Passive decoy-state quantum key distribution for the weak coherent photon source with finite-length key*

Yuan Li(李源)[1,2], Wansu Bao(鲍皖苏)[1,2,†], Hongwei Li(李宏伟)[1,2], Chun Zhou(周淳)[1,2], and Yang Wang(汪洋)[1,2]

[1] *Zhengzhou Information Science and Technology Institute, Zhengzhou* 450004, *China*
[2] *Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei* 230026, *China*

(Received 27 May 2015; revised manuscript received 1 October 2015; published online 7 December 2015)

Passive decoy-state quantum key distribution systems, proven to be more desirable than active ones in some scenarios, also have the problem of device imperfections like finite-length keys. In this paper, based on the WCP source which can be used for the passive decoy-state method, we obtain the expressions of single-photon error rates, single-photon counts, and phase error rates. According to the information of smooth min-entropy, we calculate the key generation rate under the condition of finite-length key. Key generation rates with different numbers of pulses are compared by numerical simulations. From the results, it can be seen that the passive decoy-state method can have good results if the total number of pulses reaches 10^{10}. We also simulate the passive decoy-state method with different probabilities of choosing a pulse for parameter estimation when the number of pulses is fixed.

Keywords: quantum key distribution, passive decoy-state, finite-length key, weak coherent pulses

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/25/1/010305

1. Introduction

Quantum key distribution (QKD)[1,2] allows two legitimate parties, Alice and Bob, to establish a common and secret key when the channel is accessible to an eavesdropper, Eve. Since the best-known Bennett–Brassard 1984 (BB84) protocol[1] was put forward, QKD has attracted more and more attention all over the world, due to its unconditional security based on the fundamental laws of physics: no-cloning theorem and the uncertainty principle.[3]

QKD has been developed well both theoretically and experimentally[4–11] in recent years. However, people have come across all sorts of difficulties in a real situation.[12] Though an ideal QKD system is unconditional security, in fact the necessary assumptions that ideal QKD system need are not easy to be satisfied. These practical factors such as finite resources and imperfections of setups, will undoubtedly threaten the security of the real QKD system, and Eve can take advantage of the leaks to attack the system. To prevent the attacks, many countermeasures have been applied. One of them is to employ the decoy-state method[13–17] which introduces two or more decoy states to confuse Eve so that she cannot distinguish the signal state from the decoy states. Another important approach is the notion of device-independent QKD (DI-QKD).[18–28] What is more, people make works to characterize the effects of the real imperfect factors on the security of QKD system in a mathematical way to give a security proof.[12]

The finite-length key is an important practical factor which needs to be solved in a real QKD system. Under ideal conditions, the data transformed between Alice and Bob are infinite, and QKD can generate the final secure key from the infinite data. However, in practice, the data above cannot be infinite. It may cause statistical fluctuations on relating parameters. When we regard the finite-length keys, we should reconsider the security bound in the asymptotic regime.

In recent years, many significant advances have been achieved.[29–32] In 2008, Scarani and Renner[33] creatively presented the smooth min-entropy theory to obtain the security bound for practical BB84 with finite-length keys. Then Tan and Cai[34,35] studied the passive decoy-state with finite-length keys and demonstrated its unconditional security. Their works show that the practical decoy state can reach the asymptotic limit, where the resource is large enough but not infinite. In 2014, Zhou *et al.*[36] presented a concise and stringent formula to calculate the key generation rate for QKD using SPDCSs with finite-length keys.

In this paper, we first briefly introduce the decoy state protocol. We focus on the passive decoy-state protocol and the differences from the active decoy-state protocol. Then we introduce the phase-randomized WCP source used for the passive decoy-state method. With this source, we describe the passive decoy-state protocol without considering the finite-length key.

The rest of this paper is organized as follows. In Sections 2 and 3, we briefly introduce decoy state protocol and the WCP source which has been transformed for the passive

*Project supported by the National Natural Science Foundation of China (Grant No. 11304397).
†Corresponding author. E-mail: 2010thzz@sina.com
© 2016 Chinese Physical Society and IOP Publishing Ltd

decoy-state method, respectively. Next, in Section 4, we consider the passive decoy-state method with the infinite-length key. The affect of the finite-length key on the passive decoy-state method is analyzed in detail in Section 5. The numerical simulations of this section are shown in Section 6. Finally, Section 7 concludes the paper with a summary.

2. Decoy state protocol

In Section 1, we presented the fact that the necessary assumptions an ideal QKD system needs are not easy to satisfy. In the original proposal of the BB84 protocol, a single-photon source is necessary, but the single-photon source is still unavailable with current technology. Usually, a weak coherent pulse (WCP) source is used instead and many WCP-based experiments have been done since the first QKD experiment was carried out.[37] However, due to the multiphoton pulse sent from the WCP source, the QKD system will suffer from photon-number splitting (PNS) attack.[38,39] To protect the QKD system from PNS attack, one can use the decoy-state method which could closely reach the performance of single-photon sources. Actually, the method that Alice prepares the decoy state actively can be called the active decoy-state method. Similarly, the active decoy-state method also suffers from some practical factors. Because of imperfect experiments and channels, it may bring in some side channel information that Eve can take advantage of having an attack. For the real active (regular) decoy-state experiments, it is more difficult to verify the assumption that Eve cannot distinguish decoy and signal states.[40]

However, the passive decoy-state method[41,42] can reduce the side channel information in the decoy-state preparation procedure. Different from the active decoy-state method which actively changes the intensity of the laser pulses randomly, the passive decoy-state method only has one intensity pulse. The key point to distinguish in the passive decoy-state method is clicking or no clicking for Alice's detector.

The common point between the passive decoy state and the active decoy state is that the yields and the error rates of the same photon-number states of the signal states and the decoy states shall be equal to each other, which means[14]

$$Y_m = Y'_m, \quad e_m = e'_m, \tag{1}$$

where Y_m and Y'_m denote the yields of m photons of signal states and decoy states, respectively, e_m and e'_m denote the error rates of m photons of signal states and decoy states, respectively.

3. Transformed WCP source used for the passive decoy-state method

Due to the characters of the WCP source itself, it cannot be used for the passive decoy-state method directly. Curty *et al.*[43,44] have adjusted the WCP source to make it output two Fock diagonal states, so that it can be used for the passive decoy-state method. The fundamental setups are shown in Fig. 1.

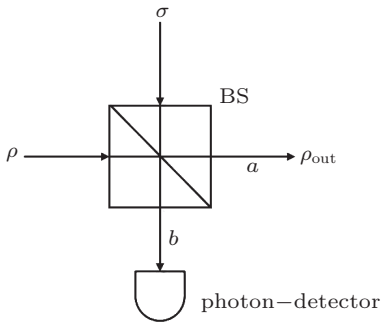


Fig. 1. The WCP sources[43,44] used for passive decoy-state method.

In Fig. 1, ρ and σ denote the coherent states of two phase-randomized WCP source states, respectively,

$$\rho = \mathrm{e}^{-\mu_1} \sum_{n=0}^{\infty} \frac{\mu_1^n}{n!} |n\rangle\langle n|, \tag{2}$$

$$\sigma = \mathrm{e}^{-\mu_2} \sum_{n=0}^{\infty} \frac{\mu_2^n}{n!} |n\rangle\langle n|, \tag{3}$$

with μ_1 and μ_2 denoting the mean photon numbers of the two signals, respectively. It should be noted that the WCP source that Curty *et al.* changed is phase-randomized WCP. Without additional explanations, the WCP source mentioned throughout this paper is the source shown in Fig. 1. We consider the threshold detector as the photon-detector in Fig. 1. In this scenario, the joint probability of having n photons in output mode a and m photons in output mode b can be written as[44]

$$p_{n,m} = \frac{\upsilon^{n+m}\mathrm{e}^{-\upsilon}}{n!m!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n (1-\gamma)^m \mathrm{d}\theta, \tag{4}$$

where the parameters υ, γ, and ξ are given by

$$\begin{aligned} \upsilon &= \mu_1 + \mu_2, \\ \gamma &= \frac{\mu_1 t + \mu_2(1-t) + \xi\cos\theta}{\upsilon}, \\ \xi &= 2\sqrt{\mu_1\mu_2(1-t)t}, \end{aligned} \tag{5}$$

where t denotes the transmittance of a beam splitter.

Whenever the sender, Alice, does not care about the result of the measurement in mode b, the probability of having n photons in mode a can be written as

$$p'_n = \sum_{m=0}^{\infty} p_{n,m} = \frac{\upsilon^n}{n!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n \mathrm{e}^{-\upsilon\gamma} \mathrm{d}\theta. \tag{6}$$

For Alice's detector, the joint probability of having n photons in mode a and no click in the threshold detector now has the form

$$p_n^{\bar{c}} = (1-d_A) \sum_{m=0}^{\infty} (1-\eta_{\mathrm{d}})^m p_{n,m}$$

$$= (1-\varepsilon)\frac{\upsilon^n \mathrm{e}^{-\eta_\mathrm{d}\upsilon}}{n!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n \mathrm{e}^{-(1-\eta_\mathrm{d})\upsilon\gamma}\mathrm{d}\theta, \quad (7)$$

where the parameter d_A denotes dark count and η_d denotes the detection efficiency of the detector, and then, the probability of having n photons in mode a and producing a click in Alice's threshold detector is

$$p_n^c = p_n^t - p_n^{\bar{c}}. \quad (8)$$

In this paper, we define that c denotes "click" of the detector while $\bar{c}$ denotes "no click". We also denote the signals that cause a click of Alice's detector as signal states. The ones that cause no click of Alice's detector are decoy states.

4. Passive decoy-state method using the WCP source with infinite-length key

In this section, we discuss the ideal passive decoy-state method. In the passive decoy-state method, two-mode states are a prerequisite as shown in Fig. 1. When Alice measures mode b with a threshold detector described by detection efficiency η_A and dark-count rate d_A, the mode a can be divided into two parts according to the result of the threshold detector: the "click" events and "no click" events. Here, we denote that the "click" events are signal states. The "no click" events are decoy states.

In Section 3, we have mentioned the parameter p_n^t, the probability of having n photons in mode a. It is divided into two parts p_n^c and $p_n^{\bar{c}}$. Usually, we describe p_n^t as $p_n^t = p_n^c + p_n^{\bar{c}}$.[38] Here, the parameters p_n^c and $p_n^{\bar{c}}$ can be written as

$$p_n^c = p_n^t P_n, \quad p_n^{\bar{c}} = p_n^t(1-P_n), \quad (9)$$

where P_n is the probability of "click" detection event when n-photon states are emitted from the WCP source, and $P_n = 1-(1-d_A)(1-\eta_A)^n$.[41]

According to the passive decoy-state method, the counting rates and the error rates of the n-photon states of the signal states and the decoy states are

$$Q_{n,c} = Y_{n,c}p_n^t P_n, \quad (10)$$

$$Q_{n,\bar{c}} = Y_n^{\bar{c}} p_n^t(1-\gamma_n). \quad (11)$$

From Eqs. (10) and (11), it is easy to find that Q_n^c and $Q_n^{\bar{c}}$ have a relation.[37] In this paper, we use a parameter δ_n to represent it, that is

$$Q_{n,c} = \delta_n Q_{n,\bar{c}}, \quad (12)$$

$$\delta_n = \frac{P_n}{1-P_n}, \quad (13)$$

where δ_n is a monotonically increasing function.

The overall gain of Alice's detector producing a click is Q_c and no click is $Q_{\bar{c}}$. They can be expressed by

$$Q_c = \sum_{n=0}^{\infty} Q_{n,c} = Q_{0,c} + Q_{1,c} + \sum_{n=2}^{\infty} Q_{n,c}, \quad (14)$$

$$Q_{\bar{c}} = \sum_{n=0}^{\infty} Q_{n,\bar{c}} = Q_{0,\bar{c}} + Q_{1,\bar{c}} + \sum_{n=2}^{\infty} Q_{n,\bar{c}}. \quad (15)$$

In order to calculate the lower bound of $Q_{1,\bar{c}}$, we eliminate $\sum_{n=2}^{\infty} Q_{n,c}$ and $\sum_{n=2}^{\infty} Q_{n,\bar{c}}$ elements. Applying equation (12) and the monotonicity of δ_n, we can obtain

$$\begin{aligned}\delta_2(Q_{\bar{c}} - Q_{0,\bar{c}} - Q_{1,\bar{c}}) &\le Q_c - Q_{0,c} - Q_{1,c} \\ &= Q_c - Q_{0,c} - \delta_1 Q_{1,\bar{c}}, \end{aligned} \quad (16)$$

and then, the lower bound $Q_{1,\bar{c}}^{\mathrm{L}}$ can be obtained[42]

$$\begin{aligned} Q_{1,\bar{c}} \ge Q_{1,\bar{c}}^{\mathrm{L}} &= \frac{\delta_2(Q_{\bar{c}} - Q_{0,\bar{c}}) - Q_c + Q_{0,c}}{\delta_2 - \delta_1} \\ &= \frac{\delta_2(Q_{\bar{c}} - Q_{0,\bar{c}}) - \delta Q_{\bar{c}} + \delta_0 Q_{0,\bar{c}}}{\delta_2 - \delta_1}, \end{aligned} \quad (17)$$

where $\delta = Q_c/Q_{\bar{c}}$. Since $Q_{1,\bar{c}}$ and $Q_{1,c}$ satisfy Eq. (12), we can obtain the lower bound of $Q_{1,c}$ as

$$Q_{1,c} = \delta_1 Q_{1,\bar{c}} \ge \delta_1 Q_{1,\bar{c}}^{\mathrm{L}} = Q_{1,c}^{\mathrm{L}}. \quad (18)$$

Next, we will calculate the upper bound of error rates of the signal state and the decoy state. According to the quantum bit error rate (QBER),

$$Q_c E_c = \sum_{n=0}^{\infty} Q_{n,c}e_{n,c} = Q_{0,c}e_{0,c} + Q_{1,c}e_{1,c} + \sum_{n=2}^{\infty} Q_{n,c}e_{n,c}, \quad (19)$$

$$Q_{\bar{c}} E_{\bar{c}} = \sum_{n=0}^{\infty} Q_{n,\bar{c}}e_{n,\bar{c}} = Q_{0,\bar{c}}e_{0,\bar{c}} + Q_{1,\bar{c}}e_{1,\bar{c}} + \sum_{n=2}^{\infty} Q_{n,\bar{c}}e_{n,\bar{c}}, \quad (20)$$

we can obtain two upper bounds of $e_{1,c}$ as

$$e_{1,c} \le e_{1,c}^{\mathrm{U}} = \frac{2E_c Q_c - Q_{0,c}}{2Q_{1,c}^{\mathrm{L}}}, \quad (21)$$

$$e_{1,c} \le e_{1,c}^{\mathrm{U}} = \frac{2E_{\bar{c}} Q_{\bar{c}} - Q_{0,\bar{c}}}{2Q_{1,\bar{c}}^{\mathrm{L}}}, \quad (22)$$

where $e_{0,c} = e_{0,\bar{c}} = 0.5$. The minimum of Eqs. (21) and (22) is the upper bound $e_{1,c}^{\mathrm{U}}$,[41]

$$e_1 \le e_1^{\mathrm{U}} = \min\left(\frac{2E_c Q_c - Q_{0,c}}{2Q_{1,c}^{\mathrm{L}}}, \frac{2E_{\bar{c}} Q_{\bar{c}} - Q_{0,\bar{c}}}{2Q_{1,\bar{c}}^{\mathrm{L}}}\right). \quad (23)$$

Due to $Q_{1,\bar{c}}, e_1 \ge 0$, a parameter x is introduced, $x = Q_{0,\bar{c}}/Q_{\bar{c}}$ and its range is

$$0 \le x \le \min(2E_c(\delta/\delta_0), 2E_{\bar{c}}). \quad (24)$$

Finally, taking the parameters above into the GLLP formula, one can obtain the following final key rate:[42]

$$\begin{aligned} R^c &= q\{-Q_c f(E_c)H_2(E_c) + Q_c \min(x) \\ &\quad \times \{\delta_0 x + Q_{1,c}^{\mathrm{L}}[1 - H_2(e_{1,c}^{\mathrm{U}})]\}\}, \end{aligned} \quad (25)$$

$$\begin{aligned} R^{\bar{c}} &= q\{-Q_c f(E_c)H_2(E_c) - Q_{\bar{c}} f(E_{\bar{c}})H_2(E_{\bar{c}}) \\ &\quad + Q_{\bar{c}} \min(x)\{(1+\delta_0)x + (1+\delta_0)Q_{1,\bar{c}}^{\mathrm{L}} \\ &\quad \times [1 - H_2(e_{1,\bar{c}}^{\mathrm{U}})]\}\}, \end{aligned} \quad (26)$$

$$R = \max\{R^c, 0\} + \max\{R^{\bar{c}}, 0\}, \quad (27)$$

where $H_2(x)$ is the binary Shannon entropy function.

5. Passive decoy-state method using the WCP source with finite-length key

Because of the finite-size data sets in real-life condition, parameters have various fluctuations. In this paper, we mainly consider the influence of the finite-size data on the single-photon yield and single-photon error rate. Here, we will use smooth min-entropy to study the passive decoy-state method with the finite-length key.

Firstly, we introduce some related definitions.

Compassable security definition[45,46] Assume a QKD protocol output keys of K_A and K_B on Alice's and Bob's sides, respectively. It is considered to be ε-secure if it satisfies both the correctness and the secrecy. Correctness means that the probability of $K_A \neq K_B$ will not exceed $\varepsilon_{\rm cor}$, i.e.,

$$P(K_A \neq K_B) \leq \varepsilon_{\rm cor}.$$

Secrecy means that K_A and K_B satisfy the inequality

$$\frac{1}{2}\|\rho_{KE} - I_K \otimes \rho_E\|_1 \leq \varepsilon_{\rm sec},$$

where K denotes either K_A or K_B, ρ_{KE} is the quantum state about K and Eve, I_K represents the uniform mixture of all possible values of K, and ρ_E is the system that Eve owns.

For QKD protocol, correctness can be regarded as the maximal probability of error-correction failure. Secrecy implies the probability that the final key is equal to the key without Eve is no less than $1-\varepsilon_{\rm sec}$.

Smooth min-entropy[45] Let $\varepsilon \geq 0$, $\sigma_B \in S(H_B)$, and $\rho_{AB} \in S_{\leq}(H_{AB})$. The smooth min-entropy $H^{\varepsilon}_{\min}(A|B)$, taken over a set of state $B^{\varepsilon}(\rho)$ that are ε-close to ρ_{AB}, is defined as

$$H^{\varepsilon}_{\min}(A|B) = \max_{\tilde{\rho}_{AB}\in B^{\varepsilon}(\rho)} \{-\log_2 \min\{\lambda > 0 : \exists \sigma_B : \tilde{\rho}_{AB} \leq \lambda {\rm id}_A \oplus \sigma_B\}\},$$

where

$$B^{\varepsilon}(\rho) := \{\tilde{\rho}_{AB} \in S_{\leq}(H_{AB}) : C(\rho_{AB}, \tilde{\rho}_{AB}) \leq \varepsilon\},$$

and ${\rm id}_A$ is the identity operator on A, and $C(\rho_{AB}, \tilde{\rho}_{AB}) := [1-({\rm tr}|\sqrt{\rho}\sqrt{\tilde{\rho}}|)^2]^{1/2}$ is a distance measure based on fidelity and ε is called the smoothing parameter, and $H^{\varepsilon}_{\min}(A|B)$ means the largest amount of information which Eve can obtain.

Chain-rule inequality for the smooth min-entropy[47] Let $\varepsilon \geq 0$, $\varepsilon', \varepsilon'' \geq 0$, and $\rho_{ABC} \in S_{\in}(H_{ABC})$, and then

$$H^{\varepsilon+\varepsilon'+2\varepsilon''}_{\min}(AB|C)_{\rho} \geq H^{\varepsilon''}_{\min}(A|BC)_{\rho} + H^{\varepsilon'}_{\min}(B|C)_{\rho} - f(\varepsilon),$$

where

$$f(\varepsilon) = \log_2 \frac{1}{1-\sqrt{1-\varepsilon^2}}.$$

Here, we make E the information that Eve can obtain from the raw key X_A of Alice, prior to the error-verification step. After the privacy amplification step, the length of the secure key S_A can be expressed by the following lemma.

Lemma 1[48,49] Let $\varepsilon_n, n_c, n_{\bar{c}} > 0$, and let $\rho^{c}_{n_c}$ and $\rho^{\bar{c}}_{n_{\bar{c}}}$ be the quantum states of the "click" and "no click" n-photon events, respectively. They are both permutation-invariant quantum states, and let $\Im$ be a positive-operator-value measure (POVM) on H_{AB} which outputs the yield and quantum bit error rate, where $\rho^{n_c+n_{\bar{c}}} \in S(H_{AB}^{\otimes n_1+n_2})$. Let $\Upsilon_{n,c}$ and $\Upsilon_{n,\bar{c}}$ be the frequency distributions of the measurement events, e.g., the yield, when applying the measurements $\Im^{n_1}$ and $\Im^{n_2}$, respectively. Then, for any elements $Y_{n,c}$ and $Y_{n,\bar{c}}$ from $\Upsilon_{n,c}$ and $\Upsilon_{n,\bar{c}}$ except with probability ε_n,

$$\frac{1}{2}\|Y_{n,c} - Y_{n,\bar{c}}\| \leq \xi(\varepsilon_n, n_c, n_{\bar{c}}), \tag{28}$$

with

$$\xi(\varepsilon_n, n_c, n_{\bar{c}}) = \sqrt{\frac{(n_c+n_{\bar{c}})(n_c+1)\ln(1/\varepsilon_n)}{8n_c^2 n_{\bar{c}}}}. \tag{29}$$

Here, we change Eq. (28) for convenience as

$$Y_{n,c} \leq Y_{n,\bar{c}} + 2\xi(\varepsilon_n, n_c, n_{\bar{c}}), \tag{30}$$

$$Y_{n,c} \geq Y_{n,\bar{c}} - 2\xi(\varepsilon_n, n_c, n_{\bar{c}}). \tag{31}$$

Lemma 2 (Secret key based on smooth min-entropy)[45,50] By applying privacy amplification with two-universal hashing, a secret key extracted from X_A is $\varepsilon_{\rm sec}$-secret if its length ℓ is chosen such that

$$\left\lfloor H^{v}_{\min}(X_A|I') - 2\log_2 \frac{1}{2\bar{v}} \right\rfloor,$$

where $v + \bar{v} \leq \varepsilon_{\rm sec}$ with v and $\bar{v}$ chosen to be proportional to $\varepsilon_{\rm sec}/p_{\rm pass}$, and $H^{v}_{\min}(X_A|I')$ quantifies the amount of uncertainty system Eve has on X_A.

Due to the influence of the finite-length key, the yields of the signal state and decoy state are no longer equal to each other, that is

$$Y_{n,c} \neq Y_{n,\bar{c}}. \tag{32}$$

However, Lemma 2 provides a relationship between $Y_{n,c}$ and $Y_{n,\bar{c}}$ under the condition of finite-length key.

Next, we can calculate the lower bound of the single-photon counting rates for the decoy state and signal state.

Similar to that in Section 4, we need to eliminate the elements of $n \geq 2$ in Eq. (15). According to Eq. (30), the elements can be expressed by

$$\sum_{n=2}^{\infty} Q_{n,\bar{c}} \leq \sum_{n=2}^{\infty} (Y_{n,\bar{c}} + 2\xi(\varepsilon_n, n_c, n_{\bar{c}}))p^{\bar{c}}_n. \tag{33}$$

After being multiplied by δ_2, the upper inequality is changed to

$$\delta_2 \sum_{n=2}^{\infty} Q_{n,\bar{c}} \leq \delta_2 \sum_{n=2}^{\infty} (Y_{n,c} + 2\xi(\varepsilon_n, n_c, n_{\bar{c}}))p^{c}_n$$

$$= \sum_{n=2}^{\infty} (Q_{n,c} + 2p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}})), \tag{34}$$

and then, replacing $\sum_{n=2}^{\infty} Q_{n,c}$ and $\sum_{n=2}^{\infty} Q_{n,\bar{c}}$ by $Q_c - Q_{0,c} - Q_{1,c}$ and $Q_{\bar{c}} - Q_{0,\bar{c}} - Q_{1,\bar{c}}$ respectively, inequality (34) can be written by

$$\begin{aligned}
&\delta_2(Q_{\bar{c}} - Q_{0,\bar{c}} - Q_{1,\bar{c}}) \\
&\le Q_c - Q_{0,c} - Q_{1,c} + 2\sum_{n=2}^{\infty} p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}}) \\
&\le Q_c - (Y_{0,\bar{c}} - 2\xi(\varepsilon_0, 0_c, 0_{\bar{c}}))p_0^c \\
&\quad - (Y_{1,\bar{c}} - 2\xi(\varepsilon_1, 1_c, 1_{\bar{c}}))p_1^c + 2\sum_{n=2}^{\infty} p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}}) \\
&= Q_c - Q_{0,c} - \delta_1 Q_{1,\bar{c}} + 2\sum_{n=0}^{\infty} p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}}).
\end{aligned} \tag{35}$$

Now, we can obtain the lower bound of $Q_{1,\bar{c}}$ as

$$\begin{aligned}
&Q_{1,\bar{c}} \ge Q_{1,\bar{c}}^{\mathrm{L}} \\
&= \frac{\delta_2(Q_{\bar{c}} - Q_{0,\bar{c}}) - Q_c + Q_{0,c} - 2\sum_{n=2}^{\infty} p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}})}{\delta_2 - \delta_1}.
\end{aligned} \tag{36}$$

Comparing inequality (36) with inequality (17) in Section 4, we find that $\sum_{n=0}^{\infty} p_n^c \xi(\varepsilon_n, n_c, n_{\bar{c}})$ should be considered. It means that in the condition of a finite-length key, the essence of the decoy state cannot be satisfied which will affect $Q_{1,\bar{c}}^{\mathrm{L}}$. By introducing the parameters p_{pe} and N, $Q_{1,\bar{c}}^{\mathrm{L}}$ can be expressed by

$$\frac{Q_{1,\bar{c}}}{Q_{\bar{c}}} \ge \frac{[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]}{\delta_2 - \delta_1}, \tag{37}$$

where N denotes the number of total pulses emitted from the WCP source and p_{pe} is the probability of choosing a pulse as the sample bits used for parameter estimation. In the QKD protocol, the signal pulses that Bob receives can be divided into two parts. One part can generate the raw keys, another part is used for parameter estimation, p_{pe} is the selection probability and χ is

$$\chi = \frac{1}{Q_{\bar{c}}} \sqrt{\frac{\ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}} \sum_{n=0}^{\infty} \sqrt{\delta_n p_n^t}. \tag{38}$$

In the ideal condition, N is infinite, n_c and $n_{\bar{c}}$ of $\xi(\varepsilon_n, n_c, n_{\bar{c}})$ are $n_c = Np_{\mathrm{pe}}p_n^c$ and $n_{\bar{c}} = Np_{\mathrm{pe}}p_n^{\bar{c}}$, respectively.

Similarly, we can obtain the lower bound of $Q_{1,c}$ according to inequalities (30), (37) and Eq. (14) as

$$\begin{aligned}
Q_{1,c} \ge Q_{1,c}^{\mathrm{L}} &= \frac{\delta_1 Q_{\bar{c}}[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]}{\delta_2 - \delta_1} \\
&\quad - \sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}}.
\end{aligned} \tag{39}$$

Next, we will recalculate the upper bounds of $e_{1,c}$ and $e_{1,\bar{c}}$.

Due to $e_{1,c} \ne e_{1,\bar{c}}$, we can obtain two sample upper bounds of $e_{1,c}$ and $e_{1,\bar{c}}$ from Eqs. (19) and (20), respectively,

$$e_{1,c} \le \frac{Q_c E_c - Q_{0,c} e_{0,c}}{Q_{1,c}}, \tag{40}$$

$$e_{1,\bar{c}} \le \frac{Q_{\bar{c}} E_{\bar{c}} - Q_{0,\bar{c}} e_{0,\bar{c}}}{Q_{1,\bar{c}}}. \tag{41}$$

Substituting elements $Q_{1,c}$ and $Q_{1,\bar{c}}$, we can obtain

$$e_{1,c} \le \frac{Q_c E_c - Q_{0,c} e_{0,c}}{Q_{1,c}} \le \frac{2Q_c E_c - \delta_0 Q_{0,\bar{c}} + \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}}}{2\left\{\frac{\delta_1 Q_{\bar{c}}[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]}{\delta_2 - \delta_1} - 2\sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}}\right\}} = e_{1,c}^{\mathrm{U}}, \tag{42}$$

$$e_{1,\bar{c}} = \frac{Q_{\bar{c}} E_{\bar{c}} - Q_{0,\bar{c}} e_{0,\bar{c}}}{Q_{1,\bar{c}}} \le \frac{(2E_{\bar{c}} - x)(\delta_2 - \delta_1)}{2\delta_1 Q_{\bar{c}}[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]} = e_{1,\bar{c}}^{\mathrm{U}}, \tag{43}$$

where $e_{0,c} = e_{0,\bar{c}} = 1/2$.

To calculate the final key generation rate, Lemma 2 is usually used to obtain the length of the secret key firstly. In this paper, we set

$$\ell_c = \left\lfloor H_{\min}^{v}(X_A|E') - 2\log_2 \frac{1}{2\bar{v}} \right\rfloor, \tag{44}$$

which considers the key generated from the signal state. Reference [50] gives the expression of the length of the secret key in this situation as follows:

$$n_0^c + n_1^c[1 - H_2(e_{\mathrm{p}}^c)] - \lambda_{\mathrm{EC}}^c - 6\log_2 \frac{10}{\varepsilon_{\mathrm{sec}}} - \log_2 \frac{2}{\varepsilon_{\mathrm{cor}}}, \tag{45}$$

where

$$\begin{aligned}
&n_0^c \ge N\left(Q_{\bar{c}}\delta_0 x - \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}}\right), \\
&n_1^c \ge N\left\{\frac{\delta_1[(\delta_2 - \delta) - (\delta_2 - \delta_0)x - \chi]}{\delta_2 - \delta_1} - \sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\mathrm{pe}})}{2Np_{\mathrm{pe}}}}\right\}, \\
&\lambda_{\mathrm{EC}}^c = NQ_c f(E_c) H_2(E_c),
\end{aligned} \tag{46}$$

and e_{p}^c denotes the phase error rate of the signal state in QKD.

The phase error rate $e_{\rm p}$ is given by

$$e_{\rm p} = \frac{(n+l)\hat{e}(j+2) - l e_{\rm ob}(j+2)}{n} \equiv e(e_{\rm ob}(j)), \quad (47)$$

where

$$\begin{aligned}
&\hat{e}(j) = \frac{e_{\rm ob}(j) + 2\varpi + 2\sqrt{\varpi\{e_{\rm ob}(j)[1-e_{\rm ob}(j)]+\varpi\}}}{1+4\varpi},\\
&e_{\rm ob}(j) = \frac{j}{l},\\
&\varpi = \frac{w^2 n}{4l(n+l-1)},\\
&\sqrt{\frac{n+l}{n}}\sqrt{\frac{w^2+2\pi}{2}}\,{\rm e}^{\beta}\Phi(w) \le \frac{\varepsilon_{\rm sec}^2}{16},\\
&\beta = \frac{1}{6n} + \frac{1}{12},\\
&\Phi(w) = \frac{1}{\sqrt{2\pi}}\int_w^{\infty} {\rm e}^{-x^2/2}\,{\rm d}x. \quad (48)
\end{aligned}$$

and $e_{\rm p}^c = e(e_{1,c}^{\rm U})$.

Combined with the lower bounds of $Q_{1,c}$, $Q_{1,\bar{c}}$ and the upper bounds of $e_{1,c}$, $e_{1,\bar{c}}$, equation (45) can be expressed by

$$\begin{aligned}
\ell_c \;=\; &\min(x)\Bigg\{N(1-p_{\rm pe})\Bigg[Q_{\bar{c}}\delta_0 x - \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\\
&+\Bigg[\frac{\delta_1 Q_{\bar{c}}((\delta_2-\delta)-(\delta_2-\delta_0)x-\chi)}{\delta_2-\delta_1}\\
&-\sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}(Q^{\bar{c}})^2}}\Bigg][1-H_2(e_{\rm p}^c)]\Bigg]\Bigg\}\\
&-(1-p_{\rm pe})\lambda_{\rm EC}^c - 6\log_2\frac{10}{\varepsilon_{\rm sec}} - \log_2\frac{2}{\varepsilon_{\rm sec}},\\
&(0\le x\le \min\{2E_c\delta/\delta_0, 2E_{\bar{c}}\}). \quad (49)
\end{aligned}$$

According to the definition of the key generation rate, it is the fraction of the length of secret key and the number of total pulses, i.e., $R = \ell/N$. One can obtain the final key generation rate as

$$\begin{aligned}
R_1 \;=\; &\min(x)\Bigg\{(1-p_{\rm pe})\Bigg[Q_{\bar{c}}\delta_0 x - \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\\
&+\Bigg[\frac{\delta_1 Q_{\bar{c}}((\delta_2-\delta)-(\delta_2-\delta_0)x-\chi)}{\delta_2-\delta_1}\\
&-\sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\Bigg][1-H_2(e_{\rm p}^c)]\Bigg]\Bigg\}\\
&-(1-p_{\rm pe})Q_c f(E_c)H_2(E_c) - \frac{6}{N}\log_2\frac{10}{\varepsilon_{\rm sec}} - \frac{1}{N}\log_2\frac{2}{\varepsilon_{\rm sec}},\\
&(0\le x\le \min\{2E_c\delta/\delta_0, 2E_{\bar{c}}\}). \quad (50)
\end{aligned}$$

However, it has been noted that the decoy state also has contributions to the key generation rate in the passive decoy-state method, so equation (44) is not suitable here. Recently, reference [36] considered the key generation rate of the decoy state of the passive decoy-state method and gave the length of the secret key in this situation as

$$\ell_{c+\bar{c}} = \left\lfloor H_{\min}^{v}(X_A^c X_A^{\bar{c}} | I^c I^{\bar{c}}) - 2\log_2\frac{1}{2\bar{v}}\right\rfloor, \quad (51)$$

where $X_A^{\bar{c}}$ is the raw key extracted from the decoy states and $I^{\bar{c}}$ is the information that Eve can get from $X_A^{\bar{c}}$.

The final secret key can be said to be $\varepsilon_{\rm sec}$-secret if its length $\ell_{c+\bar{c}}$ is chosen by

$$\begin{aligned}
\ell_{c+\bar{c}} \;\ge\; &n_0^c + n_0^{\bar{c}} + n_1^c[1-H_2(e_{\rm p}^c)] + n_1^{\bar{c}}[1-H_2(e_{\rm p}^{\bar{c}})]\\
&-\lambda_{\rm EC}^c - \lambda_{\rm EC}^{\bar{c}} - 12\log_2\frac{15}{\varepsilon_{\rm sec}} - \log_2\frac{16}{\varepsilon_{\rm cor}} - 1, \quad (52)
\end{aligned}$$

where $\lambda_{\rm EC}^{\bar{c}} = NQ_{\bar{c}}f(E_{\bar{c}})H_2(E_{\bar{c}})$.

Now, combined with the lower bounds of the single-photon counting rate and the upper bounds of the error rate that have been calculated above, one can obtain the length of the final secret key as

$$\begin{aligned}
\ell_{c+\bar{c}} \;=\; &\min(x)\Bigg\{N(1-p_{\rm pe})Q_{\bar{c}}\Bigg[\Bigg(\delta_0 x + x - \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\Bigg)\\
&+\Bigg(\delta_1\frac{Q_{1,\bar{c}}}{Q_{\bar{c}}} - \sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}(Q_{\bar{c}})^2}}\Bigg)[1-H_2(e_{\rm p}^c)]\\
&+\frac{Q_{1,\bar{c}}}{Q_{\bar{c}}}[1-H_2(e_{\rm p}^{\bar{c}})]\Bigg]\Bigg\}\\
&-N(1-p_{\rm pe})Q_c f_{\rm EC}H_2(E_c) - N(1-p_{\rm pe})Q_{\bar{c}}f_{\rm EC}H_2(E_{\bar{c}})\\
&-12\log_2\frac{15}{\varepsilon_{\rm sec}} - \log_2\frac{4}{\varepsilon_{\rm sec}} - 1,\\
&(0\le x\le \min\{2E_c\delta/\delta_0, 2E_{\bar{c}}\}), \quad (53)
\end{aligned}$$

where $e_{\rm p}^{\bar{c}} = e(e_{1,\bar{c}}^{\rm U})$, n and l can be taken from $NQ_{1,\bar{c}}(1-p_{\rm pe})$ and $NQ_{1,\bar{c}}p_{\rm pe}$.

According to the definition of the key generation rate, the final key generation rate under this condition is

$$\begin{aligned}
R_2 \;=\; &(1-p_{\rm pe})\min(x)\Bigg\{Q_{\bar{c}}x(\delta_0+1) - \sqrt{\frac{\delta_0 p_0^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\\
&+\Bigg[\frac{\delta_1 Q_{\bar{c}}((\delta_2-\delta)-(\delta_2-\delta_0)x-\chi)}{\delta_2-\delta_1}\\
&-\sqrt{\frac{\delta_1 p_1^t \ln(1/\varepsilon_{\rm pe})}{2Np_{\rm pe}}}\Bigg][1-H_2(e_{\rm p}^c)]\\
&+\frac{Q_{\bar{c}}[(\delta_2-\delta)-(\delta_2-\delta_0)x-\chi]}{\delta_2-\delta_1}[1-H_2(e_{\rm p}^{\bar{c}})]\Bigg\}\\
&-(1-p_{\rm pe})(Q_c f(E_c)H_2(E_c) - Q_{\bar{c}}f(E_{\bar{c}})H_2(E_{\bar{c}}))\\
&-\frac{12}{N}\log_2\frac{15}{\varepsilon_{\rm sec}} - \frac{1}{N}\log_2\frac{4}{\varepsilon_{\rm cor}} - \frac{1}{N},\\
&(0\le x\le \min\{2E_c\delta/\delta_0, 2E_{\bar{c}}\}), \quad (54)
\end{aligned}$$

where

$$\begin{aligned}
&Q_t = 1-(1-Y_0){\rm e}^{-\eta_{\rm sys}\omega}I_{0,\eta_{\rm sys}\xi}, \quad (55)\\
&Q_{\bar{c}} = P_{\bar{c}} - (1-d_A)(1-Y_0){\rm e}^{(\eta_{\rm d}-\eta_{\rm sys})\omega-\eta_{\rm d}\upsilon}I_{0,(\eta_{\rm d}-\eta_{\rm sys})\xi}, \quad (56)\\
&Q_c = Q_t - Q_{\bar{c}}, \quad (57)\\
&E_t = (e_0-e_{\rm d})Y_0/Q_t + e_{\rm d}, \quad (58)
\end{aligned}$$

$$E_{\bar{c}} = (e_0 - e_d)Y_0 P_{\bar{c}}/Q_{\bar{c}} + e_d, \quad (59)$$

$$E_c = E_t - E_{\bar{c}}, \quad (60)$$

and $I_{a,b}$ represents the modified Bessel function of the first kind.

Finally, the length of the final secret key is

$$R = \max\{R_1, R_2\}. \quad (61)$$

6. Numerical simulations

In this section, we will take some numerical simulations to show how the finite-length key influences the final key generation rate of the passive decoy-state method. In the scenario we considered, the yields Y_n can be expressed by

$$Y_n = 1 - (1 - Y_0)(1 - \eta_{sys})^n, \quad (62)$$

where η_{sys} denotes the overall transmittance of the system. It can be written as

$$\eta_{sys} = \eta_c \eta_{Bob}, \quad (63)$$

where η_{Bob} denotes the overall transmittance of Bob's detection apparatus and η_c is the transmittance of the quantum channel. It can be calculated by $\eta_c = 10^{-\alpha d/10}$, where d represents the transmission distance measured in km for the given QKD schemes and α denotes the loss coefficient of the channel (e.g., an optical fiber) measured in dB/km.

The parameters p_n^t, $p_n^{\bar{c}}$, and p_n^c are calculated by Eqs. (6)–(8), respectively. We set $\mu_1 = 0.5$ and $\mu_2 = 0.0001$. In this paper, ε_{sec} and ε_{cor} are 10^{-10} and 10^{-12}, respectively. The other parameter values in detail are listed in Table 1.[50]

Table 1. Experimental QKD parameters.

α/dB·km^{-1}	η_{Bob}	e_d	Y_0	η_d	d_A	$f(E_c), f(E_{\bar{c}})$
0.2	0.1	0.005	1.7×10^{-6}	0.5	3.2×10^{-6}	1.16

Figure 2 shows the relationship between the key generation rate R and the transmission distance d when the number N ($N = 10^i$, $i = 7, 8, 9, 10, \infty$) of the total pulses from the WCP source is fixed by different values. From Fig. 2, we can directly see that R becomes smaller with the increase of d. When the transmission distance d is fixed, the key generation rate R is getting larger with the increase of N. Meanwhile, when N is very small (e.g., $N = 10^7$), the declining rate is fast. It would generate few keys if $d \geq 55$ km. The curve of $N = 10^{10}$ is getting close to the ideal situation; it indicates that the number of total pulses from the WCP source can really influence the QKD system. When the number of total pulses is larger than 10^{10}, the passive decoy-state QKD with the WCP source can implement well. However, by comparing these results with the results in Ref. [50], it can be seen that the passive decoy-state method is weaker than the active one both in the key generation rate and the extra transmission distance.

Figure 3 shows the relationship between the key generation rate R and the number of total pulses N when the transmission distances are different. We can find that the passive decoy-state method can generate keys when N is 2×10^7, 3.5×10^7, 7×10^7 with 60 km, 70 km, and 80 km. When R is fixed, it needs more pulses with d becoming larger.

Finally, we analyse the relationship between R and d with different p_{pe} which means the probability of choosing a pulse as the sample bits used for parameter estimation when N is fixed. Figure 4 is an example whose $N = 10^9$. When the transmission distance is 60 km, it is easy to find that the lines of $p_{pe} = 0.5$ and $p_{pe} > 0.5$ are coincident which means that the key generation rates of $p_{pe} = 0.5$ and $p_{pe} > 0.5$ are almost equal. According to the definition of p_{pe}, the more pulses will be used to generate the key if it is getting smaller. Then, the QKD system can get more secure key bits. Hence, considering a compromised scheme, we take $p_{pe} = 0.5$ as an optimal reference value.

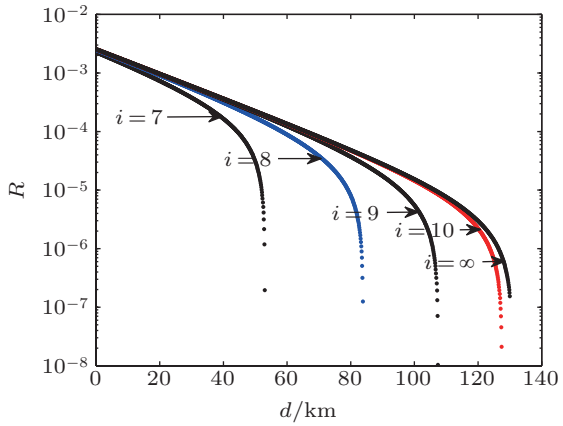


Fig. 2. (color online) Key generation rate R versus transmission distance d with different N ($N = 10^i$, $i = 7, 8, 9, 10, \infty$).

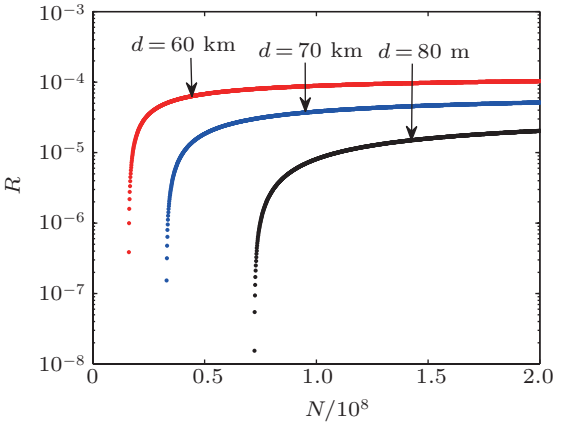


Fig. 3. (color online) Key generation rate R versus N with different d.

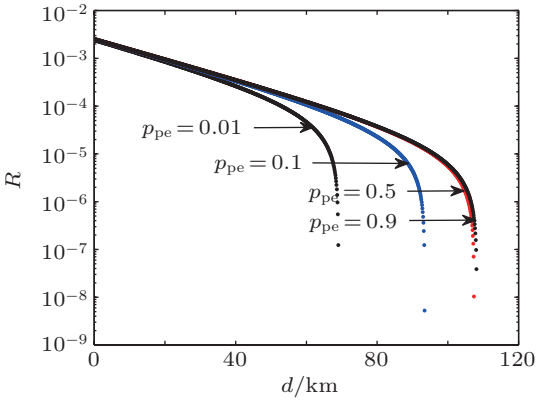


Fig. 4. (color online) Key generation rate R versus transmission distance d with different $p_{\rm pe}$.

7. Conclusions

In summary, we introduce the decoy state method and analyze the phase-randomized WCP source that can be used in passive decoy-state protocol. Then, we study the passive decoy-state method using the WCP source with an infinite-length key. After recalculating the phase error rate, counting rate, and error rate of the single photon state, we obtain the length of the secret key considering both the signal state and the decoy state in the passive decoy-state method. According to the results of numerical simulations, we find that the finite-length key influences the real QKD system. It can affect the key generation rate and the transmission distance. The key generation rate and the extreme transmission distance become larger with the increase of the number of total pulses. When the number is larger than 10^{10}, the passive decoy-state QKD with the WCP source will perform well. Meanwhile, we study the relationship between the key generation rate and the probability of choosing a pulse as the sample bits used for parameter estimation. It can help us to select the optimal value to make sure that the passive decoy-state method in this paper will be implemented best. Our work can help QKD experimentalists to improve the performance and provide references about how to choose the data-size.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing Bangalore*, India (New York: IEEE) pp. 175–179
[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[3] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press) Chaps. 2 and 12
[4] Lo H K and Chau H F 1990 *Science* **283** 2050
[5] Shor P and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[6] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[7] Wang S, Chen W, Guo J F and Yin Z Q 2012 *Opt. Lett.* **37** 1008
[8] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 *Nat. Photonics* **7** 378
[9] Wang J Y 2013 *Nat. Photonics* **7** 387
[10] Zhao L Y, Li H W, Yin Z Q, Chen W, You J and Han Z F 2014 *Chin. Phys. B* **23** 100304
[11] Li M, Treeviriyanupab P, Zhang C M, Yin Z Q, Chen W and Han Z F 2015 *Chin. Phys. B* **24** 010302
[12] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev N 2009 *Rev. Mod. Phys.* **81** 1301
[13] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[14] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[15] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[16] Wang X B 2005 *Phys. Rev. A* **72** 012322
[17] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev. A* **72** 012326
[18] Acin A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 *Phys. Rev. Lett.* **98** 230501
[19] Gisin N, Pironio S and Sangouard N 2010 *Phys. Rev. Lett.* **105** 070501
[20] Pawlowski M and Brunner N 2011 *Phys. Rev. A* **84** 010302
[21] Braunstein S L and Pirandola S 2012 *Phys. Rev. Lett.* **108** 130502
[22] Lo H K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503
[23] Tamaki K, Lo H K, Fung C H F and Qi B 2012 *Phys. Rev. A* **85** 042307
[24] Ma X F and Razavi M 2012 *Phys. Rev. A* **86** 062319
[25] Zhou C, Bao W S, Chen W, Li H W, Yin Z Q, Wang Y and Han Z F 2013 *Phys. Rev. A* **88** 052333
[26] Li F Y, Yin Z Q, Li H W, Chen W, Wang S, Wen H, Zhao Y B and Han Z F 2014 *Chin. Phys. Lett.* **31** 070302
[27] Dong C, Zhao S H, Zhang N, Dong Y, Zhao W H and Liu Y 2014 *Acta Phys. Sin* **63** 200304 (in Chinese)
[28] Dong C, Zhao S H, Dong Y, Zhao W H and Zhao J 2014 *Acta Phys. Sin* **63** 170303 (in Chinese)
[29] Hayashi M 2007 *Phys. Rev. A* **76** 012329
[30] Li H W, Zhao Y B, Yin Z Q, Wang S, Han Z F, Bao W S and Guo G C 2009 *Opt. Commun.* **282** 4162
[31] Song T T, Zhang J, Qin S J and Wen Q Y 2011 *Quantum Inf. Comput.* **11** 374
[32] Somma R D and Hughes R J 2013 *Phys. Rev. A* **87** 062330
[33] Scarani and Renner R 2008 *Phys. Rev. Lett.* **100** 200501
[34] Tan Y G and Cai Q Y 2011 *Internation Journal of Quantum Information* **9** 903
[35] Tan Y G and Cai Q Y 2010 *Eur. Phys. J. D* **56** 449
[36] Zhou C, Bao W S, Li H W, Wang Y, Li Y, Yin Z Q, Chen W and Han Z F 2014 *Phys. Rev. A* **89** 052328
[37] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J A 1992 *J. Cryptology* **5** 3
[38] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev. A* **51** 1863
[39] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[40] Ma X and Lütkenhaus N 2008 *New J. Phys.* **10** 073018
[41] Mauerer W and Silberhorn C 2007 *Phys. Rev. A* **75** 050305
[42] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
[43] Curty M, Morder T, Ma X and Lutkenhaus N 2009 *Opt. Lett.* **34** 3238
[44] Curty M, Ma X, Qi B, and Moroder T 2010 *Phys. Rev. A* **81** 022310
[45] Renner R 2008 *Int. J. Quantum Inf.* **6** 1
[46] Muller-Quade J and Renner R 2009 *New J. Phys.* **11** 085006
[47] Vitnov A, Dupuis F, Tomamichel M and Renner R 2013 *IEEE Trans. Inf. Theory* **59** 2603
[48] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 *Nat. Commun.* **3** 634
[49] Mertz M, Kampermann H, Bratzik S and Bruss D 2013 *Phys. Rev. A* **87** 012315
[50] Lim C C W, Curty M, Walenata F, Xu F and Zbinden H 2014 *Phys. Rev. A* **89** 022307