Quantum key distribution with an unknown and untrusted source

Yi Zhao, Bing Qi, and Hoi-Kwong Lo
Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, Canada M5S 3G4
(Received 20 February 2008; published 20 May 2008)

The security of a standard bidirectional "plug-and-play" quantum key distribution (QKD) system has been an open question for a long time. This is mainly because its source is equivalently controlled by an eavesdropper, which means the source is unknown and untrusted. Qualitative discussion on this subject has been made previously. In this paper, we solve this question directly by presenting the quantitative security analysis on a general class of QKD protocols whose sources are unknown and untrusted. The securities of standard Bennett-Brassard 1984 protocol, weak+vacuum decoy state protocol, and one-decoy state protocol, with unknown and untrusted sources are rigorously proved. We derive rigorous lower bounds to the secure key generation rates of the above three protocols. Our numerical simulation results show that QKD with an untrusted source gives a key generation rate that is close to that with a trusted source.

DOI: 10.1103/PhysRevA.77.052327 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) [1–3], when combined with the one-time pad algorithm, provides unconditional communication security. The unconditional security is rigorously proved based on fundamental physics principles such as quantum no-cloning theorem and Heisenberg's uncertainty principle [4] rather than unproven computational complexity assumptions. The unconditional security of QKD has been proven even when implemented on imperfect practical setups with coherent laser sources and semi-realistic models [5,6].

Unconditional security of quantum cryptography is different from "absolute security." "Unconditional" in the security proof of QKD means that we are not making any assumption about Eve's technology, except that quantum mechanics is correct. However, we do have to make assumptions on Alice's and Bob's sides to ensure the security. The concept of unconditional security in QKD is discussed in details in [7].

Recently, the ideas of device-independent security proofs of QKD and security from causality constraints have been proposed [8–10], but a complete proof of unconditional security along those lines is still missing. Moreover, any such device-independent security proofs, even if successfully constructed in the future, will not be applicable practical QKD systems due to the well-known detection efficiency loophole. This loophole can be filled under the fair sampling assumption. Unfortunately, the fair sampling assumption can be invalid in practical QKD setups due to some imperfections, such as the detection efficiency mismatch. Indeed, the detection efficiency mismatch opens a back door for several practical attacks, including the faked states attack [11,12] and the time-shift attack [13]. The latter attack has even been experimentally demonstrated on a commercial QKD system [14], thus highlighting the weakness of practical QKD systems.

It is very important to develop security proofs with testable assumptions, and test the assumptions both theoretically and experimentally. For example, the assumption of phase randomization is often made in security proofs of practical setups. However, the phases of signals are not naturally randomized in practice. Fortunately, the validity of the phase-randomization assumption can be confidently guaranteed by actively randomizing the phase of each signal, which has only been demonstrated in a recent experiment [15]. See, however [16], for a security proof that does not require the phase randomization assumption.

The validity of the coherent state assumption is also questionable. For example, it is common to use pulsed laser diodes as sources in QKD experiments. These laser diodes are driven by pulsed electrical currents. When the driving current is switched on, it will take a short while before the laser's gain reaches its stabilizing threshold. During this transition period, the output from the diode cannot be viewed as coherent state. Therefore, it is not rigorous to consider the entire pulse as a coherent state.

A more severe problem comes from the standard bidirectional (so-called "plug-and-play") design [17], which is widely used in commercial QKD systems. In this particular scheme, bright pulses are generated by Bob (a receiver) rather than Alice (a sender). The pulses will travel through the channel, which is fully controlled by Eve (an eavesdropper), before entering Alice's laboratory to get encoded and sent back to Bob. Eve can perform arbitrary operation on the pulses when they are sent from Bob to Alice. In the worst case, Eve can replace the original pulses by her own sophisticatedly prepared optical signals. Such an attack is called the Trojan horse attack [18]. Therefore, it is highly risky to assume that Alice uses a coherent state source in the security analysis of "plug-and-play" QKD systems.

Previously, a qualitative argument on the security of the bidirectional QKD system was provided in [18]. The intuition is to show that by applying heavy attenuation, an input state with arbitrary photon number distribution can be transformed into an output state with Poisson-like distribution. However, it is challenging to quantify how close to the Poissonian state the output state is.

We start from another intuition: We look into the actual photon number distribution created by the internal loss of Alice's local laboratory. The phase randomization can transform arbitrary input state into a classical mixture of number states [18]. By modeling the internal loss inside Alice's local laboratory as a beam splitter, for each particular input photon

number, the photon number of output state obeys binomial distribution. Note that this is not a binomial-like, but a rigorous binomial distribution. The analysis of binomial distribution is in general more difficult than that of Poisson distribution. However, in this way we can quantitatively and rigorously analyze its security.

The discovery of decoy methods can dramatically improve the performance (by means of higher key rate and longer transmission distance) of coherent laser based QKD systems [19–26]. The decoy method has been experimentally demonstrated over long distances [27–34].

In decoy state QKD, each bit is randomly assigned as a signal state or one of the decoy states. Each state has its unique average photon number. These states can be prepared by setting different internal transmittances λ in Alice's local laboratory. For example, if a bit is assigned as a signal state, the internal transmittance for this bit will be λ_S. If a bit is assigned as a decoy state, the internal transmittance for this bit will be $\lambda_D \neq \lambda_S$. Normally $\lambda_D < \lambda_S$.

In previous analysis on decoy state QKD [20–22,26], one important assumption is that the yield of n-photon state Y_n in signal state is the same as Y_n in decoy state, i.e., $Y_n^S = Y_n^D$. Here Y_n is defined as the conditional probability that Bob's detectors generate a click given that Alice sends out an n-photon signal. This is true because in the analysis of [20–22,26] Eve knows only the output photon number n of each pulse. Another fundamental assumption is that the quantum bit error rate (QBER) of n-photon state e_n in signal state is the same as e_n in decoy state. i.e., $e_n^S = e_n^D$. Note that, once Eve knows some additional information about the source, the above two fundamental assumptions will fail [35].

We emphasize that in the case of "plug-and-play" QKD, Eve knows both the input photon number m and the output photon number n. Therefore, she can perform an attack that depends on the values of both m and n. In Sec. VI A and Appendix A, we show explicitly that $Y_n^S \neq Y_n^D$ and $e_n^S \neq e_n^D$ in this case. The parameters that are the same for both the signal state and the decoy states are $Y_{m,n}$ (the conditional probability that Bob's detectors click given that this bit enters Alice's laboratory with photon number m and emits from Alice's laboratory with photon number n) and $e_{m,n}$ (the QBER of bits with m input photons and n output photons).

In brief, there is more information available to Eve once she controls the source. The security analysis for decoy state QKD in this case is much more challenging.

In this paper, we analyze the most general case: We consider the source as controlled by Eve. Therefore, the source is completely unknown and untrusted. Rather surprisingly, we show that even in this most general case, the security of the QKD system can be analyzed quantitatively and rigorously. We also show that the decoy method can still be used to enhance the performance of the system dramatically when the source is unknown and untrusted. For the first time, we show quantitatively that the security of "plug-and-play" QKD system is understandable and achievable. Moreover, we show what measures are necessary to ensure the security of the QKD system, and rigorously derive a lower bound of the secure key generation rate. Our numerical simulation results show that QKD with an untrusted source gives a key generation rate that is close to that with a trusted source.

It is important to implement QKD with testable assumptions. In this paper, we showed that the coherent source assumption can be removed. Nonetheless, we still keep a few standard assumptions including single mode assumption, phase randomization assumption, etc., in our security proof. To ensure that our assumptions of single-mode and phase randomization are satisfied in practice, we propose specific experimental measures for Alice to implement. More concretely, we propose that Alice uses a strong filter to filter out other optical modes and uses active phase randomization to achieve phase randomization. It would be interesting to see the security consequence of removing, say, the single mode assumption. However, this is beyond the scope of this work.

This paper is organized in the following way: in Sec. II, we propose some measures that should be included in the QKD setup, and a key term—"untagged bit"—is defined; in Sec. III, we study the experimental properties of the untagged bits; in Sec. IV, the photon number distribution for untagged bits is analyzed; in Sec. V, we prove the security of practical QKD system with unknown and untrusted source, and explicitly show the equation for the key generation rate; in Sec. VI, we prove the security of two decoy state protocols—the weak+vacuum protocol and the one-decoy protocol—with unknown and untrusted sources; in Sec. VII, numerical simulation results are shown; in Sec. VIII, we present our conclusion and discuss future directions.

II. MEASURES TO ENHANCE THE SECURITY

Here we will use three measures, which were briefly mentioned in [18], to enhance the security of the system. A general system that has applied these measures is shown in Fig. 1. There are various sources of losses inside Alice's apparatus. Here we model all the losses as a $\lambda/(1-\lambda)$ beam splitter. That is, the internal transmittance of Alice's local laboratory is λ. We assume that Alice can set λ accurately via, say, variable optical attenuator. In other words, for any photon that enters the encoding arm, it has a probability λ to get encoded and sent out from Alice.

(1) We pointed out and demonstrated in [14] that the side channel can be exploited by Eve to acquire additional information. To shut down these side channels, we need to place a filter (filter in Fig. 1) which works in spectral, spatial, and temporal domains. In other words, only pulses of the desired mode can pass through the filter. Therefore, we can use single mode assumption for each signal. Incidentally, the single mode assumption may not hold for an open-air QKD setup. This is because (1) the free space will not suppress the propagation of higher modes and (2) the collection system at Bob's side can only collect part of the beam sent from Alice.

(2) The phase randomization is a general assumption made in most security proofs on practical setups [5,6,20]. It can disentangle the input pulse from Eve by transforming it into a classical mixture of Fock states $\Sigma_{n=0}^{\infty} p_n |n\rangle\langle n|$ [18]. Its feasibility has been experimentally demonstrated [15]. Alice should apply the phase randomization on the input optical signals. In Fig. 1, this is accomplished by the phase randomizer.

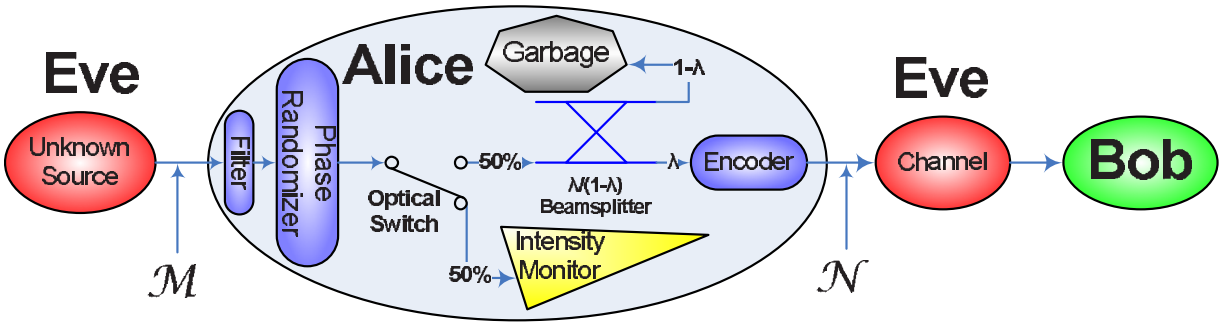

FIG. 1. (Color online) A schematic diagram of the setup that coped with the three measures as suggested: Filter is used to guarantee the single mode assumption; phase randomizer is used to guarantee the phase randomization assumption; optical switch and intensity monitor are used to randomly sample the photon number of input pulses. All of the internal losses inside Alice's local laboratory are modeled as a $\lambda/(1-\lambda)$ beam splitter. That is, any input photon has λ probability to get encoded and sent from Alice to Bob, and $1-\lambda$ probability to be discarded into the garbage. $\mathcal{M}$ and $\mathcal{N}$ are the random variables for input photon numbers and output photon numbers, respectively. Note that in a standard "plug-and-play" setup, the actual source is inside Bob's local laboratory. However, Eve can replace the pulses sent by Bob with arbitrary optical signals. This is equivalent to the general case in which Eve controls the source.

(3) We need to monitor the pulse energy to acquire some information about the photon number distribution. By randomly sampling a portion of the pulses to test the photon numbers, we can estimate some bounds on the output photon number distribution as shown in the following sections. In Fig. 1, this is accomplished by the optical switch and the intensity monitor.

Suppose that $2K$ pulses entered Alice's local laboratory, within which K pulses were randomly chosen by the optical switch in Fig. 1 for testing photon numbers (these pulses are called "sampling bits"), and the rest of the K pulses were encoded and sent to Bob (these pulses are called "coding bits"). Define the pulses with photon number $m \in [(1-\delta)N, (1+\delta)N]$ as "untagged" bits, and pulses with photon number $m < (1-\delta)N$ or $m > (1+\delta)N$ as "tagged" bits. Note that the definitions of "untagged" and "tagged" here are different from those in [5]. From random sampling theorem (see Ref. [36]) we know that the probability that there are less than $K\Delta$ tagged sampling bits and more than $(\Delta+\varepsilon)K$ tagged coding bits is asymptotically less than $e^{-O(\varepsilon^2 K)}$. ε should be chosen under the condition that $\varepsilon^2 K \gg 1$. Therefore, there are no less than $(1-\Delta-\varepsilon)K$ untagged coding bits with high fidelity.

In the following discussion, we will focus on these $(1-\Delta-\varepsilon)K$ untagged bits. Of course, there can also be some untagged bits in the rest $(\Delta+\varepsilon)K$ bits, but neglecting these out-of-scope untagged bits just makes our analysis conservative.

N and δ can, in principle, be arbitrarily chosen. However, some constraints will be applied to optimize the key generation rate. We will discuss the optimal choice later.

III. PROPERTIES OF THE UNTAGGED BITS

In QKD experiments, the two most important measurable outputs are the gain [37] and the QBER. In our analysis, we are more interested in the gain and the QBER of the untagged bits. This is because the input photon numbers of the untagged bits are concentrated within a narrow range, making it much easier to analyze the security.

However, Alice cannot in practice perform quantum nondemolition (QND) measurement on the photon number of the input pulses with current technology. Therefore, she does not know which bits are tagged and which are untagged. As a result, the gain [37] Q and the QBER E of the untagged bits cannot be measured experimentally. Here Q is defined as the conditional probability that Bob's detector clicks given that Alice sends out an untagged bit and Alice and Bob use the same basis; E is defined as the conditional probability that Bob's bit value is different from Alice's given that Bob's detector clicks, Alice sends out an untagged bit, and Alice and Bob use the same basis.

In an experiment, Alice and Bob can measure the overall gain Q_e and the overall QBER E_e. The subscript e denotes the experimentally measurable overall properties. Moreover, they know the probability of that certain bit to be tagged or untagged from the above analysis. Although they cannot measure the gain Q and the QBER E of the untagged bits directly, they can estimate the upper bounds and lower bounds of them. The upper bound and lower bound of Q are

$$\bar{Q} = \frac{Q_e}{1-\Delta-\varepsilon}, \tag{1}$$

$$\underline{Q} = \max\left(0, \frac{Q_e - \Delta - \varepsilon}{1-\Delta-\varepsilon}\right).$$

The upper bound and lower bound of EQ can be estimated as

$$\overline{EQ} = \frac{Q_e E_e}{1-\Delta-\varepsilon}, \tag{2}$$

$$\underline{EQ} = \max\left(0, \frac{Q_e E_e - \Delta - \varepsilon}{1-\Delta-\varepsilon}\right).$$

To get tighter bounds on Q and EQ, we need to minimize Δ, which means that δ should be made large so as to minimize the amount of tagged bits. See, however, discussion after Eqs. (4).

IV. PHOTON NUMBER DISTRIBUTION OF UNTAGGED BITS

Consider an untagged bit with input photon number $m \in [(1-\delta)N, (1+\delta)N]$. The conditional probability that n photons are emitted by Alice's laboratory given that m photons enter Alice's laboratory obeys binomial distribution as

$$P_n(m) = \binom{m}{n} \lambda^n (1-\lambda)^{m-n} \quad (0 \le \lambda \le 1). \tag{3}$$

For untagged bits (i.e., $m \in [(1-\delta)N, (1+\delta)N]$), we can show that the upper bound and lower bound of $P_n(m)$ are

$$\overline{P_n} = \begin{cases} (1-\lambda)^{(1-\delta)N} & \text{if } n = 0, \\ \binom{(1+\delta)N}{n} \lambda^n (1-\lambda)^{(1+\delta)N-n} & \text{if } 1 \le n \le (1+\delta)N, \\ 0 & \text{if } n > (1+\delta)N, \end{cases} \tag{4}$$

$$\underline{P_n} = \begin{cases} (1-\lambda)^{(1+\delta)N} & \text{if } n = 0, \\ \binom{(1-\delta)N}{n} \lambda^n (1-\lambda)^{(1-\delta)N-n} & \text{if } 1 \le n \le (1-\delta)N, \\ 0 & \text{if } n > (1-\delta)N, \end{cases}$$

under Condition 1,

$$(1+\delta)N\lambda < 1. \tag{5}$$

Condition 1 suggests that the expected output photon number of any untagged bit should be lower than 1. This is easy to implement experimentally. For example, for $N = 10^6$, Alice can simply set $\lambda = 10^{-7}$ so that the expected output photon number is 0.1. Most reported Bennett-Brassard 1984 (BB84) implementations satisfy Condition 1.

To get tighter bounds on $P_n(m)$, we need to minimize δ. However, as we discussed below Eq. (2), minimizing δ will lower the amount of untagged bits (i.e., there will be fewer pulses that contain photon number $m \in [(1-\delta)N, (1+\delta)N]$ as the bound becomes narrower), thus loosening the bounds on the gains and QBERs of untagged bits. As a summary, there is a trade-off between the tightness of the bounds of $P_n(m)$ and the tightness of the bounds of Q and EQ. The optimal choice of δ depends on the properties of specific system, and can be obtained numerically.

V. GENERALIZED GOTTESMAN-LO-LÜTKENHAUS-PRESKILL RESULTS WITH UNTRUSTED SOURCE

From the work of Gottesman-Lo-Lütkenhaus-Preskill (GLLP) [5], the secure key generation rate of standard BB84 protocol [1] is given by

$$R \ge \frac{1}{2}\left\{ -Q_e f(E_e) H_2(E_e) + \underline{Q\Omega}\left[1 - H_2\left(\frac{Q_e E_e}{\underline{Q\Omega}} \right) \right] \right\}, \tag{6}$$

where 1/2 is the probability that Alice and Bob use the same basis, Q_e and E_e are obtained experimentally, $f(>1)$ is the bidirectional error correction inefficiency [38], and

$$\Omega = 1 - \frac{P_M}{Q}, \tag{7}$$

where $P_M = \Sigma_{n=2}^{\infty} P_n(m)$ is the probability of output multiphoton signals. Recall that if the input photon number $m = (1+\delta)N$, we have

$$P_n[(1+\delta)N] = \begin{cases} \underline{P_n} & \text{if } n = 0, \\ \overline{P_n} & \text{if } n \ge 1. \end{cases}$$

Therefore, $\underline{P_0} + \Sigma_{n=1}^{\infty} \overline{P_n} = 1$. The upper bound of P_M is $\overline{P_M} = \Sigma_{n=2}^{\infty} \overline{P_n} = 1 - \underline{P_0} - P_1$, and the lower bound of Ω is

$$\underline{\Omega} = 1 - \frac{\overline{P_M}}{\underline{Q}}.$$

The lower bound of $Q\Omega$ is thus given by

$$\underline{Q\Omega} = \underline{Q} - \overline{P_M} = \underline{Q} + \underline{P_0} + \overline{P_1} - 1, \tag{8}$$

where $\underline{Q}$ can be obtained via Eq. (1).

Plugging Eq. (8) into Eq. (6), we have the key generation rate per bit sent by Alice, given that an untrusted source is used, as

$$R \ge \frac{1}{2}\left\{ -Q_e f(E_e) H_2(E_e) + (\underline{Q} + \underline{P_0} + \overline{P_1} - 1) \times \left[1 - H_2\left(\frac{Q_e E_e}{\underline{Q} + \underline{P_0} + \overline{P_1} - 1} \right) \right] \right\}. \tag{9}$$

The numerical simulation of the above analysis is presented in Sec. VII.

VI. COMBINING WITH DECOY STATES

Decoy method [19–25] significantly improves the performance for QKD systems with coherent state source. Here, we will show that the idea of decoy states can also be useful when the source is unknown and untrusted.

A. Weak+vacuum protocol

Among all the decoy state protocols, the weak+vacuum protocol is the most popular one. It is shown to be the optimal protocol in the asymptotic case [22]. "Asymptotic" here means infinitely long source data sequence. The weak+vacuum protocol has been used in most experimental decoy state QKD implementations [28–32].

In weak+vacuum protocol, there are three states: The signal state (for which the internal transmittance of Alice is λ_S), the weak decoy state (for which the internal transmittance of Alice is $\lambda_D < \lambda_S$), and the vacuum state (for which the internal transmittance of Alice is 0). We consider that only the signal state is used to generate the final key, while the decoy states are solely used to test the channel properties.

The error correction will consume

$$r_{\mathrm{EC}} = Q_e^S f(E_e^S) H_2(E_e^S) \tag{10}$$

bit per signal sent from Alice, where Q_e^S and E_e^S are the overall gain and overall QBER of signal state, H_2 is binary Shannon function.

The probability that Alice sends out an untagged signal which is securely transmitted to Bob is

$$r_{\mathrm{PA}} = (1-\Delta-\varepsilon)Q_1^S[1-H_2(e_1^S)], \tag{11}$$

where Q_1^S and e_1^S are the gain and the QBER of single photon state in untagged bits. This is because Alice and Bob can, in principle, measure the input photon number m and the output photon number n accurately and therefore post-select the untagged bits with $n=1$. They can then use these post-selected single photon untagged bits to generate the secure key. In practice, QND measurements on m and n by Alice are not feasible with current technology. However, Alice and Bob know the probability of a certain bit to be untagged. They can use random-hashing method to perform privacy amplification to distill the secure key. Similar technique was used in [5].

The key generation rate in standard BB84 protocol is therefore given by

$$\begin{aligned} R &\geq \frac{1}{2}(r_{\mathrm{PA}} - r_{\mathrm{EC}}) \\ &\geq \frac{1}{2}\{-Q_e^S f(E_e^S)H_2(E_e^S) + (1-\Delta-\varepsilon)\underline{Q_1^S}[1-H_2(\overline{e_1^S})]\}, \end{aligned} \tag{12}$$

where 1/2 is the probability that Alice and Bob use the same basis.

Q_e^S, E_e^S, Δ, and ε can be determined experimentally. Our main task is to estimate $\underline{Q_1^S}$ and $\overline{e_1^S}$.

In previous analysis on decoy state QKD [20–22,26], one important assumption is that the yield of n-photon state Y_n in signal state is the same as Y_n in decoy state. i.e., $Y_n^S = Y_n^D$. Here Y_n is defined as the conditional probability that Bob's detectors generate a click given that Alice sends out an n-photon signal. This is true because in the analysis of [20–22,26] Eve knows only the output photon number n of each pulse. However, as we will show below, this assumption is no longer valid in the case that the source is controlled by Eve.

The key point is that Eve knows both the input photon number m and the output photon number n when she controls both the source and the channel. Therefore, she can perform an attack that depends on the values of both m and n. In this case, the parameter that is the same for these states is $Y_{m,n}$, the conditional probability that Bob's detectors click given that this bit enters Alice's laboratory with photon number m and is emitted from Alice's laboratory with photon number n. In this case, Y_n is given by (see Appendix A for details)

$$Y_n = \sum_m P\{m|n\}Y_{m,n}, \tag{13}$$

where $P\{m|n\}$ is the conditional probability that the signal enters Alice's local laboratory with photon number m given that it is emitted from Alice's laboratory with photon number n. Note that $P\{m|n\}$ is dependent on the internal transmittance of Alice's apparatus λ. Since $\lambda_S \neq \lambda_D$, we know that $Y_n^S \neq Y_n^D$.

Another fundamental assumption for previous decoy state security studies [20–22] is that the QBER of n-photon state e_n is the same for signal state and decoy state, i.e., $e_n^S = e_n^D$. Unfortunately, from a similar analysis as above, we can show that $e_n^S \neq e_n^D$ if Eve controls the source. The parameter that is the same for the signal state and the decoy states is $e_{m,n}$.

As a brief summary, in decoy state QKD, if the source is in Alice's local laboratory and is solely accessible to Alice (that is, the source is trusted), we have $Y_n^S = Y_n^D$ and $e_n^S = e_n^D$, whereas if the source is out of Alice's local laboratory and is accessible to Eve (that is, the source is untrusted), we have $Y_{m,n}^S = Y_{m,n}^D$ and $e_{m,n}^S = e_{m,n}^D$.

The dependence of Y_n and e_n on different states (signal state or one of the decoy states) is a fundamental difference between decoy state QKD with untrusted source and decoy state QKD with trusted source. In the latter case, the independence of Y_n and e_n on different states is a very powerful constraint on Eve's ability of eavesdropping. However, this constraint is removed once the source is given to Eve.

Eve's control over the source removes the two fundamental assumptions in [20–22]. Eve is given significantly greater power, and the security analysis is much more challenging. However, rather surprisingly, it is still possible to achieve the unconditional security quantitatively even if the source is given to Eve. This is mainly because we are only focusing on the untagged bits, whose input photon numbers are concentrated in a relatively narrow range. Therefore, we are still able to estimate $\underline{Q_1^S}$ and $\overline{e_1^S}$.

Proposition 1. The lower bound of Q_1^S for untagged bits is given by

$$Q_1^S > \underline{Q_1^S} = \underline{P_1^S}\frac{\underline{Q^D P_2^S} - \overline{Q^S P_2^D} + (\underline{P_0^S P_2^D} - \overline{P_0^D P_2^S})\overline{Q^V} - \dfrac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}}{\overline{P_1^D}\,\underline{P_2^S} - \underline{P_1^S}\,\overline{P_2^D}} \tag{14}$$

under Condition 2,

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-2}{(1-\delta)N-2}\left(\frac{(1+\delta)N-2}{2\delta N}\right)^{2\delta N/[(1-\delta)N-2]}\left(\frac{(1+\delta)N-2}{(1-\delta)N-2}\frac{e^2}{2\delta N}\right)^{1/2[(1-\delta)N-2]}. \tag{15}$$

Here Q^S, Q^D, and Q^V are the gains of untagged bits of the signal state, the decoy state, and the vacuum state, respectfully. Their bounds can be estimated from Eqs. (1). The bounds of the probabilities can be estimated from Eqs. (4). Note that Condition 2 is easy to meet. For example, in the numerical simulation in Sec. VII, we choose $N=10^6$ and $\delta=0.01$. In this case we can calculate Condition 2 as $\frac{\lambda_S}{\lambda_D}>1.104$, which is very reasonable to meet experimentally. Actually, λ_S/λ_D is usually greater than 2 in previous decoy state QKD implementations [27–34].

Proof. See Appendix B.

Proposition 2. The upper bound of e_1^S for untagged bits is given by

$$e_1^S \le \overline{e_1^S} = \frac{\overline{E^S Q^S} - \underline{P_0^S} E^V Q^V}{\underline{Q_1^S}}, \tag{16}$$

in which E^S and E^V are the QBERs of untagged bits of the signal and the vacuum states, respectively. $\overline{E^S Q^S}$ and $\overline{E^V Q^V}$ can be estimated from Eqs. (2). $\underline{P_0^S}$ can be estimated by Eqs. (4). $\underline{Q_1^S}$ is given by Eq. (14).

Proof. See Appendix C.

Plugging Eqs. (14) and (16) into Eq. (12), we can easily calculate the overall key generation rate of weak+vacuum decoy state QKD protocol given the source is under Eve's control.

B. One-decoy protocol (asymptotic case)

The one-decoy protocol is the simplest decoy state protocol. In the one-decoy protocol, there are only two states: a signal state and a weak decoy state. It can be viewed as a simplified version of the weak+vacuum protocol since it does not have the vacuum state.

The one-decoy protocol is of practical interest, particularly due to the difficulty of preparing perfect vacuum state. It has also been widely used in experiments [27,33,34].

Here, we will show that the one-decoy protocol is also applicable when the source is under Eve's control in the asymptotic case. The asymptotic case means that Alice sends infinitely long bit sequence ($K\sim\infty$).

In the one-decoy protocol, there is no vacuum state. Therefore, we cannot measure $\overline{Q_e^V}$ or E_e^V, which means we cannot use Eqs. (1) to estimate $\overline{Q^V}$ in Eq. (14) or use Eqs. (2) to estimate $\overline{E^V Q^V}$ in Eq. (16). Nonetheless, we can still estimate $\underline{Q_1^S}$ and $\overline{e_1^S}$.

Proposition 3. In absence of the vacuum state, a lower bound of Q_1^S and an upper bound of e_1^S for untagged bits are given by

$$\underline{Q_1^S} = \underline{P_1^S}\frac{\underline{Q^D P_2^S} - \overline{Q^S P_2^D} + (\underline{P_0^S P_2^D} - \overline{P_0^D P_2^S})\frac{\overline{E^S Q^S}}{\underline{P_0^S} E^V} - \frac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}}{\overline{P_1^D P_2^S} - \underline{P_1^S P_2^D}}, \tag{17}$$

$$\overline{e_1^S} = \frac{\overline{E^S Q^S}}{\underline{Q_1^S}},$$

respectively, under Condition 2 in the asymptotic case. Here Q^S and Q^D are the gains of untagged bits of the signal state and the decoy state, respectively. Their bounds can be estimated from Eqs. (1). E^S is the QBER of untagged bits of the signal state. $\overline{E^S Q^S}$ can be estimated from Eqs. (2). $E^V=0.5$ in the asymptotic case. The bounds of the probabilities can be estimated from Eqs. (4).

Proof. See Appendix D.

Plugging Eqs. (17) into Eq. (12), we can easily calculate the overall key generation rate of one-decoy protocol given the source is under Eve's control.

VII. NUMERICAL SIMULATION WITH COHERENT SOURCE: ASYMPTOTIC CASE

In the asymptotic case, Alice sends infinitely long bit sequence ($K\sim\infty$). Therefore we can consider $\varepsilon\sim 0$.

A. Calculating Δ

For any $\delta\in[0,1]$, we can calculate Δ by

$$\Delta = 1 - [\Phi(N+\delta N) - \Phi(N-\delta N)], \tag{18}$$

where Φ is the cumulative distribution function of the photon number for the input pulses.

Most QKD setups are based on coherent sources, which means that the input photon number m obeys Poisson distribution. It is natural to set N to be the average input photon number. For a Poisson distribution centered at N, its cumulative distribution function is given by

$$\Phi_p(x) = \frac{\Gamma(\lfloor x+1\rfloor, N)}{\lfloor x\rfloor!},$$

where $\Gamma(x,y)$ is the upper incomplete Γ function

$$\Gamma(x,y) = \int_y^\infty t^{x-1} e^{-t} dt.$$

It is complicated to calculate $\Phi_p(x)$ numerically, particularly for large x. Therefore, in numerical simulation, we approximate the Poisson distribution by a Gaussian distribution centered at N with a variance $\sigma^2 = N$. Note this is an excellent approximation for large N. The Gaussian cumulative distribution function is given by

$$\Phi_g(x) = \frac{1}{2}\left[1 + \mathrm{erf}\left(\frac{x-N}{\sqrt{2N}}\right)\right], \tag{19}$$

where

$$\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$$

is the error function. Notice that $\mathrm{erf}(x)$ is an odd function, from Eqs. (18) and (19), we have

$$\begin{aligned}\Delta &= 1 - [\Phi_g(N+\delta N) - \Phi_g(N-\delta N)] \\ &= 1 - \frac{1}{2}\left[\mathrm{erf}\left(\frac{\delta N}{\sqrt{2N}}\right) - \mathrm{erf}\left(\frac{-\delta N}{\sqrt{2N}}\right)\right] = 1 - \mathrm{erf}\left(\sqrt{\frac{N}{2}}\delta\right).\end{aligned} \tag{20}$$

B. Simulating experimental outputs

If the photon number of an input pulse obeys Poisson distribution with average photon number N, the photon number of the output signal also follows Poisson distribution with average photon number $N\lambda$.

For a QKD setup with channel transmittance η $(=e^{-\alpha l}$, where α is the loss coefficient and l is the distance between Alice and Bob), Bob's quantum efficiency η_{Bob}, detector intrinsic error rate e_{det}, and background rate Y_0, the gain and the QBER of the signals are expected to be [22]

$$Q_e = Y_0 + 1 - \exp(-\eta\eta_{\mathrm{Bob}} N\lambda), \tag{21}$$

$$E_e = \frac{e_0 Y_0 + e_{\mathrm{det}}[1 - \exp(-\eta\eta_{\mathrm{Bob}} N\lambda)]}{Q_e}.$$

The experimental outputs are clearly determined by Alice's internal transmittance λ which needs to be set before the experiment. In our simulation, the optimal values for λ_S and λ_D are selected numerically via exhaustive search.

With these simulated experimental outputs, we can calculate the lower bound of key generation rate from Eqs. (1), (2), (4), (9), (12), and (14)–(21).

C. Simulation results

Our simulation is based on the parameters reported by [39] as shown in Table I.

We choose to set $N = 10^6$, which is very reasonable: If the wavelength is 1550 nm and the pulse repetition rate is 1 MHz, the average input laser power will be ~0.128 μW, or −38.9 dBm. Even if the channel loss from the source to Alice is 40 dB (~200 km telecom fiber), the required average output power from the source is ~1.28 mW, which can be easily provided by many commercial pulsed laser diodes. We choose δ to be 10 standard deviations as $\delta = 0.01$.

TABLE I. Simulation parameter from Goggy, Yuan, and Shields [39].

η_{Bob}	α	Y_0	e_{det}
4.5%	0.21dB/km	1.7×10^{-6}	3.3%

The simulation result for GLLP protocol is shown in Fig. 2. We can see that the key generation rate with an untrusted source is very close to that with a trusted source. Their difference is almost negligible, and is only visible by magnifying the tail (see the inset).

The simulation result for weak+vacuum protocol is shown in Fig. 3. We can see that the key generation rate with an untrusted source is still very close to that with a trusted source. By simply comparing the maximum transmission distances, we can see that the difference is merely 5 km for weak+vacuum decoy state protocol.

The simulation result for one-decoy protocol is shown in Fig. 4. We can see that the key generation rate with an untrusted source is still very close to that with a trusted source. The difference of maximum transmission distances is merely 8 km.

The above results are surprisingly good because we did not assume any *a priori* knowledge about the source in the security analysis. In other words, Alice and Bob do not know the fact that the source is Poissonian and therefore they cannot assume any photon number distribution.

One important reason for achieving this high performance is that we applied heavy attenuation on the input pulses. Note that the input pulse has ~10^6 photons, while the output pulse has less than one photon on average. The internal attenuation of Alice's local laboratory is greater than −60 dB.

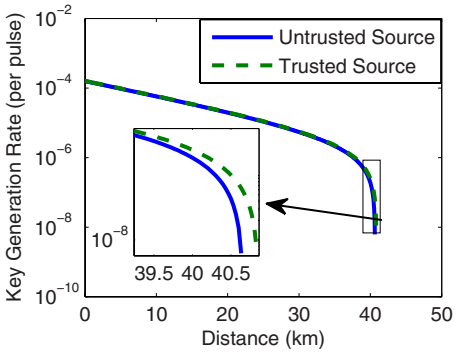

FIG. 2. (Color online) Simulation of GLLP protocol for $N = 10^6$ and $\delta = 1\%$. Citing Gobby, Yuan, and Shields (GYS) [39] data. Inset: the magnified tail. The two cases (with a trusted source and with an untrusted source) give very similar results. We need to magnify the tail (see the inset) to see the slight advantage gained by using a trusted source. We calculated the ratio of the key generation rate with an untrusted source over that with a trusted source. The ratios are 98.0%, 97.7%, and 75.3% at 0 km, 20 km, and 40 km, respectively.

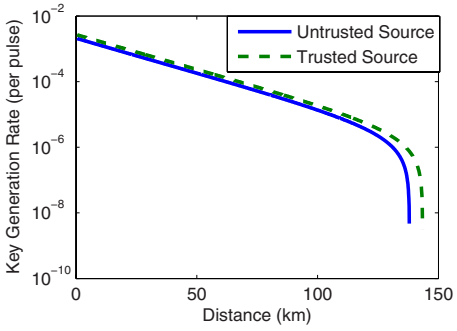

FIG. 3. (Color online) Simulation of weak+vacuum decoy state protocol for $N=10^6$ and $\delta=1\%$. Citing GYS [39] data. The two cases (with a trusted source and with an untrusted source) give very close results. We calculated the ratio of the key generation rate with an untrusted source over that with a trusted source. The ratios are 77.3%, 76.8%, and 73.6% at 0 km, 50 km, and 100 km, respectively.

We know that heavy attenuation will transform arbitrary photon number distribution into a Poisson-like distribution.

As we mentioned before, δ can be arbitrarily chosen. However, choosing δ too large or too small will make the security analysis less optimal (i.e., conservative). Examples are given in Fig. 5. We can clearly see that inappropriate choice of δ can deteriorate the performance of the system. The one-decoy protocol with untrusted source is particularly sensitive to the value of δ.

The analytical optimization of δ can be complicated. Here, we only study this problem numerically. We calculated the maximum possible transmission distances for different δ. The results are shown in Fig. 6. We can clearly see that there is an optimal choice of δ. Note that our analysis is valid for arbitrary value of δ. The optimal value of δ will give us the optimal (while still being rigorous) estimate on the security of the system. Alice and Bob do not need to choose a certain value of δ before the experiment. They only need to find an optimal value of δ during the data post-processing.

The flat top in the curve of Fig. 6 suggests the insensitivity of the maximum transmission distance on δ in a wide range. We can see that the maximum transmission distance

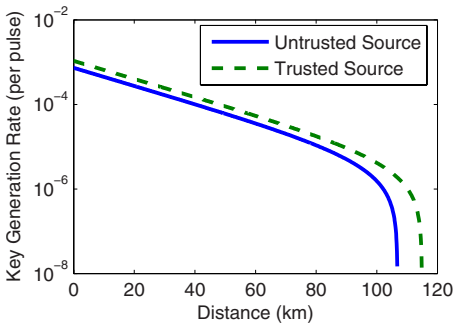

FIG. 4. (Color online) Simulation of one-decoy protocol for $N=10^6$ and $\delta=1\%$. Citing GYS [39] data. The two cases (with a trusted source and with an untrusted source) give very close results. We calculated the ratio of the key generation rate with an untrusted source over that with a trusted source. The ratios are 68.6%, 67.1%, and 37.1% at 0 km, 50 km, and 100 km, respectively.

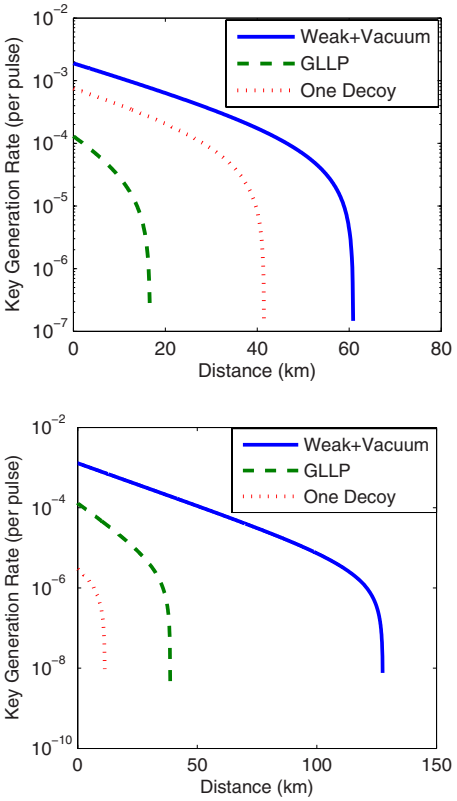

FIG. 5. (Color online) Top: Simulation results for $\delta=0.4\%$. Bottom: Simulation results for $\delta=11\%$. $N=10^6$ in both figures. Citing GYS [39] data.

changes only 8% within the range of δ from 5 standard deviations to 100 standard deviations. Therefore in practice, one can simply set δ to be a few standard deviations and achieve near-optimal results.

VIII. CONCLUSION

In this paper, we present the rigorous quantitative security analysis of a QKD system with an unknown and untrusted source. This analysis is particularly important for the security of a standard "plug-and-play" system. We showed that, rather surprisingly, even with an unknown and untrusted source, unconditional security of a QKD system is still achievable, with and without the decoy method. Moreover, we explicitly give the experimental measures that must be

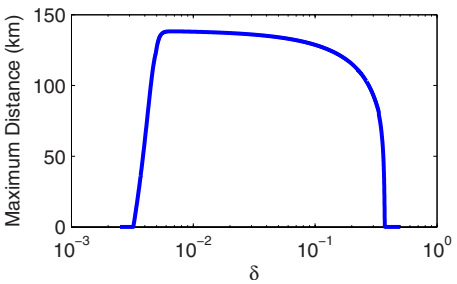

FIG. 6. (Color online) Maximum transmission distances of weak+vacuum protocol for various choices of δ.

taken to ensure the security, and the theoretical analysis that can be directly applied to calculate the final secure key generation rate. One can easily extend our analysis to understand the security of a QKD network, in which the source is often untrusted.

We have made possible the unconditional security of the "plug-and-play" QKD system with current technology. The "plug-and-play" structure has clear advantage over unidirectional structure since it does not require any active compensation on the phase or the polarization. The self-compensating property of the "plug-and-play" structure makes it much simpler to implement than the unidirectional structure, and makes it much quieter (i.e., much lower QBER). Most of the commercial QKD systems [40,41] are based on this simple and reliable structure. However, the lack of rigorous security analysis has been an obstacle for its development for a long time. With our straightforward theoretical and experimental solution, we expect the "plug-and-play" structure to receive much more attention.

The security of practical QKD systems is a serious issue. Recently, several quantum hacking works have been reported [14,42]. It is very important to implement QKD system based on tested assumptions. There are still several crucial imperfections that are not analyzed in this paper. For example, how can we understand the imperfection due to non-single-mode (note that this is particularly important for free-space QKD)? How can we analyze the fluctuation of internal transmittance λ? Also, how can we test the key assumptions in our analysis, $Y^S_{m,n}=Y^D_{m,n}$ and $e^S_{m,n}=e^D_{m,n}$? These questions suggest to us a simple fact: Although we are approaching the unconditional security of practical QKD setup, we are not there yet.

ACKNOWLEDGMENTS

We are thankful for enlightening discussions with C. H. Bennett, C.-H. F. Fung, D. Gottesman, D. F. V. James, X. Ma, J.-W. Pan, L. Qian, and X.-B. Wang. Support of the funding agencies CFI, CIPI, the CRC program, CIFAR, MITACS, NSERC, OIT, and PREA is gratefully acknowledged.

APPENDIX A: DERIVATION OF Y_n

We set $\mathcal{M}$ as the random variable of the input photon number, $\mathcal{N}$ as the random variable of the output photon number, and $\mathcal{C}$ as the random variable of Bob's detector status (y=detection). Y_n is then given by the conditional probability

$$Y_n = \Pr\{\mathcal{C}=\mathrm{y}|\mathcal{N}=n\}, \tag{A1}$$

and $Y_{m,n}$ is given by the conditional probability

$$Y_{m,n} = \Pr\{\mathcal{C}=\mathrm{y}|\mathcal{N}=n \,\&\, \mathcal{M}=m\}. \tag{A2}$$

Y_n can be expended as

$$\begin{aligned} Y_n &= \Pr\{\mathcal{C}=\mathrm{y}|\mathcal{N}=n\} = \frac{\Pr\{\mathcal{C}=\mathrm{y}\,\&\,\mathcal{N}=n\}}{\Pr\{\mathcal{N}=n\}} \\ &= \sum_{m=0}^{\infty} \frac{\Pr\{\mathcal{C}=\mathrm{y}\,\&\,\mathcal{N}=n\,\&\,\mathcal{M}=m\}}{\Pr\{\mathcal{N}=n\}} \\ &= \sum_{m=0}^{\infty} \frac{\Pr\{\mathcal{N}=n\,\&\,\mathcal{M}=m\}}{\Pr\{\mathcal{N}=n\}} \frac{\Pr\{\mathcal{C}=\mathrm{y}\,\&\,\mathcal{N}=n\,\&\,\mathcal{M}=m\}}{\Pr\{\mathcal{N}=n\,\&\,\mathcal{M}=m\}} \\ &= \sum_{m=0}^{\infty} \Pr\{\mathcal{M}=m|\mathcal{N}=n\}\Pr\{\mathcal{C}=\mathrm{y}|\mathcal{N}=n\,\&\,\mathcal{M}=m\} \\ &= \sum_{m=0}^{\infty} P\{m|n\}Y_{m,n}. \end{aligned}$$

APPENDIX B: ESTIMATE OF Q^S_1

From definition [37], we know that the gain of untagged bits is given by

$$Q = \sum_{m=(1-\delta)N}^{(1+\delta)N} \sum_{n=0}^{\infty} P_{\mathrm{in}}(m)P_n(m)Y_{m,n},$$

where $P_{\mathrm{in}}(m)$ is the probability that the input signal contains m photons (i.e., the ratio of the number of signals with m input photons over K), $P_n(m)$ is the conditional probability that the output signal contains n photons given the input signal contains m photons, and is given by Eq. (3).

The gains for signal, decoy, and vacuum states in untagged bits are therefore given by

$$Q^S = \sum_{m=(1-\delta)N}^{(1+\delta)N} \sum_{n=0}^{\infty} P_{\mathrm{in}}(m)P^S_n(m)Y_{m,n}, \tag{B1}$$

$$Q^D = \sum_{m=(1-\delta)N}^{(1+\delta)N} \sum_{n=0}^{\infty} P_{\mathrm{in}}(m)P^D_n(m)Y_{m,n},$$

$$Q^V = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)Y_{m,0},$$

respectively. Here $P^{S(D)}_n(m)$ is $P_n(m)$ for the signal (decoy) state. Their bounds can be estimated from Eqs. (4). $Q^{S(D)V}$ cannot be measured experimentally, but their upper bounds and lower bounds can be estimated from Eqs. (1). Note that $\Delta^{S(D)V}$ should be determined experimentally. In asymptotic case, $\Delta^S=\Delta^D=\Delta^V$. If the bit sequence sent by Alice is finite, $\Delta^{S(D)V}$ may not be exactly the same due to statistical fluctuation.

We know that

$$\begin{aligned} Q^S_1 &= \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)P^S_1(m)Y_{m,1} \geq \underline{P^S_1} \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\mathrm{in}}(m)Y_{m,1} \\ &= \underline{P^S_1}Z_1, \end{aligned} \tag{B2}$$

in which $\underline{P^S_1}$ can be calculated from Eqs. (4), and Z_1 is defined as

$$Z_1 = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,1}. \tag{B3}$$

If we can set a lower bound on Z_1, we will be able to estimate the lower bound of Q_1^S.

Z_1 clearly arises from the contribution of single photon signals. A natural strategy is to find an appropriate linear combination of Q^S and Q^D, in which the multiphoton signal contribution is minimized (while keeping it positive) so that we can set a lower bound on it as zero. Among all the multiphoton signals, the two-photon signal has much greater weight than signals with more photons. Therefore, we will try to eliminate the two-photon signal contribution first. Note that we can easily estimate the contribution of vacuum signals from Q^V and E^V.

Equations (4) show that $\underline{P_n^S} \le P_n^S(m) \le \overline{P_n^S}$ and $\underline{P_n^D} \le P_n^D(m) \le \overline{P_n^D}$ for untagged bits. Combining them with Eqs. (B1), we have

$$\begin{aligned}
Q^S\overline{P_2^D} - Q^D\underline{P_2^S} &= \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) \sum_{n=0}^{\infty} [P_n^S(m)\overline{P_2^D} - P_n^D(m)\underline{P_2^S}] Y_{m,n} \\
&\ge \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) \sum_{n=0}^{\infty} [\underline{P_n^S}\overline{P_2^D} - \overline{P_n^D}\underline{P_2^S}] Y_{m,n} \\
&= \sum_{n=0}^{\infty} [\underline{P_n^S}\overline{P_2^D} - \overline{P_n^D}\underline{P_2^S}] \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n} \\
&= a_0 \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,0} + a_1 \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,1} \\
&\quad + (\underline{P_2^S}\overline{P_2^D} - \overline{P_2^D}\underline{P_2^S}) \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,2} + \sum_{n=3}^{(1-\delta)N} a_2(n) \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n} + a_3 \\
&= a_0 \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,0} + a_1 \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,1} \\
&\quad + \sum_{n=3}^{(1-\delta)N} a_2(n) \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n} + a_3 \\
&= a_0 Z_0 + a_1 Z_1 + \sum_{n=3}^{(1-\delta)N} a_2(n) Z_2(n) + a_3,
\end{aligned} \tag{B4}$$

where

$$a_0 = \underline{P_0^S}\overline{P_2^D} - \overline{P_0^D}\underline{P_2^S}, \tag{B5}$$

$$a_1 = \underline{P_1^S}\overline{P_2^D} - \overline{P_1^D}\underline{P_2^S}, \tag{B6}$$

$$a_2(n) = \underline{P_n^S}\overline{P_2^D} - \overline{P_n^D}\underline{P_2^S}, \tag{B7}$$

$$\begin{aligned}
a_3 &= -\sum_{n=(1-\delta)N+1}^{(1+\delta)N} \overline{P_n^D}\underline{P_2^S} \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n} \\
&= -\sum_{n=(1-\delta)N+1}^{(1+\delta)N} \overline{P_n^D}\underline{P_2^S} Z_3(n),
\end{aligned} \tag{B8}$$

and

$$Z_0 = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,0} = Q^V, \tag{B9}$$

$$Z_2(n) = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n}, \tag{B10}$$

$$Z_3(n) = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,n}. \tag{B11}$$

Note that in Eq. (B4), when $n=2$, the term $\underline{P_n^S}\overline{P_2^D} - \overline{P_n^D}\underline{P_2^S} = 0$, which means we have removed the contribution from the two-photon signals. Our strategy is clear now: The contribution of vacuum signals ($a_0 Z_0$) can be easily bounded as a_0 can be calculated from Eqs. (B5) and an upper bound of Z_0 is given by $\overline{Z_0} = \overline{Q^V}$, which can be calculated from Eqs. (1); the contribution of single photon signals ($a_1 Z_1$) is to be esti-

mated while we know the exact value of a_1; we need to set some bounds on the higher order terms (a_2 and a_3) to complete an estimate of Z_1. As we will show below, a_1 is negative under certain condition. Therefore, we should set a lower bound on the higher order terms to find the lower bound of Z_1.

Lemma 1. a_1 is negative under Condition 2a,

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-1}{(1-\delta)N-1}.$$

Proof. By expanding Eq. (B6) we have

$$\begin{aligned} a_1 &= \underline{P_1^S}\overline{P_2^D} - \overline{P_1^D}\underline{P_2^S} \\ &= (1-\delta)N\lambda_S(1-\lambda_S)^{(1-\delta)N-1}\frac{(1+\delta)N[(1+\delta)N-1]}{2} \\ &\quad \times \lambda_D^2(1-\lambda_D)^{(1+\delta)N-2} - (1+\delta)N\lambda_D(1-\lambda_D)^{(1+\delta)N-1} \\ &\quad \times \frac{(1-\delta)N[(1-\delta)N-1]}{2}\lambda_S^2(1-\lambda_S)^{(1-\delta)N-2} \\ &= N^2(1-\delta^2)\lambda_S^2\lambda_D^2(1-\lambda_S)^{(1-\delta)N-2}(1-\lambda_D)^{(1+\delta)N-2} \\ &\quad \times \left(\frac{(1+\delta)N-1}{2\lambda_S} - \frac{(1-\delta)N-1}{2\lambda_D} - \delta N\right). \end{aligned} \tag{B12}$$

For Eq. (B12) we can see that $a_1 < 0$ under Condition 2a:

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-1}{(1-\delta)N-1}.$$

■

Lemma 1′. a_0 is negative under Condition 2a.

Proof. We have

$$\begin{aligned} a_0 &= \underline{P_0^S}\overline{P_2^D} - \overline{P_0^D}\underline{P_2^S} \\ &= (1-\lambda_S)^{(1+\delta)N}\frac{(1+\delta)N[(1+\delta)N-1]}{2}\lambda_D^2(1-\lambda_D)^{(1+\delta)N-2} - (1-\lambda_D)^{(1-\delta)N}\frac{(1-\delta)N[(1-\delta)N-1]}{2}\lambda_S^2(1-\lambda_S)^{(1-\delta)N-2} \\ &= \frac{1}{2}(1-\lambda_S)^{(1-\delta)N-2}(1-\lambda_D)^{(1-\delta)N}\{(1-\lambda_S)^{2\delta N+2}(1+\delta)N[(1+\delta)N-1]\lambda_D^2(1-\lambda_D)^{2\delta N-2} - (1-\delta)N[(1-\delta)N-1]\lambda_S^2\} \\ &< \frac{1}{2}(1-\lambda_S)^{(1-\delta)N-2}(1-\lambda_D)^{(1-\delta)N}\{(1+\delta)N[(1+\delta)N-1]\lambda_D^2 - (1-\delta)N[(1-\delta)N-1]\lambda_S^2\} \\ &= \frac{1}{2}(1-\lambda_S)^{(1-\delta)N-2}(1-\lambda_D)^{(1-\delta)N}\{[(1+\delta)N-1]^2\lambda_D^2 + [(1+\delta)N-1]\lambda_D^2 - [(1-\delta)N-1]^2\lambda_S^2 - [(1-\delta)N-1]\lambda_S^2\} < 0. \end{aligned} \tag{B13}$$

In the last step, we made use of Condition 2a. ■

Lemma 2. $a_2(n)$ is positive under Condition 2,

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-2}{(1-\delta)N-2}\left(\frac{(1+\delta)N-2}{2\delta N}\right)^{2\delta N/[(1-\delta)N-2]}\left(\frac{(1+\delta)N-2}{(1-\delta)N-2}\right)\left(\frac{e^2}{2\delta N}\right)^{1/2[(1-\delta)N-2]}.$$

Proof. Expanding Eq. (B7), note that $3 \le n \le (1-\delta)N$, we have

$$\begin{aligned} a_2(n) &= \underline{P_n^S}\overline{P_2^D} - \overline{P_n^D}\underline{P_2^S} \\ &= \binom{(1-\delta)N}{n}\lambda_S^n(1-\lambda_S)^{(1-\delta)N-n}\frac{(1+\delta)N[(1+\delta)N-1]}{2}\lambda_D^2(1-\lambda_D)^{(1+\delta)N-2} \\ &\quad - \binom{(1+\delta)N}{n}\lambda_D^n(1-\lambda_D)^{(1+\delta)N-n}\frac{(1-\delta)N[(1-\delta)N-1]}{2}\lambda_S^2(1-\lambda_S)^{(1-\delta)N-2} \\ &= \lambda_S^2\lambda_D^2(1-\lambda_S)^{(1-\delta)N-n}(1-\lambda_D)^{(1+\delta)N-n}\frac{[(1-\delta)N]![(1+\delta)N]!}{2\cdot n!}[b_1(n)-b_2(n)], \end{aligned} \tag{B14}$$

where

$$b_1(n) = \frac{\lambda_S^{n-2}(1-\lambda_D)^{n-2}}{[(1-\delta)N-n]\,![(1+\delta)N-2]!} > 0,$$

$$b_2(n) = \frac{\lambda_D^{n-2}(1-\lambda_S)^{n-2}}{[(1+\delta)N-n]\,![(1-\delta)N-2]!} > 0.$$

To show that $a_2(n)>0$, we need to show that $b_1(n)>b_2(n)$. Since they are both positive, we could try to show that $b_1(n)/b_2(n)>1$,

$$\frac{b_1(n)}{b_2(n)} = \frac{[(1+\delta)N-n]\,![(1-\delta)N-2]!}{[(1+\delta)N-2]\,![(1-\delta)N-n]!}\left(\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right)^{n-2}$$
$$= \prod_{i=3}^{n}\left(\frac{(1-\delta)N-i+1}{(1+\delta)N-i+1}\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right).$$

Define the last term of the product as

$$d(n) = \frac{(1-\delta)N-n+1}{(1+\delta)N-n+1}\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)},$$

which is a decreasing function of n. Note that $d(n)$ is always positive. Due to the decreasing nature of d_n on n, there exists a real number n_0 satisfying the following criterium: For any $n<n_0$, $d(n)>1$; for any $n\geq n_0$, $d(n)\leq 1$. We can easily see the following facts.

(1) If $n<n_0$, we know for sure that $b_1(n)/b_2(n)>1$, which means $a_2(n)>0$.

(2) If $n\geq n_0$, $b_1(n)/b_2(n)$ decreases as n increases. Since $n\leq(1-\delta)N$, we have

$$\frac{b_1(n)}{b_2(n)} = \prod_{i=3}^{n}\left(\frac{(1-\delta)N-i+1}{(1+\delta)N-i+1}\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right)$$
$$\geq \prod_{i=3}^{(1-\delta)N}\left(\frac{(1-\delta)N-i+1}{(1+\delta)N-i+1}\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right)$$
$$= \frac{[(1-\delta)N-2]\,!\,(2\delta N)!}{[(1+\delta)N-2]!}\left(\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right)^{(1-\delta)N-2}$$
$$= \frac{1}{\binom{(1+\delta)N-2}{2\delta N}}\left(\frac{\lambda_S(1-\lambda_D)}{\lambda_D(1-\lambda_S)}\right)^{(1-\delta)N-2}.$$

Therefore $a_2(n)>0$ under Condition 2b,

$$\frac{\lambda_S}{\lambda_D} > \binom{(1+\delta)N-2}{2\delta N}^{1/[(1-\delta)N-2]}.$$

Note that N is usually very large, which means the evaluation of Condition 2b can be computationally challenging. To simplify this condition, we can make use of Stirling's approximation

$$\sqrt{2\pi}n^{n+1/2}\exp\left(-n+\frac{1}{12n+1}\right) < n\,! < \sqrt{2\pi}n^{n+1/2}\exp\left(-n+\frac{1}{12n}\right),$$

which can be simplified to be

$$n^{n+1/2}e^{-n} < n\,! < n^{n+1/2}e^{-n+1}. \tag{B15}$$

With the help of Eq. (B15), we can derive a simpler and stronger version of Condition 2b.

Condition 2. We have

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-2}{(1-\delta)N-2}\left[\frac{(1+\delta)N-2}{2\delta N}\right]^{2\delta N/[(1-\delta)N-2]}\left[\frac{(1+\delta)N-2}{(1-\delta)N-2}\cdot\frac{e^2}{2\delta N}\right]^{1/2[(1-\delta)N-2]}.$$

■

Note that Condition 2 is also stronger than Condition 2a. Therefore Lemma 1 is also true under Condition 2.

Lemma 2′. $\sum_{n=3}^{(1-\delta)N} a_2(n)Z_2(n)\geq 0$ under Condition 2.

Proof. From Eq. (B10) we can clearly see that $Z_2(n)\geq 0$. ■

Lemma 3. We have

$$a_3 > -\frac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}.$$

Proof. Expanding Eq. (B8), we have

$$a_3 = -\sum_{n=(1-\delta)N+1}^{(1+\delta)N}\overline{P_n^D}\underline{P_2^S}Z_3(n)$$
$$\geq -\sum_{n=(1-\delta)N+1}^{(1+\delta)N}\overline{P_n^D}\underline{P_2^S} \quad [\because\ 0\leq Z_3(n)\leq 1]$$
$$\geq -2\delta N\overline{P_{(1-\delta)N+1}^D}\underline{P_2^S} \quad (\because\ 0\leq\overline{P_n^D}<\overline{P_{(1-\delta)N+1}^D})$$

$$= -2\delta N \binom{(1+\delta)N}{(1-\delta)N+1} \lambda_D^{(1-\delta)N+1} (1-\lambda_D)^{2\delta N-1} \underline{P_2^S}$$

$$= -2\delta N \frac{1}{[(1-\delta)N+1]!} (1-\lambda_D)^{2\delta N-1} \underline{P_2^S} \prod_{i=0}^{(1-\delta)N} \{[(1+\delta)N-i]\lambda_D\}$$

$$> -\frac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!} \quad \{\because\ [(1+\delta)N-i]\lambda_D < 1\}. \tag{B16}$$

■

Note that $|a_3|$ is in the order of $O(\frac{1}{N!})$. It is very close to 0.
From Eqs. (B4)–(B16) we can conclude that

$$Z_1 \geq \frac{Q^D\underline{P_2^S} - Q^S\overline{P_2^D} + a_0\overline{Q^V} + \sum_{n=3}^{(1-\delta)N} a_2(n)Z_2(n) + a_3}{-a_1} > \frac{\underline{Q^D P_2^S} - \overline{Q^S P_2^D} + a_0\overline{Q^V} - \frac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}}{-a_1} = \underline{Z_1}$$

under Condition 2,

$$\frac{\lambda_S}{\lambda_D} > \frac{(1+\delta)N-2}{(1-\delta)N-2}\left(\frac{(1+\delta)N-2}{2\delta N}\right)^{2\delta N/[(1-\delta)N-2]}\left(\frac{(1+\delta)N-2}{(1-\delta)N-2}\frac{e^2}{2\delta N}\right)^{1/2[(1-\delta)N-2]}.$$

Therefore, the lower bound of Q_1^S is given by

$$Q_1^S \geq \underline{P_1^S} Z_1 > \underline{P_1^S Z_1} = \underline{P_1^S}\frac{\underline{Q^D P_2^S} - \overline{Q^S P_2^D} + (\underline{P_0^S}\overline{P_2^D} - \overline{P_0^D}\underline{P_2^S})\overline{Q^V} - \frac{2\delta N(1-\lambda_D)^{2\delta N-1}\underline{P_2^S}}{[(1-\delta)N+1]!}}{\overline{P_1^D}\underline{P_2^S} - \underline{P_1^S}\overline{P_2^D}} = \underline{Q_1^S}.$$

This completes our proof of Proposition 1.

APPENDIX C: ESTIMATE OF e_1^S

The derivation of the upper bound of e_1^S is relatively simpler than that of the lower bound of Q_1^S. Similar as Eq. (B4) we have

$$E^S Q^S = \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) \sum_{n=0}^{\infty} P_n^S(m) Y_{m,n} e_{m,n},$$

where $e_{m,n}$ is the error rate for signals with m input photons and n output photons. Rearranging terms, we have

$$\begin{aligned} Q_1^S e_1^S &= E^S \cdot Q^S - Q_0^S e_0^S - \sum_{n=2}^{\infty} Q_n^S e_n^S \\ &\leq E^S Q^S - Q_0^S e_0^S \\ &= E^S Q^S - \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) P_0^S(m) Y_{m,0} e_{m,0} \\ &\leq E^S Q^S - \underline{P_0^S} \sum_{m=(1-\delta)N}^{(1+\delta)N} P_{\text{in}}(m) Y_{m,0} e_{m,0} \\ &= E^S Q^S - \underline{P_0^S} E^V Q^V. \end{aligned} \tag{C1}$$

The upper bound of e_1^S is thus given by

$$e_1^S \leq \frac{E^S Q^S - \underline{P_0^S} E^V Q^V}{Q_1^S} \leq \frac{\overline{E^S Q^S} - \underline{P_0^S E^V Q^V}}{\underline{Q_1^S}}.$$

This completes our proof of Proposition 2.

APPENDIX D: ONE-DECOY PROTOCOL

In one-decoy protocol, there is no vacuum state. Therefore, we cannot measure $\underline{Q_e^V}$ or E_e^V. If we still want to estimate $\underline{Q_1^S}$ via Eq. (14) and e_1^S via Eq. (16), we need to estimate $\overline{Q_V}$ in Eq. (14) and $\underline{E^V \cdot Q^V}$ in Eq. (16) in another way.

To estimate $\overline{Q^V}$, we can look at Eq. (C1),

$$\underline{P_0^S} E^V Q^V \leq E^S Q^S - Q_1^S e_1^S \leq E^S Q^S \leq \overline{E^S Q^S}.$$

Therefore,

$$Q^V \leq \frac{\overline{E^S Q^S}}{\underline{P_0^S} E^V} = \overline{Q^V}, \tag{D1}$$

where $\overline{E^S Q^S}$ can be estimated from Eqs. (2), $\underline{P_0^S}$ can be estimated from Eqs. (4), and $E^V = 0.5$ in asymptotic case.

Plugging Eq. (D1) into Eq. (14), we have the expression of Q_1^S with the one-decoy protocol,

$$Q_1^S > \underline{Q_1^S} = \underline{P_1^S} \frac{\underline{Q^D P_2^S} - \overline{Q^S P_2^D} + (\underline{P_0^S \overline{P_2^D}} - \overline{P_0^D} \underline{P_2^S}) \frac{\overline{E^S Q^S}}{P_0^S E^V} - \frac{2\delta N (1-\lambda_D)^{2\delta N - 1} \underline{P_2^S}}{[(1-\delta)N+1]!}}{\overline{P_1^D} \underline{P_2^S} - \underline{P_1^S} \overline{P_2^D}}.$$

As for the estimate of $\underline{E^V Q^V}$, we can simply use the following fact: $E^V Q^V \geq 0$. Therefore, the expression of $\overline{e_1^S}$ in one-decoy protocol is given by

$$e_1^S \leq \overline{e_1^S} = \frac{\overline{E^S Q^S}}{\underline{Q_1^S}}.$$

This completes our proof of Proposition 3.

[1] C. H. Bennett and G. Brassard, *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[4] D. Mayers, J. ACM **48**, 351 (2001); H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[5] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[6] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, e-print arXiv:0802.4155.
[8] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).
[9] L. Masanes and A. Winter, e-print arXiv:quant-ph/0606049.
[10] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[11] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[12] V. Makarov and J. Skaar, Quantum Inf. Comput. **8**, 0622 (2008).
[13] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quantum Inf. Comput. **7**, 73 (2007).
[14] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, e-print arXiv:0704.3253.
[15] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).
[16] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **8**, 431 (2007).
[17] D. Stucki, N. Gisin, O. Guinnard, G. Robordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).
[18] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[19] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[20] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[21] H.-K. Lo, *Proceedings of IEEE International Symposium on Information Theory* (IEEE, New York, 2004), p. 137.
[22] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[23] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[24] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[25] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print arXiv:quant-ph/0503002.
[26] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).
[27] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
[28] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, *Proceedings of IEEE International Symposium of Information Theory* (IEEE, New York, 2006), pp. 2094–2098.
[29] T. Schmitt-Manderbach *et al.*, Phys. Rev. Lett. **98**, 010504 (2007).
[30] C.-Z. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
[31] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and H. E. Nodrolth, Phys. Rev. Lett. **98**, 010503 (2007).
[32] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Opt. Express **15**, 8465 (2007).
[33] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).
[34] Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, and G.-C. Guo, e-print arXiv:0704.2941.
[35] X.-B. Wang, C.-Z. Peng, J. Zhang, and J.-W. Pan, e-print arXiv:quant-ph/0612121v3.
[36] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[37] The gain is defined to be the ratio of the number of receiver Bob's detection events to the number of signals emitted by sender Alice in the cases where Alice and Bob use the same basis. It depends mainly on the intensity of signal, channel transmittance, and Bob's quantum efficiency.
[38] G. Brassard and L. Salvail, *Lecture Notes in Computer Science* (Springer, New York, 1994), Vol. 765, pp. 410–423.
[39] C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[40] www.idquantique.com
[41] www.magiqtech.com
[42] A. Lamas-Linares and C. Kurtsiefer, Opt. Express **15**, 9388 (2007).