Vol 17 No 4, April 2008
1674-1056/2008/17(04)/1178-06

Chinese Physics B

© 2008 Chin. Phys. Soc.
and IOP Publishing Ltd

# Practical non-orthogonal decoy state quantum key distribution with heralded single photon source*

Mi Jing-Long(米景隆), Wang Fa-Qiang(王发强)†,
Lin Qing-Qun(林青群), and Liang Rui-Sheng(梁瑞生)

*Laboratory of Photonic Information Technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou 510631, China*

(Received 12 July 2007; revised manuscript received 29 October 2007)

Recently the performance of the quantum key distribution (QKD) is substantially improved by the decoy state method and the non-orthogonal encoding protocol, separately. In this paper, a practical non-orthogonal decoy state protocol with a heralded single photon source (HSPS) for QKD is presented. The protocol is based on 4 states with different intensities, i.e. one signal state and three decoy states. The signal state is for generating keys; the decoy states are for detecting the eavesdropping and estimating the fraction of single-photon and two-photon pulses. We have discussed three cases of this protocol, i.e. the general case, the optimal case and the special case. Moreover, the final key rate over transmission distance is simulated. For the low dark count of the HSPS and the utilization of the two-photon pulses, our protocol has a higher key rate and a longer transmission distance than any other decoy state protocol.

**Keywords:** quantum key distribution, decoy state, non-orthogonal encoding protocol, heralded single photon source

**PACC:** 0365, 4250, 4230

## 1. Introduction

Quantum cryptography,[1] quantum key distribution (QKD), is the most mature field in quantum information, both theoretically and experimentally. QKD allows two distant partners, Alice and Bob, to communicate in absolute security, even in the presence of an eavesdropper, Eve. Unlike conventional cryptography, the QKD promises perfect security based on the fundamental laws of physics, the non-cloning theorem and the uncertainty principle. The security of QKD has been rigorously proven in a number of recent papers.[2,3]

Unfortunately, all of the recent experiments are insecure because the QKD systems in real life are generally based on attenuated laser pulses, which occasionally give out more than one photon. Those multi-photon pulses open the door to powerful eavesdropping attacks including the photon number splitting (PNS) attack.[4,5] Eve might block all single-photon pulses and splits multi-photon pulses, keeping one part himself and sending the rest to Bob. The security of practical QKD system has been discussed before.[6]

Recently, two important schemes have been presented to counter the PNS attack. One is the non-orthogonal encoding protocol SARG04 proposed by Scarani *et al.*[7] Compared with the two non-orthogonal encoding protocols,[8,9] the SARG04 protocol uses four exactly identical states of BB84 protocol,[10] but modifies the classical communication between Alice and Bob. Instead of revealing the basis, Alice announces publicly a pair of non-orthogonal states. Thus in the sifting phase Eve only knows that the state is either of two non-orthogonal states. In order to learn the bit with certainty without introducing errors, Eve has to implement an unambiguous state discrimination on the three-photon pulses. It means that two-photon pulses can be used to generate a secure key.

The other is the decoy state method proposed by Hwang[11] and further studied by Wang,[12,13] Lo's team,[14,15] and also Harrington *et al.*[16] The main idea is that in addition to a regular signal state, Alice also uses some decoy states. Alice randomly sends a signal state or a decoy state. After Bob's measurements of all pulses, Alice tells Bob which pulse is for the decoy state. So they can, by comparing their out-

*Project supported by the National Natural Science Foundation of China (Grant No 60578055) and the State Key Development Program for Basic Research of China (Grant No 2007CB307001).

†Corresponding author. E-mail: fqwang98@sina.com

comes of the decoy states, detect the PNS attack.

In the scheme of decoy state, it is easy for Alice and Bob to catch eavesdropper even with a coherent source. However, for the coherent source, the dark count may be the most important factor that restricts the transmission distance. As the technology on heralded single photon source(HSPS), which relies on photon pairs generated by spontaneous parametric down-conversion (SPDC), has been developed to a high level, we can use an HSPS to replace the weak coherent source. Because the dark count probability is reduced by the coincidence property of SPDC, a longer transmission distance can be attained.

In this paper we propose a new protocol in which the decoy state scheme is used in the SARG04 protocol with a HSPS. Moreover, we combine the idea of Gottesman, Lo, Lutkenhaus, and Preskill (GLLP)[6] with our protocol to achieve a formula for key generation rate. For the characteristic of the HSPS, a post-selection parameter must be included in the formula.[17] Thus, the secure key generation rate of our protocol is given by

$$R \geq \frac{1}{4} P_{\text{post}}\{-Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_2[1 - H_2(e_2)]\}, \quad (1)$$

where the factor $\frac{1}{4}$ is the sifting efficiency of the SARG04 protocol; $Q_\mu$ and $E_\mu$ are the counting rate and the quantum bit error rate (QBER) of the signal state respectively; $Q_i$ and $e_i$ $(i = 1, 2)$ are the counting rate and the QBER of the $i$-photon state respectively; $f(E_\mu)$ is the bidirectional error correction efficiency;[18] $H_2(x)$ is the binary Shannon information entropy function given by

$$H_2(x) = -x \log_2 x - (1 - x) \log_2 (1 - x). \quad (2)$$

Six key variables are needed in inequality (1). $Q_\mu$ and $E_\mu$ can be measured directly. On the other hand, we discuss how to estimate $Q_i$ and $e_i$ $(i = 1, 2)$ by using the decoy state idea. Firstly we derive a general theory for our protocol with three decoy states. Secondly, we propose a special three-decoy-state protocol — one-vacuum-and-two-weak-decoy-state protocol. Finally, we also discuss a two-decoy-state protocol. Moreover, using the experimental parameters of the experiment of Gobby, Yuan, and Shields (GYS),[19] we show that our protocol can be substantially increase both the transmission distance and the key generation rate.

# 2. Practical decoy method

As analysed in Ref.[15], for practical implementation, only a few decoy states are sufficient for the estimation. In our protocol, we should estimate the lower bounds of $Y_1$ and $Y_2$ and the upper bounds of $e_1$ and $e_2$. Intuitively, only three decoy states are needed for the estimation. Here, we investigate how to use three decoy states to estimate those bounds.

Suppose that Alice randomly changes the intensity of her pump light among 4 values (three decoy states and a signal state) such that the intensity of one mode of the two mode source is randomly changed among $x_1$, $x_2$, $x_3$ and $\mu$, which satisfy

$$0 \leq x_3 < x_2 < x_1 < \mu, \quad \frac{x_3}{1 + x_3} + \frac{x_2}{1 + x_2} < \frac{\mu}{1 + \mu},$$

$$\left(\frac{x_1}{1 + x_1}\right)^2 + \frac{x_1}{1 + x_1}\frac{x_2}{1 + x_2} + \left(\frac{x_2}{1 + x_2}\right)^2 = \left(\frac{\mu}{1 + \mu}\right)^2, \quad (3)$$

where $x_1$, $x_2$ and $x_3$ are the expected photon numbers of the decoy states and $\mu$ is the expected photon number of the signal state.

## 2.1. Three weak decoy states

For convenience, we make $Q'_x = P_{\text{post}} Q_x$. According to Eq.(7) in Ref.[20], the modified counting rates are given by

$$Q'_{x_3} = P_{\text{post}} Q_{x_3} = \frac{d_{\text{A}} Y_0}{1 + x_3} + \sum_{n=1}^{\infty} Y_n [1 - (1 - \eta_{\text{A}})^n] \times \frac{x_3^n}{(1 + x_3)^{n+1}}, \quad (4)$$

$$Q'_{x_2} = P_{\text{post}} Q_{x_2} = \frac{d_{\text{A}} Y_0}{1 + x_2} + \sum_{n=1}^{\infty} Y_n [1 - (1 - \eta_{\text{A}})^n] \times \frac{x_2^n}{(1 + x_2)^{n+1}}, \quad (5)$$

$$Q'_{x_1} = P_{\text{post}} Q_{x_1} = \frac{d_{\text{A}} Y_0}{1 + x_1} + \sum_{n=1}^{\infty} Y_n [1 - (1 - \eta_{\text{A}})^n] \times \frac{x_1^n}{(1 + x_1)^{n+1}}, \quad (6)$$

$$Q'_{\mu} = P_{\text{post}} Q_{\mu} = \frac{d_{\text{A}} Y_0}{1 + \mu} + \sum_{n=1}^{\infty} Y_n [1 - (1 - \eta_{\text{A}})^n] \times \frac{\mu^n}{(1 + \mu)^{n+1}}. \quad (7)$$

First, Alice and Bob can estimate the lower bound of background rate $Y_0$ by

$$
\begin{aligned}
&x_2(1+x_3)Q_{x_3}-x_3(1+x_2)Q_{x_2}\\
=&(x_2-x_3)d_{\rm A}Y_0-\left\{x_3\sum_{n=1}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\left(\frac{x_2}{1+x_2}\right)^n-x_2\sum_{n=1}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\left(\frac{x_3}{1+x_3}\right)^n\right\}\\
\leq&(x_2-x_3)d_{\rm A}Y_0. \qquad (8)
\end{aligned}
$$

Thus, a crude lower bound of $Y_0$ is given by

$$
Y_0\geq Y_0^L=\frac{x_2(1+x_3)Q_{x_3}-x_3(1+x_2)Q_{x_2}}{(x_2-x_3)d_{\rm A}}. \qquad (9)
$$

Then Alice and Bob can estimate the lower bound of $Y_1$ by combining expressions (4), (5)and (8), under the condition, expression (3). We have

$$
\begin{aligned}
&(1+x_2)Q'_{x_2}-(1+x_3)Q'_{x_3}\\
=&Y_1\eta_{\rm A}\left(\frac{x_2}{1+x_2}-\frac{x_3}{1+x_3}\right)+\sum_{n=2}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\left[\left(\frac{x_2}{1+x_2}\right)^n-\left(\frac{x_3}{1+x_3}\right)^n\right]\\
\leq&Y_1\eta_{\rm A}\left(\frac{x_2}{1+x_2}-\frac{x_3}{1+x_3}\right)+\frac{\left(\frac{x_2}{1+x_2}\right)^2-\left(\frac{x_3}{1+x_3}\right)^2}{\left(\frac{\mu}{1+\mu}\right)^2}\left[Q'_{\mu}(1+\mu)-Y_0d_{\rm A}-Y_1\eta_{\rm A}\frac{\mu}{1+\mu}\right]\\
\leq&Y_1\eta_{\rm A}\left[\frac{x_2-x_3}{(1+x_3)(1+x_2)}\right]-\frac{(x_2+x_3+2x_3x_2)(x_2-x_3)(1+\mu)^2}{(1+x_3)^2(1+x_2)^2\mu^2}g\left[Q'_{\mu}(1+\mu)-Y_0^Ld_{\rm A}-Y_1\eta_{\rm A}\frac{\mu}{1+\mu}\right], \qquad (10)
\end{aligned}
$$

where $Y_0^L$ is defined in expression (9). Here, to prove the first inequality in expression(10), we have made use of the inequality, $a^i-b^i\leq a^2-b^2$ when $0<a+b<1$ and $i\geq 2$. The first equality sign holds only if Eve raises the yield of two-photon state and blocks all the states with a photon number greater than 2.

From expression (10), the lower bound of $Y_1$ is given by

$$
\begin{aligned}
Y_1^{x_2,x_3}\geq&\frac{(1+x_1)^2(1+x_2)^2\mu}{(x_2-x_1)[(1-x_1x_2)\mu-(x_1+x_2+2x_1x_2)]\eta_{\rm A}}\Big\{(1+x_2)Q'_{x_2}-(1+x_1)Q'_{x_1}\\
&-\frac{(x_1+x_2+2x_1x_2)(x_2-x_1)(1+\mu)^2}{(1+x_1)^2(1+x_2)^2\mu^2}[Q'_{\mu}(1+\mu)-Y_0^Ld_{\rm A}]\Big\}. \qquad (11)
\end{aligned}
$$

Next, we use expressions (5) and (6) to estimate the lower bound of $Y_2$ with the same method.

$$
\begin{aligned}
&(1+x_1)Q'_{x_1}-(1+x_2)Q'_{x_2}\\
=&Y_1\eta_{\rm A}\left(\frac{x_1}{1+x_1}-\frac{x_2}{1+x_2}\right)+Y_2[1-(1-\eta_{\rm A})^2]\left[\left(\frac{x_1}{1+x_1}\right)^2-\left(\frac{x_2}{1+x_2}\right)^2\right]\\
&+\sum_{n=3}^{\infty}Y_n[1-(1-\eta_{\rm A})^n]\left[\left(\frac{x_1}{1+x_1}\right)^n-\left(\frac{x_2}{1+x_2}\right)^n\right]\\
\leq&Y_1\eta_{\rm A}\left(\frac{x_1}{1+x_1}-\frac{x_2}{1+x_2}\right)+Y_2[1-(1-\eta_{\rm A})^2]\left[\left(\frac{x_1}{1+x_1}\right)^2-\left(\frac{x_2}{1+x_2}\right)^2\right]\\
&+\frac{\left(\frac{x_1}{1+x_1}\right)^3-\left(\frac{x_2}{1+x_2}\right)^3}{\left(\frac{\mu}{1+\mu}\right)^3}\left[Q'_{\mu}(1+\mu)-Y_0d_{\rm A}-Y_1\eta_{\rm A}\frac{\mu}{1+\mu}-Y_2[1-(1-\eta_{\rm A})^2]\left(\frac{\mu}{1+\mu}\right)^2\right]\\
\leq&Y_2[1-(1-\eta_{\rm A})^2]\left[\left(\frac{x_1}{1+x_1}\right)^2-\left(\frac{x_2}{1+x_2}\right)^2\right]\\
&+\frac{\left(\frac{x_1}{1+x_1}\right)^3-\left(\frac{x_2}{1+x_2}\right)^3}{\left(\frac{\mu}{1+\mu}\right)^3}\left[Q'_{\mu}(1+\mu)-Y_{\rm o}^Ld_{\rm A}-Y_2[1-(1-\eta_{\rm A})^2]\left(\frac{\mu}{1+\mu}\right)^2\right]. \qquad (12)
\end{aligned}
$$

In order to prove the first inequality in expression (12), we have made use of the inequality that $a^i - b^i \leq a^3 - b^3$ when $0 < b < a < 1$ and $i \geq 3$. The first equality sign holds only if Eve raises the yield of three-photon state and blocks all the states with a photon number greater than 3. In addition, in order to obtain the last inequality, under the condition, expression (3), we have let $x_1$ and $x_2$ satisfy

$$\frac{x_1}{1+x_1} - \frac{x_2}{1+x_2} - \frac{\left(\frac{x_1}{1+x_1}\right)^3 - \left(\frac{x_2}{1+x_2}\right)^3}{\left(\frac{\mu}{1+\mu}\right)^2} = 0. \quad (13)$$

From expression (12), we can obtain the lower bound of $Y_2$ given by

$$Y_2^{x_1,x_2} \leq \frac{(1+x_1)Q'_{x_1} - (1+x_2)Q'_{x_2} - \frac{\left(\frac{x_1}{1+x_1}\right)^3 - \left(\frac{x_2}{1+x_2}\right)^3}{\left(\frac{\mu}{1+\mu}\right)^3}[Q'_\mu(1+\mu) - Y_0^L d_A]}{\left[\left(\frac{x_1}{1+x_1}\right)^2 - \left(\frac{x_2}{1+x_2}\right)^2 - \frac{\left(\frac{x_1}{1+x_1}\right)^3 - \left(\frac{x_2}{1+x_2}\right)^3}{\left(\frac{\mu}{1+\mu}\right)}\right][1-(1-\eta_A)^2]} g. \quad (14)$$

According to Eq.(9) in Ref.[20], the QBERs of the decoy states are given by

$$E_{x_3}Q_{x_3} = \frac{e_0 Y_0}{1+x_3} + \sum_{n=1}^{\infty} e_{\text{base}}[1-(1-\eta_A)^n]Y_n \frac{x_3^n}{(1+x_3)^{n+1}}, \quad (15)$$

$$E_{x_2}Q_{x_2} = \frac{e_0 Y_0}{1+x_2} + \sum_{n=1}^{\infty} e_{\text{base}}[1-(1-\eta_A)^n]Y_n \frac{x_2^n}{(1+x_2)^{n+1}}, \quad (16)$$

$$E_{x_1}Q_{x_1} = \frac{e_0 Y_0}{1+x_1} + \sum_{n=1}^{\infty} e_{\text{base}}[1-(1-\eta_A)^n]Y_n \frac{x_1^n}{(1+x_1)^{n+1}}. \quad (17)$$

An upper bound of $e_1$ can be obtained from expressions (15) and (16) to be

$$e_1^{x_3,x_2} \leq \frac{(1+x_2)(1+x_3)[(1+x_2)E_{x_2}Q_{x_2} - (1+x_3)E_{x_3}Q_{x_3}]}{Y_1^{x_3,x_2}\eta_A(x_2-x_3)}. \quad (18)$$

And we can have the upper bound of $e_2$ directly from expression (17)

$$e_2^{x_1,x_2} \leq \frac{E_{x_1}Q_{x_1}(1+x_1) - e_0 Y_0}{Y_2^{x_1,x_2}[1-(1-\eta_A)^2]\left(\frac{x_1}{1+x_1}\right)^2}. \quad (19)$$

## 2.2. One vacuum and two weak decoy states

Here, we investigate a special case of three decoy states, i.e. one vacuum and two weak decoy states. Now, the equality sign in expression (9) holds. Thus, when a vacuum decoy state ($x_3 = 0$) is used we can estimate $Y_0$ accurately from expression (9). Moreover, the second inequality in expression (10) is tight. According to expression (11), the lower bound of $Y_1$ is given by

$$Y_1^{0,x_2} \leq \frac{1}{\eta_A(\mu - x_2)}\left\{\frac{(1+x_2)^3\mu}{x_2}Q'_{x_2} - \frac{(1+\mu)^3 x_2}{\mu}Q'_\mu + Y_0 d_A\left[\frac{(1+\mu)^2 x_2}{\mu} - \frac{(1+x_2)^2\mu}{x_2}\right]\right\}. \quad (20)$$

By substituting $Y_0$ for $Y_0^L$ in expression (14), we have the lower bound of two-photon state, $Y_2'^{x_1,x_2}$.

According to expression (18), the upper bound of $e_1$ is given by

$$e_1^{0,x_2} \leq \frac{(1+x_2)^2 E_{x_2}Q_{x_2} - e_0 d_A d_B(1+x_2)}{Y_1^{0,x_2}\eta_A x_2}. \quad (21)$$

By substituting $Y_2'^{x_1,x_2}$ for $Y_2^{x_1,x_2}$ in expression (19), we can obtain the upper bound of $e_2$.

### 2.3. Two weak decoy states

Suppose that Alice and Bob use the one-vacuum-and-two-weak-decoy-state method, but they have not prepared the vacuum state enough to estimate $Y_0$ very well. Thus, the three-decoy-state method is reduced to a two-decoy-state method. We claim this two-decoy-state protocol to be the same as the three-decoy-state protocol, except the exact value of $Y_0$ unknown to us. So, we derive an upper bound of $Y_0$ from expression (16) as

$$Y_0^{x_2} \leq \frac{(1+x_2)E_{x_2}Q_{x_2}}{e_0}. \tag{22}$$

Substituting the above upper bound into expressions (20) and (14), we have the upper bounds of $Y_1$ and $Y_2$

A simple lower bound on $e_1$ can be derived as follows:

$$e_1^{x_2} = \frac{E_{x_2}Q_{x_2}(1+x_2)^2}{Y_1^{x_2}\eta_{\rm A}x_2}. \tag{23}$$

Next, by substituting the upper bound of $Y_2$ of this protocol into expression (19), we can obtain the upper bound of $e_2$.

## 3. Numerical simulation

In practical implementation, we often use the non-degenerate SPDC to produce photon pairs. One photon is generated at such a wavelength that it is convenient to detect, acting as a heralding signal on Alice's side. The other falls into the telecommunication window for optimal propagation along the fibre or on the air, acting as a heralded signal on Bob's side. In general, the heralding photon is adapted to 800 nm, wavelength range and the heralded one is near 1550 nm wavelength range.

For convenience of comparing the result of coherent states, we use the same parameters as those for the coherent state system in our simulation. The key parameters are shown in Table 1, in addition $d_{\rm A} = 5 \times 10^{-8}$[21] and $f(E_\mu) = 1.16$. We use the above formulas and the key experimental parameters to estimate the values of $Q_i$ and $e_i$ $(i = 1, 2)$ and then simulate the final key rate by using expression (1).

**Table 1.** Key parameters in GYS[19].

| $\lambda$/nm | $\alpha/(d_{\rm B}/{\rm km})$ | $e_{\rm base}/\%$ | $d_{\rm B}/10^{-6}$ | $\eta_{\rm B}/\%$ |
|---|---|---|---|---|
| 1550 | 0.21 | 3.3 | 1.7 | 4.5 |

In simulation, the optimal $\mu$ is chosen for each case. But our optimization is different from that in Ref.[22]. The results are shown in Figs.1–3 respectively.

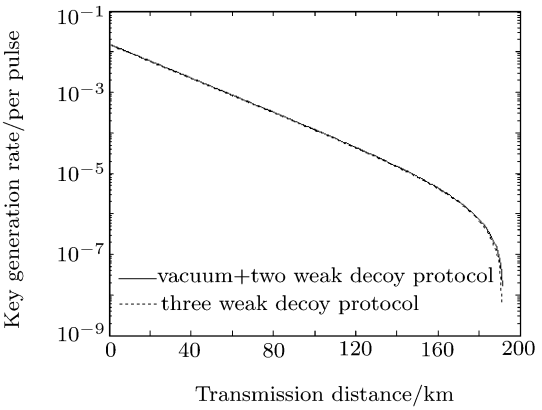



**Fig.1.** Simulation results of three-weak-decoy protocol and one-vacuum-and-two-weak-decoy protocol.

Figure 1 shows the key generation rate over a transmission distance of the general three-decoy-state protocol and the one-vacuum-and-two-weak-decoy protocol with HSPS. From the curves in Fig.1, we learn that the one-vacuum-and-two-weak-decoy protocol performs better than the general three-decoy-state protocol. This proves that decreasing $x_2 + x_3$ can improve the estimations of $Y_1$ and $e_1$. So the smaller the value of $x_2 + x_3$ is, the better performance the protocol will have. Thus, in the next simulation, we consider only the one-vacuum-and-two-weak-decoy protocol.

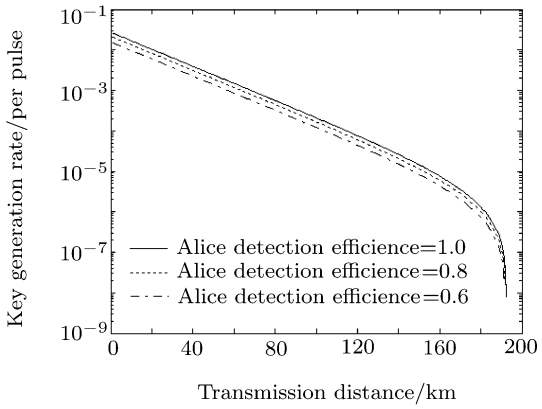



**Fig.2.** A comparison among the final key rates for different detection efficiencies on Alice's side.

From Eq.(5) in Ref.[20], we notice that the counting rate of our protocol is associated with the detection efficiency of Alice's detector, $\eta_{\rm A}$. In other words, the key generation rate and the transmission distance are affected by $\eta_{\rm A}$. In Fig.2, we compare the final key rate with different values of $\eta_{\rm A}$. The results demonstrate

that $\eta_{\rm A}$ changes the key generation rate observably and has a faint influence on the transmission distance.

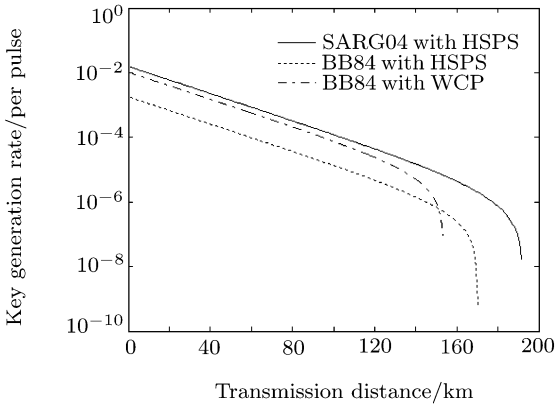



**Fig.3.** A comparison among the final key rates of the decoy method applied separately in the SARG04 with HSPS, the BB84 with HSPS, and BB84 with WCP. $\eta_{\rm A} = 0.6$.

Figure 3 shows the simulations obtained separately by using the decoy state method applied in the SARG04 protocol with HSPS, the decoy state method applied in the BB84 with HSPS, and the BB84 decoy state method with weak coherent pulses (WCP). Owing to the lower dark count of the HSPS than that of the WCP, the protocols with HSPS have a longer transmission distance than those with WCP. However, in Fig.3 the BB84 with HSPS shows a low key generation rate compared with the BB84 with WCP. Because the HSPS is basically a thermal field, it has a higher multi-photon probability than that obtained from the Poissonian distribution with the same expected photon number. But in our protocol, this drawback has been compensated, for we can use the two-photon pulses to generate a key. And our protocol even has a higher key generation rate than the BB84 with WCP.

## 4. Conclusion

Three cases of decoy state QKD protocol with HSPS have been analysed. The first case is the general case which is based on three weak decoy states and one signal state. The second case is the optimal case which is based on one vacuum and two weak decoy states. And the third case is the special case which is based on two decoy states. Our simulation results reveal that the one-vacuum-and-two-weak-decoy-state protocol performs better than the general case. Nonetheless, in practice, it might not be easy to prepare a vacuum state. Therefore, our general theory on nonzero decoy states investigated here is important for practical application.

Using the experimental parameters in the GYS[19] QKD experiment, we have shown that our protocol can be secure over 192 km, which is 45 km longer than that of the BB84 decoy state with WCP and 20 km longer than that of the BB84 decoy state with HSPS. On the other hand, we also study the effect of the detection efficiency of Alice's detector, $\eta_{\rm A}$. The simulation shows that the key generation rate changes more observably with the $\eta_{\rm A}$ than with the transmission distance.

## References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Ekert A K and Huttner B 1996 *J. Mod. Opt.* **41** 2455
[3] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popsescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818
[4] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[5] Lutkenhaus N and Jahma M 2002 *New. J. Phys.* **4** 44
[6] Gottesman D, Lo H K, Lutkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325
[7] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[8] Zeng G H and Zhu H W 2002 *Acta Phys. Sin.* **51** 0727 (in Chinese)
[9] Zhang Q and Zhang E Y 2002 *Acta Phys. Sin.* **51** 1684 (in Chinese)
[10] Bennett C H and Brassard G 1984 *Proceeding of IEEE International Conference on Computers, Systems and Signal Processing* (New York: IEEE) p175
[11] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[12] Wang X B 2005 *Phys. Rev.* A **72** 012322
[13] Wang X B 2005 *Phys. Rev. Lett.* **74** 230503
[14] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[15] Ma X, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[16] Harrington J W, Ettinger J M, Hughes R J and Nordholt J E 2005 http://arxiv.org/abs/quant-ph/0503002
[17] Lutkenhaus N 2000 *Phys. Rev.* A **61** 052304
[18] Brassard G and Slvail L 1994 *in advances in Cryptology—EUROCRYPT'93* (Berlin: Springer-Verlag) **765** 410
[19] Gobby C, Yuan Z L and Shields A L 2004 *Appl. Phys. Lett.***84** 3762
[20] Mi J L, Wang F Q, Lin Q Q, Liang R S and Liu S H 2008 *Acta Phys. Sin.* **57** (in Chinese)
[21] Townsend P D 1998 *IEEE Photonics Technol. Lett.* **10** 1048
[22] Zhao F, Lu Y Q, Fu M X and Liu S H 2007 *Chin. Phys.* **16** 3402