New protocols for non-orthogonal quantum key distribution*

Zhou Yuan-Yuan(周媛媛)†, Zhou Xue-Jun(周学军), Tian Pei-Gen(田培根), and Wang Ying-Jian(王瑛剑)

School of Electronic Engineering, Naval University of Engineering, Wuhan 430033, *China*

(Received 1 June 2012; revised manuscript received 9 July 2012)

Combining the passive decoy-state idea with the active decoy-state idea, a non-orthogonal (SARG04) decoy-state protocol with one vacuum and two weak decoy states is introduced based on a heralded pair coherent state photon source for quantum key distribution. Two special cases of this protocol are deduced, i.e., a one-vacuum-and-one-weak-decoy-state protocol and a one-weak-decoy-state protocol. In these protocols, the sender prepares decoy states actively, which avoids the crude estimation of parameters in the SARG04 passive decoy-state method. With the passive decoy-state idea, the detection events on Bob's side that are non-triggered on Alice's side are not discarded, but used to estimate the fractions of single-photon and two-photon pulses, which offsets the limitation of the detector's low efficiency and overcomes the shortcoming that the performance of the active decoy-state protocol critically depends on the efficiency of detector. The simulation results show that the combination of the active and passive decoy-state ideas increases the key generation rate. With a one-vacuum-and-two-weak-decoy-state protocol, one can achieve a key generation rate that is close to the theoretical limit of an infinite decoy-state protocol. The performance of the other two protocols is a little less than with the former, but the implementation is easier. Under the same condition of implementation, higher key rates can be obtained with our protocols than with existing methods.

Keywords: quantum key distribution, non-orthogonal encoding protocol, active decoy state, passive decoy state

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/22/1/010305

1. Introduction

Quantum key distribution (QKD)[1] has drawn considerable attention as a method of achieving a shared unconditional secure private key. However, there are still some technical limitations in practice, such as an imperfect single source, large loss channel, and inefficient detectors, which will threaten the security and reduce the performance of the practical QKD. Recently, many methods[2–10] have been devised to deal with these imperfect conditions, among which, the decoy-state method[2] is thought to be a very useful candidate for substantially enhancing the performance of QKD. The motivation of decoy states is to estimate the channel properties better. To do that, Alice uses extra states (decoy states) with different light intensities during key transmission. Then Alice and Bob can consider detection statistics from the signal and decoy states separately, from which they can better estimate the channel transmittance and error probability.

Recently, it has become the most efficient and prominent method[11–25] to bring decoy states and different kinds of photon sources together for a better performance and an earlier implementation of the real-life QKD system. With the application of a decoy-state method in a weak coherent source (WCS) model, the key rate can be improved and the secure distance can be prolonged from 30 km (without decoy states) to 140 km for BB84 protocol.[5,11] Subsequently, the heralded single photon source (HSPS) brings a further improvement to 170 km in the secure distance,[13] but only supplies a moderate key rate at a short and medium distance compared with that of BB84+WCS. Some researchers gave a consideration[17–19] of the non-orthogonal encoding protocol (SARG04),[20] and there was also a crossover between the maximal secure distance and the secure key generation rate in short and middle distance if one applies these two sources (WCS and HSPS) in a practical decoy-state QKD. In order to obtain the optimal secure key generation rate for each transmission distance, Zhang *et al*.[19] used a heralded pair coherent state (HPCS) photon source in decoy-state QKD and gained a good result.

The above decoy-state methods are all active decoy-state methods, in which Alice needs actively prepared decoy states through adding attenuators or photon sources. In order to decrease the implementation difficulty, a passive decoy-state method[21–27] was proposed, where Alice does not actively prepare decoy states, but chooses decoy and signal states by passive measurements. Therefore, a passive decoy-state method does not require any additional hardware change on the standard QKD system for creating decoy states, and performs similar to a one-weak-active-decoy-state method.[28]

In this paper, we consider the SARG04 protocol. From the BB84 to the SARG04 protocol, only a modification of the classical communication part changes the foundation of secu-

*Project supported by the National High Technology Research and Development Program of China (Grant No. 2011AA7014061) and the Science Foundation of Naval University of Engineering, China (Grant No. HGDQNJJ11022).

†Corresponding author. E-mail: zyy_hjgc@yahoo.com.cn

© 2013 Chinese Physical Society and IOP Publishing Ltd

rity and makes two-photon signals secure. Therefore, it is not difficult to perform the SARG04 scheme only if the experiment of the BB84 protocol is available.[29] Thus, it is important to investigate the performance of the SARG04 scheme in order to determine which protocol one should perform. Because the number of parameters estimated in SARG04 is twice that in the BB84 protocol, the existing SARG04 active decoy-state methods[17–19] use more decoy states than BB84, which will increase the difficulty of implementation. However, SARG04 passive decoy-state methods[26,27] are not very efficient for a crude estimation. In this paper, we will combine the active decoy-state idea with the passive decoy-state idea, and present a new SARG04 one-vacuum-and-two-weak-decoy-state protocol with an HPCS. Combining the two weak decoy states in the above protocol, a one-vacuum-and-one-weak-decoy-state protocol is presented for easier implementation. Considering the imperfect extinction ratio of the practical laser, vacuum states are not prepared easily. Therefore, a simpler protocol with one weak decoy state is proposed. Furthermore, by use of the experimental parameters of the experiment by Gobby, Yuan, and Shields (GYS),[30] our protocols can obtain better performance compared with existing methods.

2. Improved decoy-state methods

The pair coherent state (PCS), which was originally proposed by Agarwal,[31] is a two-mode correlated coherent state. The two modes of the PCS are symmetric. By tracing out any mode, the other mode will definitely follow

$$\rho = \sum_{n=0}^{\infty} P_n |n\rangle \langle n| = \sum_{n=0}^{\infty} \frac{1}{I_0(2x)} \frac{x^{2n}}{(n!)^2} |n\rangle \langle n|, \tag{1}$$

where $|n\rangle$ represents an n-photon state, x is the intensity of one mode, P_n is the probability to gain an n-photon pair, and I_0 is the modified Bessel's function of the first kind.

In our scheme, a PCS source is used as a heralded pair coherent state source. One mode goes to Alice's own detector as the triggering signal, and the other mode is used as a triggered single photon state for the QKD and sent out to Bob. When Alice's detector clicks, we call it a trigger. We divide the detection events on Bob's side into two groups depending on whether Alice gets a trigger or not: triggered detection events and non-triggered detection events. The difference from the active decoy-state method is that Bob's detector needs to work no matter if Alice's detector is triggered or not and both triggered and non-triggered components are used to deduce a more accurate value of the key generation rate. Here, we are interested in the case that Alice and Bob use threshold detectors.

We define Y_n as the yield of an n-photon state, i.e., the probability that Bob's detector clicks whenever Alice sends out state $|n\rangle$. We also define G_n to be the gain of an n-photon state, i.e., the rate of events when Alice emits an n-photon state and Bob detects the signal, which can be divided into two groups, one group triggered by Alice, $G_n^{(\mathrm{t})}$, and the rest, $G_n^{(\mathrm{nt})}$.

$$G_n^{(\mathrm{t})} = Y_n [1-(1-\eta_{\mathrm{A}})^n] \frac{1}{I_0(2x)} \frac{x^{2n}}{(n!)^2}, \tag{2}$$

$$G_n^{(\mathrm{nt})} = Y_n (1-\eta_{\mathrm{A}})^n \frac{1}{I_0(2x)} \frac{x^{2n}}{(n!)^2}, \tag{3}$$

where η_{A} is the detecting efficiency on Alice's side.

Then we define Q_x to be the overall rate according to the intensity x. The Q_x can also be divided into two groups, $Q_x^{(\mathrm{t})}$ and $Q_x^{(\mathrm{nt})}$, which can be expressed as

$$Q_x^{(\mathrm{t})} = \frac{Y_0 d_{\mathrm{A}}}{I_0(2x)} + \sum_{n=1}^{\infty} G_n^{(\mathrm{t})}, \tag{4}$$

$$Q_x^{(\mathrm{nt})} = \frac{Y_0 (1-d_{\mathrm{A}})}{I_0(2x)} + \sum_{n=1}^{\infty} G_n^{(\mathrm{nt})}, \tag{5}$$

where d_{A} is the dark count rate of Alice's detector.

We denote the error rate of the n-photon state as e_n. Similar to expressions (4) and (5), the quantum bit error rates (QBERs) are given by

$$E_x^{(\mathrm{t})} Q_x^{(\mathrm{t})} = \frac{Y_0 e_0 d_{\mathrm{A}}}{I_0(2x)} + \sum_{n=1}^{\infty} G_n^{(\mathrm{t})} e_n, \tag{6}$$

$$E_x^{(\mathrm{nt})} Q_x^{(\mathrm{nt})} = \frac{Y_0 e_0 (1-d_{\mathrm{A}})}{I_0(2x)} + \sum_{n=1}^{\infty} G_n^{(\mathrm{nt})} e_n, \tag{7}$$

where $e_0 = 1/2$ is the error rate of background counts.

All the data measured can be grouped according to Alice's detection events, so we can apply the Gottesman–Lo–Lütkenhaus–Preskill (GLLP)[32] idea to each group. The final key generation rate will be given by summing over contributions from both the groups, $R^{(\mathrm{both})} = R^{(\mathrm{t})} + R^{(\mathrm{nt})}$.

Both $R^{(\mathrm{t})}$ and $R^{(\mathrm{nt})}$ can be expressed by

$$\begin{aligned} R^{(\mathrm{t})} \geq \frac{1}{4} \Big\{ & -Q_u^{(\mathrm{t})} f\left(E_u^{(\mathrm{t})}\right) H_2\left(E_u^{(\mathrm{t})}\right) + G_0^{(\mathrm{t})} \\ & + G_1^{(\mathrm{t})} [1-H_2(e_1)] + G_2^{(\mathrm{t})} [1-H_2(e_2)] \Big\}, \end{aligned} \tag{8}$$

$$\begin{aligned} R^{(\mathrm{nt})} \geq \frac{1}{4} \Big\{ & -Q_u^{(\mathrm{nt})} f\left(E_u^{(\mathrm{nt})}\right) H_2\left(E_u^{(\mathrm{nt})}\right) + G_0^{(\mathrm{nt})} \\ & + G_1^{(\mathrm{nt})} [1-H_2(e_1)] + G_2^{(\mathrm{nt})} [1-H_2(e_2)] \Big\}, \end{aligned} \tag{9}$$

where the factor 1/4 is the sifting efficiency of the SARG04 protocol, $f(E_u)$ is the bidirectional error correction efficiency, and $H_2(x)$ is the binary Shannon information entropy function given by $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$.

If the transmission distance is too large, the non-triggered components will cease to contribute a positive key generation rate.[21] Hence, if either of them contributes a negative key generation rate, we should assign it 0. In this case, the final key rate is given by $R = \max\{R^{(\mathrm{both})}, R^{(\mathrm{t})}\}$.

In the experiment, $Q_u^{(\mathrm{t})}$, $Q_u^{(\mathrm{nt})}$, $E_u^{(\mathrm{t})}$, and $E_u^{(\mathrm{nt})}$ can be observed directly. In order to distill the secure final key, we need to deduce the lower bounds of Y_1 and Y_2 as well as the upper bounds of e_1 and e_2.

2.1. One vacuum and two weak decoy states

In our scheme, we require Alice to randomly change the intensity of her pump light between four values, so that the intensity of one mode is randomly changed between 0, v_1, v_2, and u ($0 < v_1 < u$, $0 < v_2 < u$).

In the next step, we will use the triggered events of v_1 ($Q_{v_1}^{(\mathrm{t})}$) and the non-triggered events of u ($Q_u^{(\mathrm{nt})}$) to deduce a tight lower bound of the yield of single photon (Y_1). Expressions (4) and (5) lead to

$$\begin{aligned} & I_0(2u)Q_u^{(\mathrm{nt})}\left[1-(1-\eta_{\mathrm{A}})^2\right]v_1^4 - I_0(2v_1)Q_{v_1}^{(\mathrm{t})}(1-\eta_{\mathrm{A}})^2u^4 \\ = & Y_0\left\{(1-d_{\mathrm{A}})\left[1-(1-\eta_{\mathrm{A}})^2\right]v_1^4 - d_{\mathrm{A}}(1-\eta_{\mathrm{A}})^2u^4\right\} \\ & + Y_1\left\{u^2v_1^4(1-\eta_{\mathrm{A}})\left[1-(1-\eta_{\mathrm{A}})^2\right] - v_1^2u^4\eta_{\mathrm{A}}(1-\eta_{\mathrm{A}})^2\right\} \\ & + \sum_{n=3}^{\infty}\frac{Y_n}{(n!)^2}\{u^{2n}v_1^4(1-\eta_{\mathrm{A}})^n\left[1-(1-\eta_{\mathrm{A}})^2\right] \\ & - v_1^{2n}u^4\left[1-(1-\eta_{\mathrm{A}})^n\right](1-\eta_{\mathrm{A}})^2\}. \end{aligned} \tag{10}$$

Assume the condition

$$\begin{aligned} & u^{2n}v_1^4(1-\eta_{\mathrm{A}})^n\left[1-(1-\eta_{\mathrm{A}})^2\right] \\ & - v_1^{2n}u^4\left[1-(1-\eta_{\mathrm{A}})^n\right](1-\eta_{\mathrm{A}})^2 \le 0 \end{aligned}$$

can be satisfied when

$$u\left\{\frac{(1-\eta_{\mathrm{A}})^{n-2}\left[1-(1-\eta_{\mathrm{A}})^2\right]}{1-(1-\eta_{\mathrm{A}})^n}\right\}^{1/(2n-4)} \le v_1 < u.$$

Then, the lower bound of Y_1 is given by

$$Y_1 \ge Y_1^{\mathrm{L}} = \frac{I_0(2u)Q_u^{(\mathrm{nt})}\left[1-(1-\eta_{\mathrm{A}})^2\right]v_1^4 - I_0(2v_1)Q_{v_1}^{(\mathrm{t})}(1-\eta_{\mathrm{A}})^2u^4 - Y_0\left\{(1-d_{\mathrm{A}})\left[1-(1-\eta_{\mathrm{A}})^2\right]v_1^4 - d_{\mathrm{A}}(1-\eta_{\mathrm{A}})^2u^4\right\}}{u^2v_1^4(1-\eta_{\mathrm{A}})\left[1-(1-\eta_{\mathrm{A}})^2\right] - v_1^2u^4\eta_{\mathrm{A}}(1-\eta_{\mathrm{A}})^2}. \tag{11}$$

In the same way, we can use $Q_{v_2}^{(\mathrm{t})}$ and $Q_u^{(\mathrm{nt})}$ to deduce a lower bound of the yield of two photons (Y_2).

$$\begin{aligned} & I_0(2u)Q_u^{(\mathrm{nt})}v_2^2\eta_{\mathrm{A}} - I_0(2v_2)Q_{v_2}^{(\mathrm{t})}u^2(1-\eta_{\mathrm{A}}) \\ = & Y_0\left[(1-d_{\mathrm{A}})\eta_{\mathrm{A}}v_2^2 - d_{\mathrm{A}}(1-\eta_{\mathrm{A}})u^2\right] + Y_2\left\{\frac{u^4v_2^2}{4}(1-\eta_{\mathrm{A}})^2\eta_{\mathrm{A}} - \frac{v_2^4u^2}{4}\left[1-(1-\eta_{\mathrm{A}})^2\right](1-\eta_{\mathrm{A}})\right\} \\ & + \sum_{n=3}^{\infty}\frac{Y_n}{(n!)^2}\left\{u^{2n}v_2^2(1-\eta_{\mathrm{A}})^n\eta_{\mathrm{A}} - v_2^{2n}u^2\left[1-(1-\eta_{\mathrm{A}})^n\right](1-\eta_{\mathrm{A}})\right\}. \end{aligned} \tag{12}$$

In the condition that $u\left\{\frac{(1-\eta_{\mathrm{A}})^{n-1}\eta_{\mathrm{A}}}{1-(1-\eta_{\mathrm{A}})^n}\right\}^{1/(2n-2)} \le v_2 < u$, we can obtain the lower bound of Y_2 as

$$Y_2 \ge Y_2^{\mathrm{L}} = \frac{4\left\{I_0(2u)Q_u^{(\mathrm{nt})}v_2^2\eta_{\mathrm{A}} - I_0(2v_2)Q_{v_2}^{(\mathrm{t})}u^2(1-\eta_{\mathrm{A}}) - Y_0\left[(1-d_{\mathrm{A}})\eta_{\mathrm{A}}v_2^2 - d_{\mathrm{A}}(1-\eta_{\mathrm{A}})u^2\right]\right\}}{u^4v_2^2(1-\eta_{\mathrm{A}})^2\eta_{\mathrm{A}} - v_2^4u^2\left[1-(1-\eta_{\mathrm{A}})^2\right](1-\eta_{\mathrm{A}})}. \tag{13}$$

Because the values of u, v_1, and v_2 can be chosen independently, the above assumption can be easily satisfied in the experiment.

According to expressions (6) and (7), an upper bound of e_1 and e_2 can be obtained

$$e_1 \le e_1^{\mathrm{U}} = \min\left\{\frac{E_u^{(\mathrm{t})}Q_u^{(\mathrm{t})}I_0(2u) - Y_0e_0d_{\mathrm{A}}}{Y_1^{\mathrm{L}}\eta_{\mathrm{A}}u^2}, \frac{E_u^{(\mathrm{nt})}Q_u^{(\mathrm{nt})}I_0(2u) - Y_0e_0(1-d_{\mathrm{A}})}{Y_1^{\mathrm{L}}(1-\eta_{\mathrm{A}})u^2}\right\}, \tag{14}$$

$$e_2 \le e_2^{\mathrm{U}} = \min\left\{\frac{4E_u^{(\mathrm{t})}Q_u^{(\mathrm{t})}I_0(2u) - 4Y_0e_0d_{\mathrm{A}}}{Y_2^{\mathrm{L}}\left[1-(1-\eta_{\mathrm{A}})^2\right]u^4}, \frac{4E_u^{(\mathrm{nt})}Q_u^{(\mathrm{nt})}I_0(2u) - 4Y_0e_0(1-d_{\mathrm{A}})}{Y_2^{\mathrm{L}}(1-\eta_{\mathrm{A}})^2u^4}\right\}. \tag{15}$$

2.2. One vacuum and one weak decoy state

As is well known, when the number of decoy states is bigger, the practical implementation of QKD is more difficult. In order to decrease the implementation difficulty, we combine the two weak decoy states (v_1, v_2) in the above protocol and obtain a simple method with one vacuum and one weak decoy state (v)

$$\max\left\{u\left\{\frac{(1-\eta_{\mathrm{A}})^{n-2}\left[1-(1-\eta_{\mathrm{A}})^2\right]}{1-(1-\eta_{\mathrm{A}})^n}\right\}^{1/(2n-4)}, u\left\{\frac{(1-\eta_{\mathrm{A}})^{n-1}\eta_{\mathrm{A}}}{1-(1-\eta_{\mathrm{A}})^n}\right\}^{1/(2n-2)}\right\} \le v < u. \tag{16}$$

By substituting v in Eqs. (11) and (13) with v_1 and v_2, we have the lower bounds ($Y_1^{L'}$ and $Y_2^{L'}$) of Y_1 and Y_2. By substituting Y_1^{L} and Y_2^{L} in Eqs. (14) and (15) with $Y_1^{L'}$ and $Y_2^{L'}$, the upper bounds ($e_1^{U'}$ and $e_2^{U'}$) of e_1 and e_2 are obtained.

2.3. One weak decoy state

Considering the imperfect extinction ratio of the practical laser, vacuum states are not prepared easily to estimate Y_0 very well. Thus, the method with one vacuum and one weak decoy state is reduced to a one-decoy-state method. Hence, we need to derive an upper bound of Y_0 from expressions (6) and (7) as

$$Y_0 \leq Y_0^{U} = \min\left\{\frac{E_u^{(t)}Q_u^{(t)}I(2u)}{e_0 d_A}, \frac{E_u^{(nt)}Q_u^{(nt)}I(2u)}{e_0(1-d_A)}\right\}. \quad (17)$$

By substituting the above upper bound into expressions (11) and (13), we have the lower bounds ($Y_1^{L''}$ and $Y_2^{L''}$) of Y_1 and Y_2. The crude upper bounds of e_1 and e_2 can be derived as follows:

$$e_1 \leq e_1^{U''} = \min\left\{\frac{E_u^{(t)}Q_u^{(t)}I_0(2u)}{Y_1^{L''}\eta_A u^2}, \frac{E_u^{(nt)}Q_u^{(nt)}I_0(2u)}{Y_1^{L''}(1-\eta_A)u^2}\right\}, \quad (18)$$

$$e_2 \leq e_2^{U''} = \min\left\{\frac{4E_u^{(t)}Q_u^{(t)}I_0(2u)}{Y_2^{L''}\left[1-(1-\eta_A)^2\right]u^4}, \frac{4E_u^{(nt)}Q_u^{(nt)}I_0(2u)}{Y_2^{L''}(1-\eta_A)^2u^4}\right\}. \quad (19)$$

3. Numerical simulation

Now, by substituting the bounds of Y_1, Y_2, e_1, and e_2 into expressions (8) and (9), we can calculate the final key rate. We use the parameters mainly from GYS experiment.[30] At Alice's side, $d_A = 10^{-6}$, $\eta_A = 0.3$; at Bob's side, $d_B = 1.7\times10^{-6}$, $\eta_B = 0.045$, $e_d = 0.033$, and $f = 1.22$. In simulation, the optimal u is chosen at each distance for each case.

Figure 1 shows that the key generation rate of the one-vacuum-and-two-weak-decoy-state protocol is the best, and the secure transmission distance can reach about 173 km. The performance of the one-vacuum-and-one-weak-decoy-state protocol is lower than that of the one-vacuum-and-two-weak-decoy-state protocol with unobvious difference. The key generation rate of the one-weak-decoy-state protocol is close to that of the former two protocols when the distance is not too large. However, its key generation rate will decrease obviously at a further distance. The reason is that estimation accuracy of parameters is reduced with less decoy states, but sacrifice of performance is exchanged for an easier implementation.

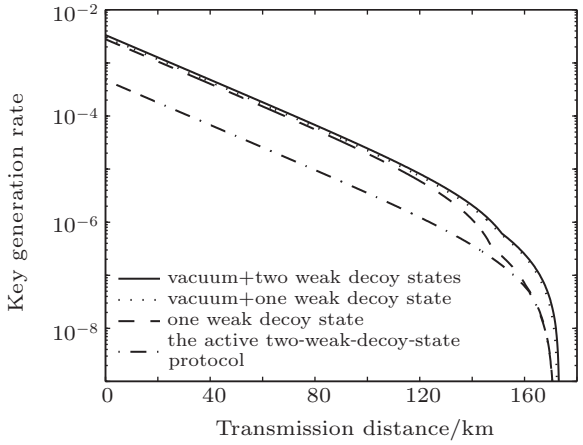


Fig. 1. Comparison among the performances of different SARG04 decoy-state menthods with HPCS.

In Fig. 1, there is an inflexion in each curve of our protocols; the inflexion of the one-vacuum-and-two-weak-decoy-state protocol is at a distance of about 151 km, the inflexion of the one-vacuum-and-one-weak-decoy-state protocol is at about 150 km, and the inflexion of the one-weak-decoy-state protocol is at about 147 km. Now, we will analyze the essence of the phenomenon. The function of Alice's detector is to detect the vacuum states. Hence, Bob avoids detecting a vacuum state as an i-photon state ($i \neq 0$). Because the real-life detector is not perfect, it is possible for Alice's detector to detect an i-photon state ($i \neq 0$) as a vacuum state. Here, Bob's detector will stop working in the active decoy-state method, namely, the i-photon states ($i \neq 0$) misdeemed are abandoned. In our protocols, Bob's detector needs to work no matter if Alice's detector is triggered or not. That is to say, the non-triggered detection events are not discarded, but used to estimate the parameters and generate the secure key. However, only the single-photon states and 2-photon states detected as vacuum states by Alice's detector can contribute to key generation. For the high-loss channel, the transmission distance of this part of the photon states is not too large. Hence, the non-triggered detection events can give a further improvement of the key generation rate at close range. It is obvious that the performance of our one-weak-decoy protocol is better than that of the active two-weak-decoy-state SARG04 protocol with HPCS in Ref. [19]. Consequently, the contribution of non-triggered detection events is considerable.

In Fig. 2, R_t represents the key generation rate of the theoretical limit of our protocol with infinite decoy states. The parameters R_{v2}, R_{v1} and R_1 denote the key generation rates of the one-vacuum-and-two-weak-decoy-state protocol, one-vacuum-and-one-weak-decoy-state protocol, and one-weak-decoy-state protocol, respectively. The ratio R_{v2}/R_t, which is the highest, exceeds 90% at a distance less than 169 km, and is higher than 95% within a range of 147 km. Compared with the other two protocols, the one-vacuum-and-two-weak-decoy-state protocol is more difficult to implement, but has the

distinct advantage of performance. The ratio R_{v1}/R_t is higher than 90% at a distance less than 164 km. Therefore, the one-vacuum-and-one-weak-decoy protocol sacrifices a fraction of performance to reduce the implementation difficulty. The ratio R_1/R_t is higher than 80% at a distance less than 117 km, even higher than 85% within a range of 95 km. If the demand of transmission distance for QKD is not too high, we can choose the one-weak-decoy protocol due to its simplicity of implementation and good performance.

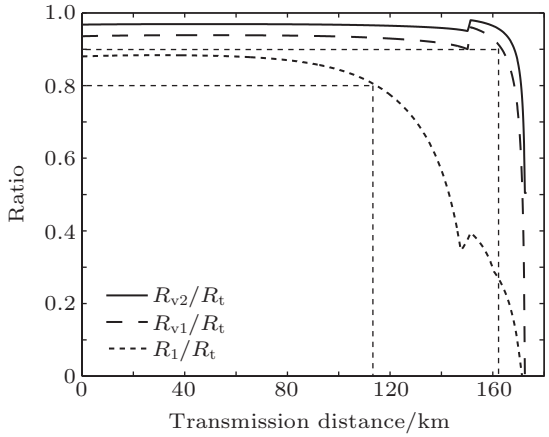


Fig. 2. Ratios of the key generation rate of the decoy-state methods to the theoretical limit of our protocol with infinite decoy states.

We calculate the final key rates of the one-vacuum-and-one-weak-decoy-state protocol with different detection efficiencies on Alice's side respectively ($\eta_A = 0.9, 0.6, 0.3, 0.1$). Figure 3 shows that the four cases provide approximately the same final key rate when the distance is not too large, and the four performance curves almost cannot be distinguished at short range with the resolution of this figure. Although the contribution of the triggered components to key generation descends with the decrease of η_A, the contribution of the non-triggered components increases. Contrarily, the contribution of the triggered components increases and that of the non-triggered components decreases with the increase of η_A. As one decreases, another increases. Thus, the total key generation rate does not change obviously. The performance of the active two-weak-decoy-state method in Ref. [19] decreases obviously when η_A changes from 0.9 to 0.1 because only the triggered components are used to generate keys. As a matter of fact, all active decoy-state protocols with heralded photon sources encounter the same problem that the performance critically relies on η_A. Fortunately, our protocols overcome this shortcoming and offset the limitation of the detector's low efficiency.

In Fig. 4, the three protocols are all one-weak-decoy-state protocols combining the passive decoy-state idea with the active decoy-state idea. That is to say, they are under the same condition of implementation. We can see that SARG04+HPCS is the optimal combination for the best performance.

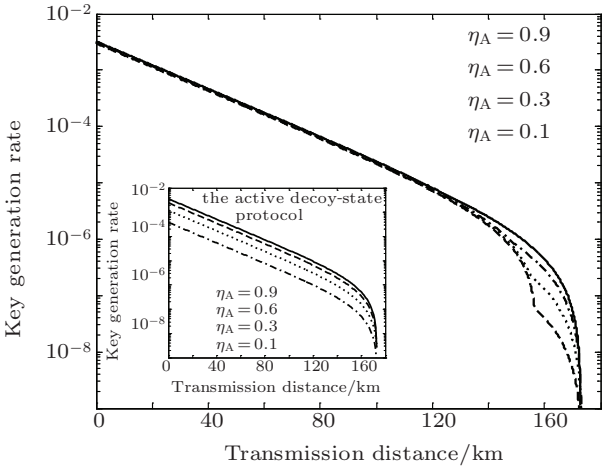


Fig. 3. Comparison of the performances of the one-vacuum-and-one-weak-decoy protocol with different detecting efficiencies on Alice's side.

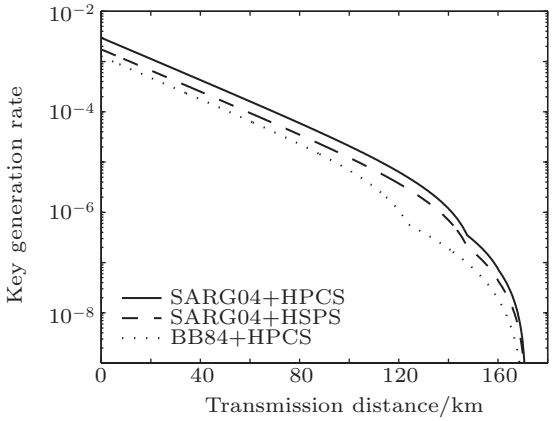


Fig. 4. Comparison of the performances of different decoy-state methods with one weak decoy state.

4. Conclusion

With an HPCS photon source, three SARG04 decoy-state protocols have been introduced, which combine the passive decoy-state idea with the active decoy-state idea. The first protocol is characterized by the best key generation rate and the longest secure distance with one vacuum and two weak decoy states. The second protocol with one vacuum and one weak decoy state permits an easier implementation. The third protocol with one weak decoy state is proposed for considering the difficult preparation of vacuum states. Our protocols have four merits. Firstly, different from the active decoy-state method, non-triggered detection events are not discarded and are used to estimate the parameters and generate the secure keys, which offsets the limitation of the detector's low efficiency. Secondly, different from the passive decoy-state method, decoy states need to be prepared actively, which provides a better estimation compared with the passive decoy-

state method for the SARG04 protocol. Thirdly, with the one-vacuum-and-two-weak-decoy-state protocol, one can achieve a key generation rate close to the theoretical limit of an infinite decoy-state protocol. With one of the other two protocols, a moderate performance and simplicity of implementation can be obtained. Thus, our protocols offer choices for different applications. Lastly, under the same condition of implementation, the performances of our methods are better than that of existing methods.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India) p. 175

[2] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[3] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[4] Wang X B 2005 *Phys. Rev.* A **72** 012322

[5] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[6] Smith G, Renes J M and Smolin J A 2008 *Phys. Rev. Lett.* **100** 170502

[7] Yin Z Q, Han Z F, Sun F W and Guo G C 2007 *Phys. Rev.* A **76** 014304

[8] Usenko V C and Paris M G A 2007 *Phys. Rev.* A **75** 043812

[9] Zhang L B, Zhong Y Y and Kang L 2008 *Chin. Sci. Bull* **53** 2668

[10] Christoph S, Hugues D R, Mikael A, Nicolas S, Hugo Z and Nicolas G 2007 *Phys. Rev. Lett.* **98** 190503

[11] Ma X F, Qi B, ZhaoY and Lo H K 2005 *Phys. Rew.* A **72** 012326

[12] Li J B and Fang X M 2006 *Chin. Phys. Lett.* **23** 775

[13] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev.* A **75** 012312

[14] Yin Z Q, Han Z F, Sun F W and Guo G C 2007 *Phys. Rev.* A **76** 014304

[15] Hu H P, Wang J D, Huang Y X, Liu S H and Lu W 2010 *Acta Phys. Sin.* **59** 287 (in Chinese)

[16] Mi J L, Wang F Q, Lin Q Q, Liang R S and Liu S H 2008 *Acta Phys. Sin.* **57** 678 (in Chinese)

[17] Zhang S L, Zou X B, Li K, Jin C H and Guo G C 2007 *Phys. Rev.* A **76** 044304

[18] Mi J L, Wang F Q, Lin Q Q and Liang R S 2008 *Chin. Phys.* B **17** 1178

[19] Zhang S L, Zou X B, Li C F, Jin C H and Guo G C 2009 *Chin. Sci. Bull* **54** 1863

[20] Scarani V, Acin A, Ribordy G and Gisi N 2004 *Phys. Rev. Lett.* **92** 057901

[21] Mauerer W and Silberhorn C 2007 *Phys. Rev.* A **75** 050305

[22] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503

[23] Quan D X, Pei C X, Zhu C H and Liu D 2008 *Acta Phys. Sin.* **57** 5600 (in Chinese)

[24] Curty M, Moroder T, Ma X F and Lütkenhaus N 2009 *Opt. Lett.* **34** 3238

[25] Curty M, Ma X F, Qi B and Moroder T 2010 *Phys. Rev.* A **81** 022310

[26] Xu F X, Wang S, Han Z F and Guo G C 2010 *Chin. Phys.* B **19** 100312

[27] Zhou Y Y and Zhou X J 2011 *Acta Phys. Sin.* **60** 100301 (in Chinese)

[28] Ma X F and Lo H K 2008 *New J. Phys.* **10** 073018

[29] Fung C H F, Tamaki K and Lo H K 2006 *Phys. Rev.* A **73** 012337

[30] Gobby C, Yuan Z L and Shields A J 2004 *Phys. Rev. Lett.* **84** 3762

[31] Agarwal G S 1986 *Phys. Rev. Lett.* **57** 827

[32] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inform. Comput.* **4** 325