eta). \tag{14}$$

The PND at P5 is also a Bernoulli trasformation of that at P1,

$$P_5(m, \eta) = \sum\nolimits_{n=m}^{\infty} P_1(n) \left(\begin{array}{c} n \\ m \end{array} \right) [\eta(1 - \eta_{BS})\eta_D]^m [1 - \eta(1 - \eta_{BS})\eta_D]^{n-m}. \tag{15}$$

For simplification, one set

$$(1 - \eta_{BS})\eta_D = \eta_{BS}. \tag{16}$$

Combining the results in Eqs. (10), (15) and (16), one has

$$P_5(m, \eta) = P_3(m, \eta). \tag{17}$$

Based on Eqs. (11), (14) and (17), one can bound the parameters $\{a'_m, a_m, b_m\}$ with the knowledge of $F(m, \eta)$. In a real system, one needs to consider the practical imperfections of the source monitor [37, 38, 43]. In the following, the effects of statistical fluctuation and detection noise are quantitatively analyzed.

3.2.1 Infinite Data Size and Noiseless Source Monitor

Suppose that M is the total number of optical pulses sent from Alice to Bob, while $p'M(= M_s)$, $p_1 M(= M_1)$, and $p_2 M = (M_2)$ is the number of signal, decoy-1, and decoy-2 pulses, correspondingly. Let j_m^s, j_m^{d1}, and j_m^{d2} denote the number of detected signal, decoy-1 and decoy-2 pulses at P5 given the PNR detector records m photoelectrons. Using the *random sampling theory* [46], each $F(m, \eta_s) \in [j_m^s/M_s - \varepsilon', j_m^s/M_s + \varepsilon']$ with a confidence level $1 - 2\exp(-M_s {\varepsilon'}^2/2)$ for signal pulses, and each $F(m, \eta_{1(2)}) \in [{j_m}^{d1(2)}/M_{1(2)} - \varepsilon_{1(2)}, {j_m}^{d1(2)}/M_{1(2)} + \varepsilon_{1(2)}]$ with a confidence level $1 - 2\exp(-M_1(2)\varepsilon_{1(2)}^2/2)$ for decoy-1(2) pulses can be estimated.

Step1. When the data size $M \to \infty$, one has ${a'_m}^L = {a'_m}^U = F(m, \eta_s) = j_m^s/M_s$, $a_m^L = a_m^U = F(m, \eta_{d1}) = j_m^{d1}/M_1$, $b_m^L = b_m^U = F(m, \eta_{d2}) = j_m^{d2}/M_2$.

Step2. The conditions in Eqs. (7) and (8) turn to

$$\frac{F(k, \eta_s)}{F(k, \eta_{d1})} \geq \frac{F(3, \eta_s)}{F(3, \eta_{d1})} \geq \frac{F(2, \eta_s)}{F(2, \eta_{d1})} \geq \frac{F(1, \eta_s)}{F(1, \eta_{d1})} \text{ (for all } k \geq 4),$$
$$1 + \frac{F(3, \eta_{d1})F(1, \eta_s) - F(1, \eta_{d1})F(3, \eta_s)}{F(2, \eta_{d1})F(3, \eta_s) - F(3, \eta_{d1})F(2, \eta_s)} \frac{F(2, \eta_{d2})}{F(2, \eta_{d1})} > 0.$$

Step3. In case-1, the gain of 1-photon state is calculated by Eq. (5) based on the recorded data $F(m, \eta)$, and all the errors are assumed from 1-photon state $e_1 = E_\mu Q_\mu / Q_1$. In case-2,

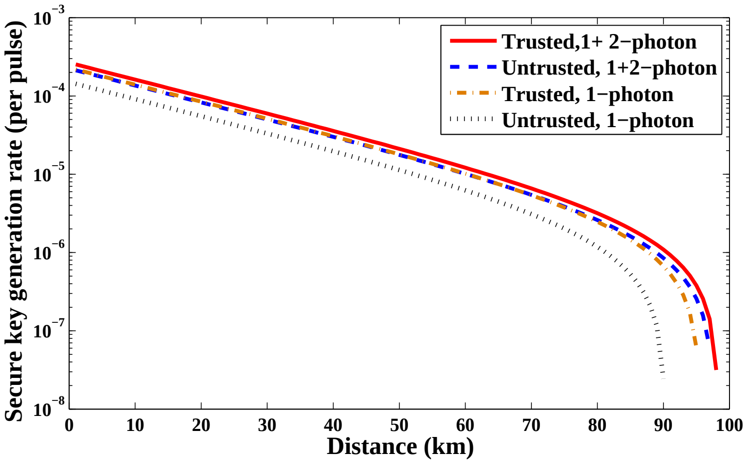

Fig. 2. (Color online) Simulation results of the SARG04 protocol for the trusted source, compared with the untrusted source in both case-1 and case-2 when the data size is infinite. In the trusted source case, infinite decoy state method is used to estimate the values of Q_1, Q_2, e_1, e_2 as in Eq. (4). The top (red) line is the simulation results for the trusted source, where one considers the contribution from both 1-photon and 2-photon states. The second (yellow) line is the simulation results for the untrusted source in case-2. The third (blue) line is the simulation results for the trusted source, where one considers the contribution from only 1-photon state. The bottom (green) line is the simulation results for the untrusted source in case-1. In all the simulations, the PND for both trusted and untrusted source is assumed to be of Poissonian statistics.

the gains of 1-photon and 2-photon states are calculated by Eqs. (5) and (6) based on the recorded data $F(m, \eta)$, and $e_{1(2)}$ are chosen numerically to lower bound the secure key rate.

Step4. Calculate the final secure key rate.

For testing the efficiency of the passive scheme, the simulation results for the trusted source are compared with that for the untrusted source (shown in Fig. 2), where the data size is assumed to be infinite. The PND for the trusted and the untrusted source is assumed to be of Poissonian statistics to perform simulations. The error correction efficiency $f(E_\mu) = 1.22$. The transmittance η_{BS} of the BS is 0.13 and the detection efficiency η_D of the PNR detector is 0.15. The other experimental parameters are cited from the GYS experiment [45] as shown in Table 3.2.1, where η_{Bob} is the efficiency of Bob's detection, e_0 is the probability that a dark count hit the erroneous detector in Bob's side. Suppose the average photon number (APN) for signal, decoy-1 and decoy-2 sources are μ, v_1 and v_2, respectively. The conditions in Eqs. (7) and (8) turn to $\frac{e^{-\mu}\mu^k}{e^{-v_1}{v_1}^k} \geq \frac{e^{-\mu}\mu^3}{e^{-v_1}{v_1}^3} \geq \frac{e^{-\mu}\mu^2}{e^{-v_1}{v_1}^2} \geq \frac{e^{-\mu}\mu}{e^{-v_1}v_1}$ (for all $k \geq 4$), and $1 - \frac{v_2}{v_1}\frac{v_1+\mu}{\mu} > 0$. As shown in Fig. 2, the performance of the untrusted source based on the passive source monitor is very close to that of the trusted source, and the 2-photon state makes positive contribution to the secure key rate.

Table 1. The simulation parameters for Figs. 2-5.

η_D	η_{BS}	η_{Bob}	α	Y_0	e_{det}	e_0
0.15	0.13	0.045	0.21	1.7×10^{-6}	3.3%	0.5

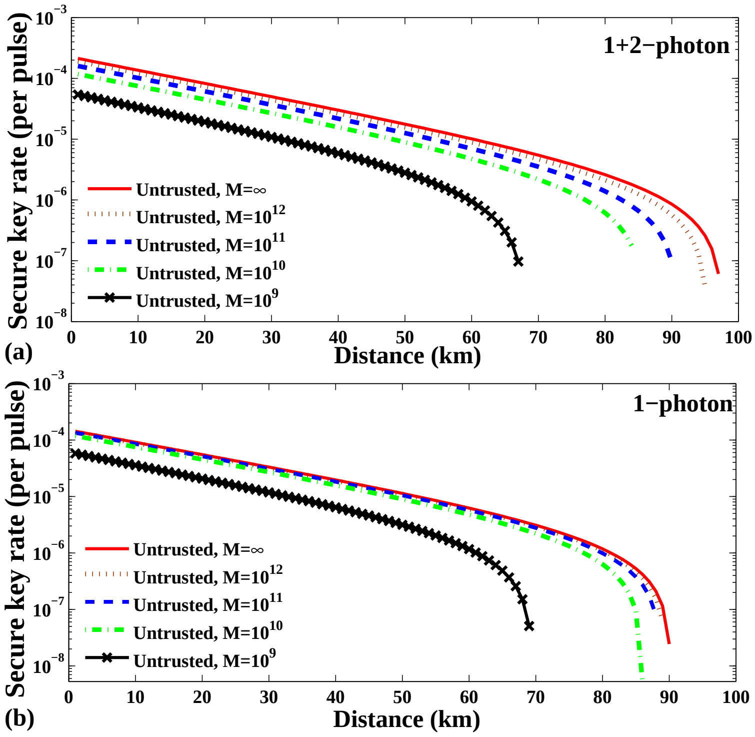

Fig. 3. (Color online) Simulation results for the SARG04 protocol with an untrusted source in case-1 and case-2 with data size M, based on the passive source monitor. The PND of the untrusted source is assumed to be Poissonian. The other experimental parameters are cited from Table 3.2.1. (a) Simulation results in case-2 with data size $M = \infty, 10^{12}, 10^{11}, 10^{10}, 10^{9}$, respectively. (b) Simulation results in case-1 with data size $M = \infty, 10^{12}, 10^{11}, 10^{10}, 10^{9}$, respectively. The confidence level is set to be $1 - 10^{-6}$.

3.2.2 Finite Data Size and Noiseless Source Monitor

Suppose that M is finite and j_m^s, j_m^{d1}, and j_m^{d2} denote the number of detected signal, decoy-1 and decoy-2 pulses at P5 given the PNR detector records m photoelectrons.

Step1. We prove that, to estimate $Q_{1(2)}$ and verify the conditions in Eqs. (7) and (8) with finite data size, one only needs to bound the parameters $\{{a'_m}^L, a_m^U, b_n^L\}$ for $m = 0, 1, \cdots, J$ and $n = 0, 1, 2$ (see Appendix B). Simultaneously, $F(m, \eta_s) \in [j_m^s/M_s - \varepsilon', j_m^s/M_s + \varepsilon']$, $F(m, \eta_1) \in [j_m^{d1}/M_1 - \varepsilon_1, j_m^{d1}/M_1 + \varepsilon_1]$ for $m = 0, 1, 2, \cdots, J$, and $F(n, \eta_2) \in [j_n^{d2}/M_2 - \varepsilon_2, j_n^{d2}/M_2 + \varepsilon_2]$ for $n = 0, 1, 2$ are approximately estimated with a confidence level $\alpha = 1 - 2(J+1)\exp(-M_s{\varepsilon'}^2/2) - 2(J+1)\exp(-M_1{\varepsilon_1}^2/2) - 6\exp(-M_2{\varepsilon_2}^2/2)$. From Eqs. (11), (14) and (17), one gets

$$ {a'_m}^L = \frac{k_m^s}{M_s} - \varepsilon', \; a_m^U = \frac{k_m^{d1}}{M_1} + \varepsilon_1, \; b_n^L = \frac{k_n^{d2}}{M_2} - \varepsilon_2, \tag{18} $$

for $m = 0, 1, 2, \cdots, J$ and $n = 0, 1, 2$ with confidence level α.

Step2. It is challenging to verify directly the condition in Eq. (7) with finite data size: a) In hardware, the PNR detector is required to discriminate the photon number $n = 0, 1, \cdots, \infty$; b)

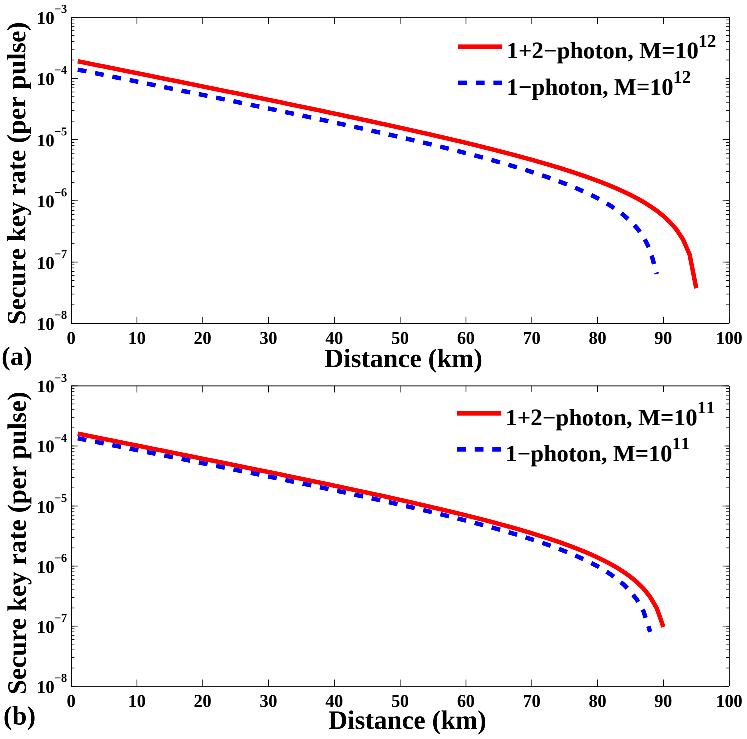

Fig. 4. (Color online) Comparison between case-1 and case-2 for the SARG04 protocol with an untrusted source: (a) with data size $M = 10^{12}$; (b) with data size $M = 10^{11}$. The PND of the untrusted source is assumed to be Poissonian. The other experimental parameters are cited from Table 3.2.1. The confidence level is set to be $1 - 10^{-6}$.

When the photoelectron number m is large enough, one always gets $k_m^s = k_m^{d1} = 0$. One needs a reasonable cutoff value of m. Suppose $j_m^{d1} = 0$ for all $m > J$ while $j_J^{d1} > 0$. To lower bound the gains of Q_1 and Q_2 with finite data size, one can replace the condition in Eq. (7) as

$$\frac{{a'_k}^L}{a_k^U} \geq \frac{{a'_3}^L}{a_3^U} \geq \frac{{a'_2}^L}{a_2^U} \geq \frac{{a'_1}^L}{a_1^U}, \text{ (for all 4} \leq \text{k} \leq \text{J)}, \tag{19}$$

where the PNR detector is only required to discriminate photon number $n = 0, 1, \cdots, J$ (see Appendix B for details). The condition in Eq. (8) turns to

$$1 + \frac{F(3,\eta_{d1})F(1,\eta_s) - F(1,\eta_{d1})F(3,\eta_s)}{F(2,\eta_{d1})F(3,\eta_s) - F(3,\eta_{d1})F(2,\eta_s)} \frac{F(2,\eta_{d2})}{F(2,\eta_{d1})} > 0. \tag{20}$$

Step3. If the conditions in step2 are satisfied, one can lower bound the parameters $Q_{1(2)}$.

Step4. Calculate the secure key rate for case-1 and case-2 with Eqs. (9) and (3).

For testing the effects of finite data size, we choose an untrusted source of Poissonian statistics to perform simulations in both case-1 and case-2. The error correction efficiency $f(E_\mu)$ are chosen to be 1.22. The other experimental parameters are cited from Table 3.2.1. Simulation results for case-2 and case-1 are shown in Fig. 3(a) and (b), and the data size are set to be $M = \infty$, 10^{12}, 10^{11}, 10^{10} and 10^{9}, respectively. To compare the two cases more clearly, Fig. 4 shows the simulation results for case-1 and case-2 with $M = 10^{12}$ and 10^{11}, respectively. In all the above simulations, the confidence level is set to be $\alpha = 1 - 10^{-6}$. The simulation results show that statistical fluctuation has negative effect on performance of the QKD system. When the data size is large enough, the 2-photon state has positive contribution to the secure key rate.

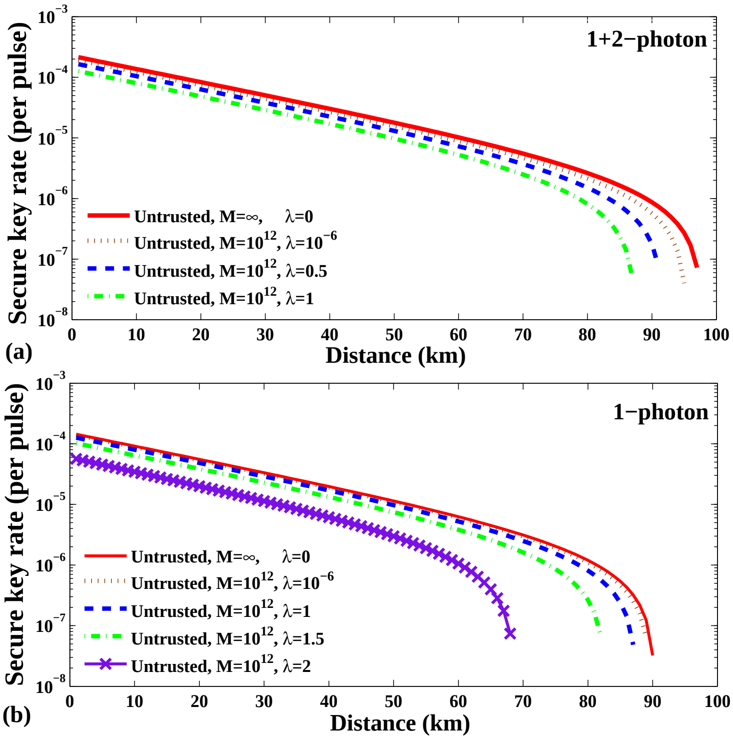

Fig. 5. (Color online) Simulation results for the SARG04 protocol with an untrusted source based on the passive scheme: (a) with finite data size $M = 10^{12}$, and the average dark count rate of the Poissonian detection noise $\lambda = 0, 10^{-6}, 0.5$, and 1, respectively, in case-2; (b) with finite data size $M = 10^{12}$, and the average dark count rate of the Poissonian detection noise $\lambda = 0, 10^{-6}, 1, 1.5$, and 2, respectively, in case-1. The PND of the untrusted source and the distribution of detection noise are assumed to be Poissonian. The other experimental parameters are cited from Table 3.2.1. The confidence level is $1 - 10^{-6}$.

3.2.3 Finite Data Size and Source Monitor with Random 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 P5 satisfy $m' = m + y$. One can calculate the lower and upper bound of PND $P_5(m, \eta)$ at P5 based on the photoelectron distribution $F(m, \eta)$ 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) [48, 49], transition-edge sensor (TES) [50], or a threshold detector together with a VOA [51]. In case of independent Poisson statistics noise, the probability of detecting m' photoelectrons is $F(m',\eta)=\sum_{d=0}^{m'}N(y=m'-d)P_5(d,\eta)$ where $N(y=d)=e^{-\lambda}\lambda^d/d!$ is the probability that d dark counts occur in the PNR detector, and λ is the average dark count rate. Then, one has

$$\begin{bmatrix} P_5(0,\eta) \\ P_5(1,\eta) \\ P_5(2,\eta) \\ P_5(3,\eta) \end{bmatrix} = \begin{bmatrix} F(0,\eta) & 0 & 0 & 0 \\ F(1,\eta) & F(0,\eta) & 0 & 0 \\ F(2,\eta) & F(1,\eta) & F(0,\eta) & 0 \\ F(3,\eta) & F(2,\eta) & F(1,\eta) & F(0,\eta) \end{bmatrix} \begin{bmatrix} e^{\lambda} \\ -\lambda e^{\lambda} \\ \lambda^2 e^{\lambda}/2 \\ -\lambda^3 e^{\lambda}/6 \end{bmatrix}. \tag{21}$$

Step1. Using *random sampling theory* [46], simultaneously, $F(m,\eta_s)\in[j_m^s/M_s-\varepsilon', j_m^s/M_s+\varepsilon']$, $F(m,\eta_{d1})\in[j_m^{d1}/M_1-\varepsilon_1, j_m^{d1}/M_1+\varepsilon_1]$, and $F(n,\eta_{d2})\in[j_n^{d2}/M_2-\varepsilon_2, j_n^{d2}/M_2+\varepsilon_2]$ for $m=0,1,2,\cdots,J$ and $n=0,1,2$ are estimated with a confidence level $1-2(J+1)\exp(-M_s{\varepsilon'}^2/2)-2(J+1)\exp(-M_1{\varepsilon_1}^2/2)-6\exp(-M_2{\varepsilon_2}^2/2)$. Then, one yields

$$\begin{aligned}
a_0 &\le e^{\lambda}(\frac{j_{m=0}^{d1}}{M_1}+\varepsilon'),\\
b_0 &\ge e^{\lambda}(\frac{j_{m=0}^{d2}}{M_2}-\varepsilon_2),\\
a_0' &\ge e^{\lambda}(\frac{j_{m=0}^{s}}{M_s}-\varepsilon'),\\
a_1 &\le e^{\lambda}(\frac{j_{m=1}^{d1}}{M_1}+\varepsilon_1)-\lambda e^{\lambda}(\frac{j_{m=0}^{d1}}{M_1}-\varepsilon_1),\\
b_1 &\ge e^{\lambda}(\frac{j_{m=1}^{d2}}{M_2}-\varepsilon_2)-\lambda e^{\lambda}(\frac{j_{m=0}^{d2}}{M_2}+\varepsilon_2),\\
a_1' &\ge e^{\lambda}(\frac{j_{m=1}^{s}}{M_s}-\varepsilon')-\lambda e^{\lambda}(\frac{j_{m=0}^{s}}{M_s}+\varepsilon'),\\
a_2 &\le e^{\lambda}(\frac{j_{m=2}^{d1}}{M_1}+\varepsilon_1)-\lambda e^{\lambda}(\frac{j_{m=1}^{d1}}{M_1}-\varepsilon_1)+\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=0}^{d1}}{M_1}+\varepsilon_1),\\
b_2 &\ge e^{\lambda}(\frac{j_{m=2}^{d2}}{M_2}-\varepsilon_2)-\lambda e^{\lambda}(\frac{j_{m=1}^{d2}}{M_2}+\varepsilon_2)+\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=0}^{d2}}{M_2}-\varepsilon_2),\\
a_2' &\ge e^{\lambda}(\frac{j_{m=2}^{s}}{M_s}-\varepsilon')-\lambda e^{\lambda}(\frac{j_{m=1}^{s}}{M_s}+\varepsilon')+\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=0}^{s}}{M_s}-\varepsilon'),\\
a_3 &\le e^{\lambda}(\frac{j_{m=3}^{d1}}{M_1}+\varepsilon_1)-\lambda e^{\lambda}(\frac{j_{m=2}^{d1}}{M_1}-\varepsilon_1)+\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=1}^{d1}}{M_1}+\varepsilon_1)\\
&\quad -\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=0}^{d1}}{M_1}-\varepsilon_1),\\
a_3' &\ge e^{\lambda}(\frac{j_{m=3}^{s}}{M_s}-\varepsilon')-\lambda e^{\lambda}(\frac{j_{m=2}^{s}}{M_s}+\varepsilon')+\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=1}^{s}}{M_s}-\varepsilon')\\
&\quad -\frac{\lambda^2}{2}e^{\lambda}(\frac{j_{m=0}^{s}}{M_s}+\varepsilon').
\end{aligned}$$

Our analysis is not limited to the Poissonian noise case. Generally, when the random-positive detection noise y with distribution $N(y)$ is known to Alice, one can still use the same method in [43] to estimate the parameters $\{{a_0'}^L,\ b_0^L,\ a_0^U,\ {a_1'}^L,\ b_1^L,\ a_1^U,\ {a_2'}^L,\ b_2^L,\ a_2^U,\ {a_3'}^L,\ a_3^U\}$ with a certain confidence level.

Step2. Using the same method, one can estimate the bound values $\{{a'_k}^L, a_k^U\}$ for $4 \leq k \leq J$, and verify the conditions in Eqs. (8) and (19). Since the expressions of $\{{a'_k}^L, a_k^U\}$ for $4 \leq k \leq J$ are much complex and trivial, we assume the above conditions are satisfied as in [36, 40].

Step3. Lower bound the parameters Q_1 and Q_2.

Step4. Calculate the secure key rate for case-1 and case-2 with Eqs. (9) and (3).

For testing the effect of dark count noise, the simulation results for case-2 are shown in Fig. 5(a), with finite data size $M = 10^{12}$ and average dark count rate $\lambda = 0$, 10^{-6}, 0.5, and 1, respectively. The simulation results for case-1 are shown in Fig. 5(b) with $M = 10^{12}$ and $\lambda = 0$, 10^{-6}, 1, 1.5 and 2, respectively. The confidence level is set to be $\alpha = 1 - 10^{-6}$.

4 Summary and Conclusion Remark

In summary, we have shown the unconditional security of the SARG04 protocol with an untrusted source, given that the bound of a few key statistical parameters of the untrusted source are known. Furthermore, an active and a passive source monitors are proposed to verify these parameters experimentally. Finally, the effects of the practical imperfections in the passive source monitor are quantitatively analyzed, such as finite data size and additive detection noise. Asymptotically, the performance of the QKD system with an untrusted source combined with passive source monitor is very close to that of a trusted source. Our results can be directly applied to plug-and-play QKD system with SARG04 protocol.

Acknowledgements

This work is supported by the Key Project of National Science Foundation of China (Grant No. 60837004 and 61101081), National Hi-Tech Research and Development (863) Program.

References

1. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: Public key distribution and coin tossing*, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York), p. 175.
2. V. Scarani, A. Acin, G. Ribordy, and N. Gisin (2004), *Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations*, Phys. Rev. Lett., Vol. **92**, p. 057901.
3. A. K. Ekert (1991), *Quantum cryptography based on Bells theorem*, Phys. Rev. Lett., Vol. **67**, p. 661.
4. F. Grosshans and P. Grangier (2002), *Continuous Variable Quantum Cryptography Using Coherent States*, Phys. Rev. Lett., Vol. **88**, p. 057902.
5. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Düsek, N. Lütkenhaus, and M. Peev (2009), *The security of practical quantum key distribution*, Rev. Mod. Phys., Vol. **81**, p. 1301.
6. P. W. Shor and J. Preskill (2000), *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett., Vol. **85**, p. 441.
7. H. Inamori, N. Lütkenhaus, and D. Mayers (2007), *Unconditional security of practical quantum key distribution*, Eur. Phys. J. D, Vol. **41**, p. 599.
8. D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill (2004), *Security of quantum key distribution with imperfect devices*, Quantum Inf. Comput., Vol. **4**, p. 325.
9. C. H. F. Fred, K. Tamaki, and H. K. Lo (2006), *Performance of two quantum-key-distribution protocols*, Phys. Rev. A, Vol. **73**, p. 012337.

10. A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani (2007), *Device-Independent Security of Quantum Cryptography against Collective Attacks*, Phys. Rev. Lett., Vol. **98**, p. 230501.
11. R. Garcia-Patron and N. J. Cerf (2006), *Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution*, Phys. Rev. Lett., Vol. **97**, p. 190503.
12. M. Navascues, F. Grosshans and A. Acin (2006), *Security Bounds for Continuous Variables Quantum Key Distribution*, Phys. Rev. Lett., Vol. **94**, p. 020505.
13. H. K. Lo and Y. Zhao (2009), *Quantum Cryptography*, Encyclopedia of Complexity and Systems Science (Springer New York), Vol. 8, p. 7265.
14. X. B. Wang (2007), *Decoy-state quantum key distribution with large random errors of light intensity*, Phys. Rev. A, Vol. **75**, p. 052301.
15. X. B. Wang, C. Z. Peng, and J. W. Pan (2007), *Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source*, Appl. Phys. Lett., Vol. **90**, p. 031110.
16. V. Makarov, A. Anisimov, and J. Skaar (2006), *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A, Vol. **74**, p. 022313.
17. V. Makarov and J. Skaar (2008), *Fakes states attack using detector efficiency mismatch on SARG04, Phase-Time, DPSK, and Ekert protocols*, Quantum Inf. Comput., Vol. **8**, p. 0622.
18. B. Qi, C. H. F. Fung, H. K. Lo and X. F. Ma (2007), *Time-shift attack in practical quantum cryptosystems*, Quantum Inf. Comput., Vol. **7**, p.0073.
19. Y. Zhao, C. H. F. Fung, B. Qi, C. Chen and H. K. Lo (2008), *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A, Vol. **78**, p. 042333.
20. C. H. F. Fung, K. Tamaki, B. Qi, H. K. Lo and X. Ma (2009), *Security proof of quantum key distribution with detection efficiency mismatch*, Quantum Inf. Comput., Vol. **9**, p. 0131.
21. L. Lydersen and J. Skaar (2010),*Security of quantum key distribution with bit and basis dependent detector flaws*, Quantum Inf. Comput., Vol. **10**, p. 0060.
22. V. Makarov (2009), *Controlling passively quenched single photon detectors by bright light*, New J. Phys., Vol. **11**, p. 065003.
23. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov (2010), *Hacking commercial quantum cryptography by tailored bright illumination*, Nat. Photonics, Vol. **4**, p. 686.
24. I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov (2011), *Full-field implementation of a perfect eavesdropper on a quantum cryptography system*, Nat. Comm., Vol. **2**, p. 349.
25. N. Lütkenhaus (2000), *Security against individual attacks for realistic quantum key distribution*, Phys. Rev. A, Vol. **61**, p. 052304.
26. W. Y. Hwang (2003), *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Phys. Rev. Lett., Vol. **91**, p. 057901.
27. H. K. Lo (2004), *Quantum Key Distribution with Vacua or Dim Pulses as Decoy States*, in Proceedings of the International Symposium on Information Theory (ISIT) (IEEE Press, Chicago), p. 137.
28. X. B. Wang (2005), *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography* , Phys. Rev. Lett., Vol. **94**, p. 230503.
29. H. K. Lo, X. Ma, and K. Chen (2005), *Decoy State Quantum Key Distribution*, Phys. Rev. Lett., Vol. **94**, p. 230504.
30. X. B. Wang (2005), *Decoy-state protocol for quantum cryptography with four different intensities of coherent light* , Phys. Rev. A, Vol. **72**, p. 012322.
31. X. Ma, B. Qi, Y. Zhao, and H. K. Lo (2005), *Practical decoy state for quantum key distribution*, Phys. Rev. A, Vol. **72**, p. 012326.
32. W. Mauerer and C. Silberhorn (2007), *Quantum key distribution with passive decoy state selection*, Phys. Rev. A, Vol. **75**, p. 050305.
33. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy (2006), *Trojan-horse attacks on quantum-key-distribution systems*, Phys. Rev. A, Vol. **73**, p. 022320.
34. X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi (2007), *Quantum information with Gaus-*

sian states , Phys. Rep., Vol. **448**, p. 1.

35. Y. Zhao, B. Qi, and H. K. Lo (2008), *Quantum key distribution with an unknown and untrusted source*, Phys. Rev. A, Vol. **77**, p. 052327.
36. X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo (2008), *Experimental quantum-key distribution with an untrusted source*, Opt. Lett., Vol. **33**, p. 2077.
37. Y. Zhao, B. Qi, H. K. Lo, and L. Qian (2010), *Security analysis of an untrusted source for quantum key distribution: passive approach*, New J. Phys., Vol. **12**, p. 023024.
38. X. Peng, B. Xu, and H. Guo (2010), *Passive-scheme analysis for solving the untrusted source problem in quantum key distribution*, Phys. Rev. A, Vol. **81**, p. 042320.
39. X. B. Wang, C. Z. Peng, J. Zhang, L. Yang and J. W. Pan (2008), *General theory of decoy-state quantum cryptography with source errors*, Phys. Rev. A, Vol. **77**, p. 042311.
40. X. B. Wang, L. Yang, C. Z. Peng, and J. W. Pan (2009), *Decoy-state quantum key distribution with both source errors and statistical fluctuations*, New J. Phys., Vol. **11**, p. 075006.
41. J. Z. Hu and X. B. Wang (2010), *Reexamination of the decoy-state quantum key distribution with an unstable source* , Phys. Rev. A, Vol. **82**, p. 012331.
42. F. X. Xu, Y. Zhang, Z. Zhou, W. Chen, Z. F. Han, and G. C. Guo (2009), it Experimental demonstration of counteracting imperfect sources in a practical one-way quantum-key-distribution system, Phys. Rev. A, Vol. **80**, p. 062309.
43. B. Xu, X. Peng, and H. Guo (2010), it Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system, Phys. Rev. A, Vol. **82**, p. 042301.
44. www.idquantique.com
45. C. Gobby, Z. L. Yuan, and A. J. Shields (2004), *Quantum key distribution over 122 km of standard telecom fiber*, Appl. Phys. Lett., Vol. **84**, p. 3762.
46. J. V. Uspensky (1937), *Introduction to mathematical probability*, McGraw-Hill (New York).
47. C. J. Clopper and E. S. Pearson (1934), *The use of confidence or fiducial limits illustrated in the case of the binomial*, Biometrika Vol. **26**, p. 404.
48. D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, and I. A. Walmsley (2003), *Fiber-assisted detection with photon number resolution*, Opt. Lett., Vol. **28**, p. 2387.
49. D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson (2004), *Photon-number-resolving detection using time-multiplexing*, J. Mod. Opt., Vol. **51**, p. 1499.
50. D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam (2005), *Noise-free high-efficiency photon-number-resolving detectors* , Phys. Rev. A, Vol. **71**, p. 061803.
51. G. Zambra, A. Andreoni, M. Bondani, M. Gramegna, M. Genovese, G. Brida, A. Rossi, and M. G. A. Paris (2005), *Experimental Reconstruction of Photon Statistics without Photon Counting*, Phys. Rev. Lett., Vol. **95**, p. 063602.

Appendix A

Suppose Alice sends M pulses to Bob in the whole quantum process. At any time i, where $i \in \{1, 2, \cdots, M\}$, Alice randomly produces vacuum ($|0\rangle\langle 0|$), decoy-1 ($\rho_{1i} = \sum_{n=0}^{\infty} a_{ni} |n\rangle\langle n|$), decoy-2 ($\rho_{2i} = \sum_{n=0}^{\infty} b_{ni} |n\rangle\langle n|$), and signal ($\rho_{si} = \sum_{n=0}^{\infty} a'_{ni} |n\rangle\langle n|$) source with the probability p_0, p_1, p_2, and p', respectively, where $\{a_{ni},\ b_{ni},\ a'_{ni}\}$ are controlled by Eve.

Following the methods in [39, 40], some definitions are necessary for further analysis.

- *Definition 1.* In the protocol, Alice sends M pulses, and Bob gets M observations. If Bob's detector click at time i, we say that "the ith pulse from Alice has caused a count".
- *Definition 2.* Sets C and c_n: Set C contains any pulse that has caused a count; set c_n contains any n-photon pulse that has caused a count.

- *Definition 3.* Denote the lower (upper) bound of $\{a'_{ni},\ a_{ni},\ b_{ni}\}$ as $\{{a'_n}^{L(U)},\ a_n^{L(U)},\ b_n^{L(U)}\}$ for $i = 1, 2, \cdots, M$, which can be experimentally estimated by the source monitor in Fig. 1 [43].

Define

$$d_{0i} = \frac{1}{p_0 + p_1 a_{0i} + p_2 b_{0i} + p' a'_{0i}},\ d_{ki} = \frac{1}{p_1 a_{ki} + p_2 b_{ki} + p' a'_{ki}}\ (k \geq 1), \tag{A.1}$$

and

$$D_k = \sum_{i \in c_k} d_{ki}. \tag{A.2}$$

If the ith pulse contains zero photon, the probability that it comes from the vacuum source is $P_{vi|0} = p_0 d_{0i}$. Therefore, the number of counts caused by vacuum source is

$$N_0 = \sum_{i \in c_0} p_{vi|0} = \sum_{i \in c_0} p_0 d_{0i}. \tag{A.3}$$

Similarly, if the ith pulse contains zero photon, the probability that it comes from the decoy-1, decoy-2 and signal source are $P_{1i|0} = p_1 a_{0i} d_{0i}$, $P_{2i|0} = p_2 b_{0i} d_{0i}$, and $P_{si|0} = p' a'_{0i} d_{0i}$, respectively. Then the number of counts caused by zero photon state in decoy-1, decoy-2 and signal source are

$$n_{0d1} = \sum_{i \in c_0} p_1 a_{0i} d_{0i},\ n_{0d2} = \sum_{i \in c_0} p_2 b_{0i} d_{0i},\ n_{0s} = \sum_{i \in c_0} p' a'_{0i} d_{0i}, \tag{A.4}$$

respectively. It is clear that

$$\begin{aligned} n_{0d1}^U = \frac{p_1 a_0^U N_0}{p_0} \geq &\quad n_{0d1} &\geq \frac{p_1 a_0^L N_0}{p_0} = n_{0d1}^L, \\ n_{0d2}^U = \frac{p_2 b_0^U N_0}{p_0} \geq &\quad n_{0d2} &\geq \frac{p_2 b_0^L N_0}{p_0} = n_{0d2}^L, \\ n_{0s}^U = \frac{p' {a'_0}^U N_0}{p_0} \geq &\quad n_{0s} &\geq \frac{p' {a'_0}^L N_0}{p_0} = n_{0s}^L. \end{aligned} \tag{A.5}$$

The number of counts caused by decoy-1(2) and signal sources are

$$\begin{aligned} N_{d1} &= n_{0d1} + p_1 \sum_{i \in c_1} a_{1i} d_{1i} + p_1 \sum_{i \in c_2} a_{2i} d_{2i} + p_1 \sum_{k=3}^{\infty} \sum_{i \in c_k} a_{ki} d_{ki}, \\ N_{d2} &= n_{0d2} + p_2 \sum_{i \in c_1} b_{1i} d_{1i} + p_2 \sum_{i \in c_2} b_{2i} d_{2i} + p_2 \sum_{k=3}^{\infty} \sum_{i \in c_k} b_{ki} d_{ki}, \\ N_s &= n_{0s} + p' \sum_{i \in c_1} a'_{1i} d_{1i} + p' \sum_{i \in c_2} a'_{2i} d_{2i} + p' \sum_{k=3}^{\infty} \sum_{i \in c_k} a'_{ki} d_{ki}, \end{aligned} \tag{A.6}$$

which can be rewritten as

$$N_{d1} = n_{0d1} + p_1 a_1^U D_1 + p_1 a_2^U D_2 + p_1 \Lambda_1 - \xi_1, \tag{A.7}$$

$$N_{d2} = n_{0d2} + p_2 b_1^L D_1 + p_2 b_2^L D_2 + p_2 \Lambda_2 + \xi_2, \tag{A.8}$$

$$N_s = n_{0s} + p' {a'_1}^L D_1 + p' {a'_2}^L D_2 + p' \Lambda' + \xi_3, \tag{A.9}$$

where $\Lambda_1 = \sum_{k=3}^{\infty} a_k^U D_k,\ \Lambda_2 = \sum_{k=3}^{\infty} b_k^L D_k,\ \Lambda' = \sum_{k=3}^{\infty} {a'_k}^L D_k$, and $\xi_1 \geq 0,\ \xi_2 \geq 0,\ \xi_3 \geq 0$. According to the definition, we have

$$ {a'_2}^L D_2 + \Lambda' = \frac{{a'_2}^L}{a_2^U}(a_z^U D_2 + \Lambda_1) + \xi_4 \tag{A.10} $$

and

$$ \xi_4 = \Lambda' - \frac{{a'_2}^L}{a_2^U}\Lambda_1. \tag{A.11} $$

Further we assume

$$ \frac{{a'_k}^L}{a_k^U} \geq \frac{{a'_2}^L}{a_2^U} \geq \frac{{a'_1}^L}{a_1^U},\ \text{(for all } k \geq 3), \tag{A.12} $$

which leads to $\xi_4 \geq 0$. Then, one can rewrite the Eqs. (A.7) and (A.9) as

$$ N_{d1} = n_{0d1} + p_1 a_1^U D_1 + p_1(a_2^U D_2 + \Lambda_1) - \xi_1, \tag{A.13} $$

$$ N_s = n_{0s} + p' {a'_1}^L D_1 + p' \frac{{a'_2}^L}{a_2^U}(a_2^U D_2 + \Lambda_1) + \xi_3 + p'\xi_4. \tag{A.14} $$

Combining the Eqs. (A.13) and (A.14), one can lower bound the D_1 as

$$ D_1 \geq D_1^L = \frac{\frac{{a'_2}^L}{p_1} N_{d1} - \frac{a_2^U}{p'} N_S - \frac{{a'_2}^L}{p_1} n_{0d1}^U + \frac{a_2^U}{p'} n_{0s}^L}{{a'_2}^L a_1^U - a_2^U {a'_1}^L}. \tag{A.15} $$

Further, one can lower bound the gain of 1-photon state in signal source, $Q_1 = p' \sum\limits_{i \in c_1} a'_{1i} d_{1i} \frac{1}{p'M} \geq \frac{{a'_1}^L D_1^L}{M}$ as shown in Eq. (5). We can lower bound the Q_2 in a similar way. Define

$$ \xi = \Lambda' - {a'_3}^L / a_3^U \Lambda_1, \tag{A.16} $$

and assume

$$ \frac{{a'_k}^L}{a_k^U} \geq \frac{{a'_3}^L}{a_3^U} \geq \frac{{a'_2}^L}{a_2^U} \geq \frac{{a'_1}^L}{a_1^U},\ \text{(for all } k \geq 4) \tag{A.17} $$

which leads to $\xi \geq 0$, one has

$$ N_s = n_{0s} + p' {a'_1}^L D_1 + p' {a'_2}^L D_2 + p' \frac{{a'_3}^L}{{a_3}^U}\Lambda_1 + p'\xi + \xi_3. \tag{A.18} $$

Combining Eqs. (A.7) and (A.18), one has

$$ D_2 = \frac{\frac{{a'_3}^L}{p_1} N_{d1} - \frac{a_3^U}{p'} N_s - \frac{{a'_3}^L}{p_1} n_{0d1} + \frac{a_3^U}{p'} n_{0s} + (a_3^U {a'_1}^L - {a'_3}^L a_1^U) D_1 + \frac{{a'_3}^L}{p_1}\xi_1 + \frac{a_3^U}{p'}(\xi_3 + p'\xi)}{{a'_3}^L a_2^U - a_3^U {a'_2}^L}. \tag{A.19} $$

Since ξ_1, ξ_3 and ξ are all non-negative, ${a'_3}^L a_2^U - a_3^U {a'_2}^L \geq 0$ and ${a'_3}^L a_1^U - a_3^U {a'_1}^L \geq 0$, one has

$$ D_2 \geq \frac{\frac{{a'_3}^L}{p_1} N_{d1} - \frac{a_3^U}{p'} N_S - \frac{{a'_3}^L}{p_1} n_{0d1}^U + \frac{a_3^U}{p'} n_{0s}^L + (a_3^U {a'_1}^L - {a'_3}^L a_1^U) D_1^U}{{a'_3}^L a_2^U - a_3^U {a'_2}^L}. \tag{A.20} $$

It is clear that $N_{d2} \geq n_{0d2}^L + p_2 b_1^L D_1 + p_2 b_2^L D_2$. Then one has

$$D_1 \leq \frac{N_{d2} - n_{0d2}^L}{p_2 b_1^L} - \frac{b_2^L}{b_1^L} D_2 = D_1^U. \tag{A.21}$$

Combine the results of Eqs. (A.20) and (A.21), one has

$$D_2 \geq D_2^L = \frac{\frac{{a_3'}^L}{p_1} N_{d1} - \frac{a_3^U}{p'} N_S - \frac{{a_3'}^L}{p_1} n_{0d1}^U + \frac{a_3^U}{p'} n_{0s}^L + (a_3^U {a_1'}^L - {a_3'}^L a_1^U) \frac{N_{d2} - n_{0d2}^L}{p_2 b_1^L}}{c({a_3'}^L a_2^U - a_3^U {a_2'}^L)}, \tag{A.22}$$

under conditions $\frac{{a_k'}^L}{a_k^U} \geq \frac{{a_3'}^L}{a_3^U} \geq \frac{{a_2'}^L}{a_2^U} \geq \frac{{a_1'}^L}{a_1^U}$ (for all $k \geq 4$) and $c = 1 + \frac{a_3^U {a_1'}^L - {a_3'}^L a_1^U}{{a_3'}^L a_2^U - a_3^U {a_2'}^L} \frac{b_2^L}{b_1^L} > 0$. Further, one can estimate the lower bound of gain of 2-photon state in signal source $Q_2 \geq \frac{{a_2'}^L D_2^L}{M}$ as shown in Eq. (6). It is clear that once the condition in Eq. (A.17) is satisfied, the condition in Eq. (A.12) is also satisfied. To lower bound the gain of Q_1 and Q_2 with Eqs. (A.15) and (A.22), one only need to verify the conditions

$$\frac{{a_k'}^L}{a_k^U} \geq \frac{{a_3'}^L}{a_3^U} \geq \frac{{a_2'}^L}{a_2^U} \geq \frac{{a_1'}^L}{a_1^U} \text{ (for all k} \geq 4), \ \mathrm{c} = 1 + \frac{\mathrm{a}_3^\mathrm{U} {\mathrm{a}_1'}^\mathrm{L} - {\mathrm{a}_3'}^\mathrm{L} \mathrm{a}_1^\mathrm{U}}{{\mathrm{a}_3'}^\mathrm{L} \mathrm{a}_2^\mathrm{U} - \mathrm{a}_3^\mathrm{U} {\mathrm{a}_2'}^\mathrm{L}} \frac{\mathrm{b}_2^\mathrm{L}}{\mathrm{b}_1^\mathrm{L}} > 0. \tag{A.23}$$

Appendix B

The APN of signal source is $\mu \sim O(10^{-1})$ while the APN of decoy-1 source is $v_1 \sim O(10^{-2})$. When the data size is finite (e.g. $M = 10^{12}$), one may always observe that $j_m^{d1} = 0$ for all $m > J$ while $j_{m=J}^{d1} > 0$ (e.g. $J = 10$) in a real experiment, which is a cutoff value of the detected photoelectron number m. The counts caused by the photon number states $m > J$ in decoy-1 source can be ignored in the experiment. For instance, given that the PND of the decoy-1 source is Poissonian with an APN $v_1 = 0.01$, the probability that the decoy-1 source sends out photon number states $n > 10$ is less than 10^{-25}, which can be ignored for data size $M = 10^{12}$.

Suppose that one observe $j_m^{d1} = 0$ for all $m > J$ while $j_{m=J}^{d1} > 0$, and $j_m^s = 0$ for all $m > J'$ while $j_{m=J'}^s > 0$ ($J' \geq J$) in a real experiment. Generally one can assume $J' \geq J$ due to that the signal intensity of signal source is much strongger than that of decoy-1 source. Similar to Eqs. (A.6), one has

$$Q_{d1} = \sum_{k=0}^{J} Q_k^{d1} + \sum_{k=J+1}^{\infty} Q_k^{d1}, \tag{B.1}$$

where $Q_{d1} = N_{d1}/M_1$ is the count rates of the decoy-1 source, and $Q_k^{d1} = p_1 \sum_{i \in c_k} a_{ki} d_{ki}/M_1$ is the gain of k-photon state in decoy-1 source which can be explained as the probability that Alice produces a k-photon pulse in decoy-1 source and the pulse causes a count at Bob's detectors. Clearly, $Q_k^{d1} \leq a_k$ and $Q_{d1} \leq \sum_{k=0}^{J} Q_k^{d1} + \sum_{k=J+1}^{\infty} a_k$, which infers,

$$N_{d1} \leq n_{0d1} + p_1 \sum_{k=1}^{J} \sum_{i \in c_k} a_{ki} d_{ki} + M_1 P_J, \tag{B.2}$$

where $P_J = \sum_{k=J+1}^{\infty} a_k$. Using the Clopper-Pearson confidence interval theory [47], one can upper bound P_J with a confidence level $1 - \alpha$, where $(1 - P_J^U)^{M_1} = \alpha/2$ and $P_J^U \sim \frac{1}{M_1}$ is the upper bound of P_J. Similar to Eqs. (A.6), one has

$$\begin{aligned} N'_{d1} &\leq n_{0d1} + p_1 \sum_{i\in c_1} a_{1i} d_{1i} + p_1 \sum_{i\in c_2} a_{2i} d_{2i} + p_1 \sum_{k=3}^{J} \sum_{i\in c_k} a_{ki} d_{ki}, \\ N_s &\geq n_{0s} + p' \sum_{i\in c_1} a'_{1i} d_{1i} + p' \sum_{i\in c_2} a'_{2i} d_{2i} + p' \sum_{k=3}^{J} \sum_{i\in c_k} a'_{ki} d_{ki}, \end{aligned}$$

where $N'_{d1} = N_{d1} - M_1 P_J^U$. Then one can calculate the lower bounds of D_1 and D_2 the same as Eqs. (A.15) and (A.22) except replacing the N_{d1} by N'_{d1}, and the condition in Eq. (7) is replaced by

$$\frac{{a'_k}^L}{a_k^U} \geq \frac{{a'_3}^L}{a_3^U} \geq \frac{{a'_2}^L}{a_2^U} \geq \frac{{a'_1}^L}{a_1^U}, \text{ (for all } 4 \leq \text{k} \leq \text{J).} \tag{B.3}$$