A universal quantum key distribution method*

ZHANG He-qing (张合庆)[1], **ZHOU Yuan-yuan** (周媛媛)[2]**, **ZHOU Xue-jun** (周学军)[2], **and TIAN Pei-gen** (田培根)[2]

1. School of Electronic and Information Engineering, Beihang University, Beijing 100191, China

2. Electronic Engineering College, Naval University of Engineering, Wuhan 430033, China

(Received 19 March 2013)

Combining heralded pair coherent state (HPCS) with passive decoy-state idea, a new method is presented for quantum key distribution (QKD). The weak coherent source (WCS) and heralded single photon source (HSPS) are the most common photon sources for state-of-the-art QKD. However, there is a prominent crossover between the maximum secure distance and the secure key generation rate if these two sources are applied in a practical decoy-state QKD. The method in this paper does not prepare decoy states actively. Therefore, it uses the same experimental setup as the conventional protocol, and there is no need for a hardware change, so its implementation is very easy. Furthermore, the method can obtain a longer secure transmission distance, and its key generation rate is higher than that of the passive decoy-state method with WCS or HSPS in the whole secure transmission distance. Thus, the limitation of the mentioned photo sources for QKD is broken through. So the method is universal in performance and implementation.

Document code: A **Article ID:** 1673-1905(2013)05-0389-4

DOI 10.1007/s11801-013-3053-z

In state-of-the-art quantum cryptographical application, it has become the most efficient and prominent method[1-18] to bring decoy states[19] and different kinds of photon sources together for better performance and easier implementation. The weak coherent source (WCS) and heralded single photon source (HSPS) are the most common photon sources for the real-life quantum key distribution (QKD)[20] system. However, if these two sources are applied in a practical decoy-state QKD, there is a crossover between the maximum secure distance and the secure key generation rate in short and middle distance (crossover distance). Within the crossover distance, the key generation rate of HSPS QKD is less than that of WCS QKD. But the result is opposite to the former when the distance is longer than the crossover distance. That is to say, to optimize the final perfromance, the photon source should be WCS within the threshold distance, but should be HSPS if the distance is out of the threshold. Due to different mechanics in state preparation, it is not easy to change the source frequently from WCS to HSPS. In order to get optimal secure key generation rate for each transmission distance, Ref.[10] used a heralded pair coherent state (HPCS) photon source in decoy-state QKD, and obtained a good result.

The above decoy-state methods with HPCS are all active decoy-state methods, in which Alice needs to actively prepare decoy states through adding attenuators or photon sources. So these methods are not easy to be implemented, and may introduce side information which would be used by Eve. We present a new method combining HPCS with passive decoy-state idea. This method can not only overcome the shortcomings of active decoy-state methods, but also obtain better performance than the existing passive decoy-state methods with WCS or HSPS.

The pair coherent state (PCS) is a two-mode correlated coherent state, and can be written as

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

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

It is a deficiency for PCS applied to QKD system that PCS can generate large numbers of vacuum states. Fortunately, the proportion of vacuum states to the overall photon states can be lessened with the technique of heralding the photon numbers. HPCS is that one mode goes to the encoding module of Alice as a signal mode, and the other mode is sent to the detector of Alice as the triggering mode to forecast the photon number and the arrival time of signal mode, which can weaken the influence of dark count on long-distance QKD.

We define the yield Y_n to be the probability of Bob getting a detection event conditioned on Alice sending an n-photon state.

* This work has been supported by the National High Technology Research and Development Program of China (No.2011AA7014061).

** E-mail: zyy_hjgc@aliyun.com

$$Y_n=1-(1-d_B)(1-\eta)^n, \tag{2}$$

where d_B is the dark count rate of Bob's detection system, and η is the overall transmission between Alice and Bob.

$$\eta = t_{AB}\eta_B, \tag{3}$$

$$t_{AB} = 10^{-\alpha l/10}, \tag{4}$$

where t_{AB} is the transmittance between Alice and Bob, η_B is the transmittance in Bob's side, α is the attenuation coefficient of optical fiber, and l is the transmission distance.

The error rate of the n-photon state is given by

$$e_nY_n= e_dY_n + (e_0-e_d)\, d_B, \tag{5}$$

where e_0=0.5 is the error rate of the background, and e_d is the probability of the survived photon hiting a wrong detector.

Alice only generates a signal state with the intensity of u in our method. According to triggering situation of the Alice's detector, the receiver's detection events are divided into two groups of triggered component and nontriggered component. The triggered and nontriggered components are used as signal state and decoy state, respectively. In our method, there is no strict definition of decoy and signal states, because the nontriggered components not only detect the Eve's presence but also have positive contribution to the final key generation. Here, we are interested in the case that Alice and Bob use threshold detectors.

We define G_n as 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, triggered by Alice of $G_n^{(t)}$ and the rest of $G_n^{(nt)}$, which can be expressed as

$$G_n^{(t)} = Y_n\left[1-(1-\eta_A)^n + d_A\right]\frac{1}{I_0(2u)}\frac{u^{2n}}{(n!)^2}, \tag{6}$$

$$G_n^{(nt)} = Y_n\left[(1-\eta_A)^n - d_A\right]\frac{1}{I_0(2u)}\frac{u^{2n}}{(n!)^2}, \tag{7}$$

where η_A is the detecting efficiency at Alice's side, and d_A is the dark count rate of Alice's detector.

Then we define Q as the overall rate. Q can also be divided into two groups of $Q^{(t)}$ and $Q^{(nt)}$, which can be expressed as

$$Q^{(t)} = \frac{Y_0 d_A}{I_0(2u)} + \sum_{n=1}^{\infty} G_n^{(t)}, \tag{8}$$

$$Q^{(nt)} = \frac{Y_0(1-d_A)}{I_0(2u)} + \sum_{n=1}^{\infty} G_n^{(t)}. \tag{9}$$

Similar to Eqs.(8) and (9), the quantum bit error rates (QBERs) are given by

$$E^{(t)}Q^{(t)} = \frac{Y_0 e_0 d_A}{I_0(2u)} + \sum_{n=1}^{\infty} G_n^{(t)} e_n, \tag{10}$$

$$E^{(nt)}Q^{(nt)} = \frac{Y_0 e_0(1-d_A)}{I_0(2u)} + \sum_{n=1}^{\infty} G_n^{(nt)} e_n. \tag{11}$$

All the measured data can be grouped according to Alice's detection events, so we can apply Gottesman-Lo-Lütkenhaus-Preskill (GLLP)[21] idea to each group. The final key generation rate can be given by summing the contributions from both the groups, i.e., $R^{(\text{both})} = R^{(t)} + R^{(nt)}$. $R^{(t)}$ and $R^{(nt)}$ can be expressed as

$$R^{(t)} \geq \max\left(q\left\{-Q^{(t)}f\left(E^{(t)}\right)H_2\left(E^{(t)}\right) + G_0^{(t)} + G_1^{(t)}\left[1-H_2(e_1)\right]\right\}, 0\right), \tag{12}$$

$$R^{(nt)} \geq \max\left(q\left\{-Q^{(nt)}f\left(E^{(nt)}\right)H_2\left(E^{(nt)}\right) + G_0^{(nt)} + G_1^{(nt)}\left[1-H_2(e_1)\right]\right\}, 0\right), \tag{13}$$

where q is the basis reconciliation factor, and the q for the 1984 protocol of Bennett and Brassard (BB84 protocol) is 1/2. $f(x)$ is the bidirectional error correction efficiency. $H_2(x)$ is the binary Shannon information entropy function given by $H_2(x)= -x\log_2(x)-(1-x)\log_2(1-x)$. $Q^{(t)}$, $Q^{(nt)}$, $E^{(t)}$ and $E^{(nt)}$ can be observed in the experiment.

If the difference between the estimated result and the theoretical secure threshold is too big, this quantum communication may be eavesdropped by Eve, and must be abandoned. The new quantum key distribution should be implemented. If the estimated result is secure, the secure key can be distilled according to Eqs.(12) and (13).

Firstly, the upper bound of Y_0 is deduced, which is a preparation for the estimations of Y_1 and e_1.

$$E^{(t)}Q^{(t)} > \frac{Y_0 e_0 d_A}{I_0(2u)}, \tag{14}$$

$$E^{(nt)}Q^{(nt)} > \frac{Y_0 e_0(1-d_A)}{I_0(2u)}. \tag{15}$$

Thus, a simple bound of Y_0 is given by

$$Y_0 \leq Y_0^U = \min\left\{\frac{E^{(t)}Q^{(t)}I_0(2u)}{e_0 d_A}, \frac{E^{(nt)}Q^{(nt)}I_0(2u)}{e_0(1-d_A)}\right\}. \tag{16}$$

In the next step, we use the triggered events ($Q^{(t)}$) and the nontriggered events ($Q^{(nt)}$) to deduce a tight lower bound of Y_1. Eqs.(8) and (9) lead to

$$\begin{aligned} &I_0(2u)\left[1-(1-\eta_A)^2\right]Q^{(nt)} - I_0(2u)(1-\eta_A)^2 Q^{(t)} = \\ &Y_0\left[1-(1-\eta_A)^2 - d_A\right] + Y_1 u^2\eta_A(1-\eta_A) + \\ &\sum_{n=3}^{\infty} Y_n \frac{u^{2n}}{(n!)^2}\left\{(1-\eta_A)^n\left[1-(1-\eta_A)^2\right] - \right. \\ &\left.(1-\eta_A)^2\left[1-(1-\eta_A)^n\right]\right\}. \end{aligned} \tag{17}$$

Because $(1-\eta_A)^n - (1-\eta_A)^2 \leq 0$ ($n \geq 3$), we can obtain the lower bound of Y_1.

$$Y_1 \geq Y_1^L = \frac{I_0(2u)\left[1-(1-\eta_A)^2\right]Q^{(nt)}}{u^2\eta_A(1-\eta_A)} - \frac{I_0(2u)(1-\eta_A)^2 Q^{(t)} + Y_0\left[1-(1-\eta_A)^2 - d_A\right]}{u^2\eta_A(1-\eta_A)} \quad . \quad (18)$$

According to Eqs.(10) and (11), the following inequations can be given

$$E^{(t)}Q^{(t)} \geq \frac{Y_0 e_0 d_A}{I_0(2u)} + \frac{Y_1\eta_A e_1 u^2}{I_0(2u)}, \quad (19)$$

$$E^{(nt)}Q^{(nt)} \geq \frac{Y_0 e_0 (1-d_A)}{I_0(2u)} + \frac{Y_1(1-\eta_A)e_1 u^2}{I_0(2u)} . \quad (20)$$

And an upper bound of e_1 can be obtained as

$$e_1 \leq e_1^U = \min\left\{\frac{E^{(t)}Q^{(t)}I_0(2u) - Y_0 e_0 d_A}{Y_1\eta_A u^2}, \frac{E^{(nt)}Q^{(nt)}I_0(2u) - Y_0 e_0(1-d_A)}{Y_1(1-\eta_A)u^2}\right\} . \quad (21)$$

Now, by substituting the bounds of Y_1 and e_1 into Eqs.(12) and (13), the final key rate can be calculated. We use the parameters mainly from Gobby-Yuan-Shields (GYS) experiment[22]. At Alice's side, d_A =10^{-6} and η_A=0.6; at Bob's side, d_B = 1.7×10^{-6}, η_B =0.045, e_d =0.033 and f= 1.22. In simulation, the optimal u is chosen at each distance for each case.

Fig.1 shows that there is a crossover in 135 km between the two passive decoy-state performance curves of WCS QKD and HSPS QKD. The key generation rate of WCS QKD is higher than that of HSPS QKD at a distance less than the crossover distance. On the contrary, the key generation rate of HSPS QKD is higher than that of WCS QKD when the transmission distance is out of the crossover distance. Now, the passive decoy-state method with HPCS in this paper can obtain the highest key generation rate and the longest transmission distance compared with the former methods.

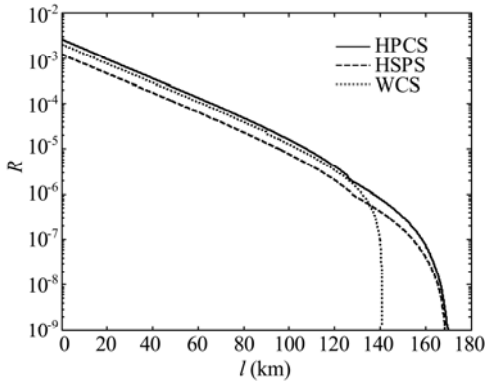

Fig.1 The performance of BB84 passive decoy-state methods with different sources

As shown in Fig.2, there is an inflexion at the distance about 154 km in the performance curve of the passive decoy-state method with HPCS. Because of the contribution of nontriggered components to key generation, the key generation rate of our passive decoy-state method is obviously higher than that of the active decoy-state method at a distance less than the inflexion distance. However, the function of nontriggered components is lessened out of the inflexion distance. Now, we analyze the reason of the phenomenon. The function of Alice's detector is to detect the vacuum states, so Bob avoids detecting a vacuum state as an i-photon state (i≠0). Because the real-life detector is not perfect, it is possible for Alice's detector to detect an i-photon state (i≠0) as a vacuum state. Here, Bob's detector will stop working in active decoy-state method, namely, the i-photon states (i≠0) are misdeemed and 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 nontriggered detection events are not discarded, but are used to estimate the parameters and generate the secure key. However, only the single-photon states detected as vacuum states by Alice's detector can contribute to key generation. For the high loss channel, the transmission diatance of this part photon states is not too large. Hence, the nontriggered detection events can give a further improvement of the key generation rate at a close range.

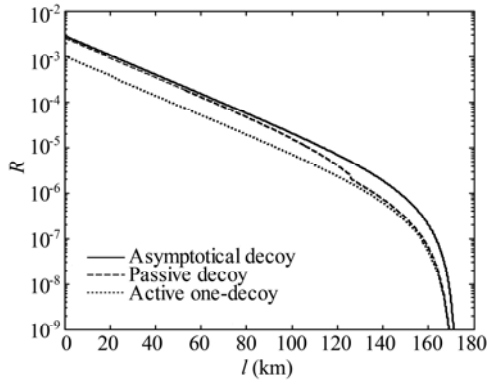

Fig.2 The performance of different BB84 decoy-state methods with HPCS

At the same time, Fig.2 shows that the performance of the passive decoy-state method with HPCS is very close to the theoretical limit of an infinite active decoy-state method with HPCS within the inflexion distance, and is slightly lower than the theoretical limit. The reason is that Alice doesn't prepare decoy states actively, so the estimations of parameters are not very accurate compared with those of the infinite active decoy-state method. Actually, the infinite decoy-state method can not be implemented. The active decoy-state method with finite decoy states has the performance close to theoretical limit, but its shortcomings are difficult implementation, low transmission rate and introduction of side information. However, the passive decoy-state method does not

need to prepare decoy states actively. Thus, it is easy to implement, avoids side information, and can be applied to QKD at high transmission rate.

In summary, a new method is presented for QKD combining HPCS with passive decoy-state idea, which has two advantages. Firstly, our method overcomes the limitations of the methods with WCS or HSPS, and has better performance than the existing passive decoy-state methods. So it is universal in performance. Secondly, the method does not prepare decoy states actively. Therefore, it may use the same experimental setup as the conventional protocol, there is no need for a hardware change, and it can be applied to QKD at high transmission rate. So the method is universal in implementation. Altogether, the passive decoy-state method presented in this paper is universal, simple and feasible for QKD.

References

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

[2] Ma X. F., Qi B., Zhao Y. and Lo H. K., Phys. Rev. A **72**, 012326 (2005).

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

[4] Sun S. H., Gao M., Dai H. Y., Chen P. X. and Li C. Z., Chin. Phys. Lett. **25**, 2358 (2008).

[5] Wang Q., Chen W., Xavier G., Swillo M., Zhang T., Sauge S., Tengner M., Han Z. F., Guo G. C. and Karlsson A., Phys. Rev. Lett. **100**, 090501 (2008).

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

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

[8] Mi J. L., Wang F. Q., Lin Q. Q., Liang R. S. and Liu S. H., Chin. Phys. B **17**, 1178 (2008). (in Chinese)

[9] Scarani V., Bechmann-Pasquinucci H., Cerf N. J., Dušek M., Lütkenhaus N. and Peev M., Rev. of Modern Phys. **81**, 1301 (2009).

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

[11] Yang J., Xu B. J., Peng X. and Guo H., Phys. Rev. A **85**, 052302 (2012).

[12] Mauerer W. and Silberhorn C., Phys. Rev. A **75**, 050305 (2007).

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

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

[15] Zhou Y. Y., Zhou X. J. and Gao J., Optoelectron. Lett. **6**, 396 (2010).

[16] Zhou Y. Y. and Zhou X. J., Optoelectron. Lett. **7**, 389 (2011).

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

[18] Zhou Y. Y., Zhou X. J., Tian P. G. and Wang Y. J., Chin. Phys. B **22**, 010305 (2013).

[19] Hwang W. Y., Phys. Rev. Lett. **91**, 057901 (2003).

[20] Bennett C. H. and Brassard G., Quantum Cryptography: Public Key Distribution and Coin Tossing, IEEE International Conference on Computer, Systems and Signals Processing, 175 (1984).

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

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