A practical two-way system of quantum key distribution with untrusted source*

Chen Ming-Juan(陈明娟) and Liu Xiang(刘 翔)†

Key Laboratory of Low-Dimensional Quantum Structures and Quantum Control of Ministry of Education, and Department of Physics, Hunan Normal University, Changsha 410081, *China*

(Received 5 November 2010; revised manuscript received 17 April 2011)

The most severe problem of a two-way "*plug-and-play*" (p & p) quantum key distribution system is that the source can be controlled by the eavesdropper. This kind of source is defined as an "untrusted source". This paper discusses the effects of the fluctuation of internal transmittance on the final key generation rate and the transmission distance. The security of the standard BB84 protocol, one-decoy state protocol, and weak+vacuum decoy state protocol, with untrusted sources and the fluctuation of internal transmittance are studied. It is shown that the one-decoy state is sensitive to the statistical fluctuation but weak+vacuum decoy state is only slightly affected by the fluctuation. It is also shown that both the maximum secure transmission distance and final key generation rate are reduced when Alice's laboratory transmittance fluctuation is considered.

Keywords: statistic fluctuation, untrusted source, quantum key distribution

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/20/10/100305

1. Introduction

Quantum key distribution (QKD) involves secure communication between authorized partners, whose security is determined by the laws of quantum mechanics.[1−4] There is currently significant interest in the two-way "*plug-and-play*" (p & p) QKD system, in which the birefringence is compensated for automatically.[5−11] However, the scheme has a severe problem, namely, the sources can be completely controlled by the eavesdropper (Eve) before entering Alice's laboratory. This is known as Trojan-horse attacks[9] and such a source is defined as an "untrusted source".[12,13] Therefore, much effort has been devoted to proposing and demonstrating the stability of the p & p QKD system with an untrusted source.[13−15] The numerical simulation results of the untrusted source given by Zhao *et al.*[13] show that unconditional security can be achieved by the p & p QKD system; however, they did not consider the fluctuation of transmittance for Alice's devices on the key generation rate and the transmission distance. Since imperfect devices in QKD may give rise to a potential loophole on the final key[16] in practice, the security is not only based on the principles of quantum mechanics but also the imperfections of the devices.

In this paper, we focus on the effects of the fluctuation of internal transmittance on the final key generation rate and the transmission distance in p & p QKD systems with an untrusted source. The security of the standard BB84 protocol, one-decoy state protocol and weak+vacuum decoy state protocol, with untrusted sources affected by the fluctuation of internal transmittance are studied.

2. Effects of the fluctuation of transmittance on the QKD with an untrusted source

Firstly, we review briefly a general system which has been applied in some necessary measurement to ensure the security of the QKD system,[9] as shown in Fig. 1. The actual source is inside Bob's local laboratory and a strong laser pulse travels on the quantum channel from Bob to Alice. Then, Alice attenuates this pulse to a suitably weak intensity, codes the information and sends the remaining pulse back to Bob who detects the information. The total losses of the Alice internal laboratory are modeled as a $\lambda/(1-\lambda)$ beam splitter,[13] where λ is the internal transmittance of Alice's local laboratory. Usually, Alice cannot set

*Project supported by the National Natural Science Foundation of China (Grant No. 11074072).

†Corresponding author. E-mail: Liuxiang64@medmail.com.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

an accurate value of λ in practice. Therefore, Alice's apparatus transmittance fluctuation should be considered in the experiments. That is, the photons inputted to the system have a probability of λ ($\lambda \in [(1-\sigma)\lambda_{\rm o}, (1+\sigma)\lambda_{\rm o}]$) to be encoded, and $1-\lambda$ to be discarded, where $\lambda_{\rm o}$ is the optimal transmittance, and σ is the fluctuation of the transmittance. The interferometers will become self-stabilized since the light passes twice between them. Eve's Trojan-horse attacks at the position 1, which would assist her photon-number splitting (PNS) to attack at the position 2 (see Fig. 1). To enhance the security of the system, Alice uses a strong filter to filter out a part of the legitimate signal and uses active phase randomization to achieve phase randomization. The phase randomization separates Alice from any possible reference system that Eve may have prepared in advance. 50% of the pulses can be chosen freely by optical switch and sent to the beam splitter and the other 50% would be sent to the intensity monitor. The latter is used to test the number of photons.

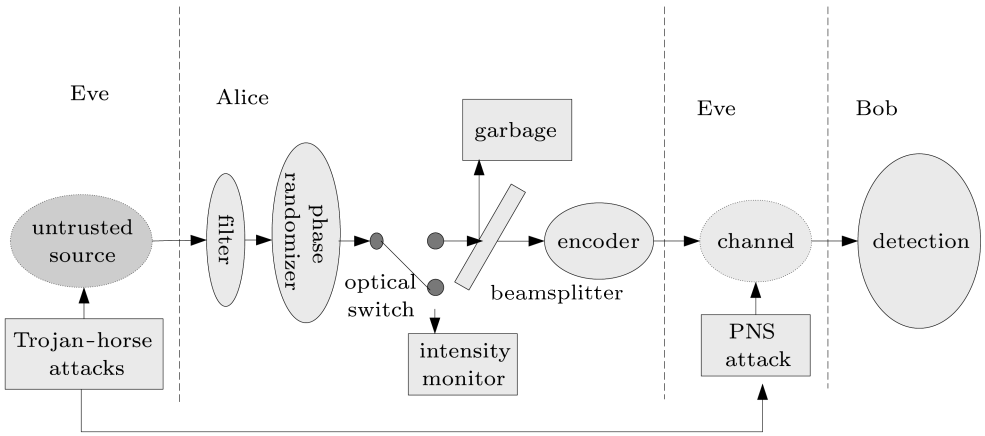


Fig. 1. Schematic diagram of the experiment.

The effects of the fluctuation of internal transmittance λ ($\lambda \in [(1-\sigma)\lambda_{\rm o}, (1+\sigma)\lambda_{\rm o}]$) on the QKD key generation rate are studied. The pulse passing through Alice's laboratory has a probability of $N\lambda$ to be encoded, and $N(1-\lambda)$ to be discarded, where N is the average photon number of the inputted pulse. In a practical QKD system with imperfect sources, there are two kinds of qubit that should be discussed separately: one is the tagged bit which is not secure, the other is the untagged bit which is secure and can be used to distill the final key.[10] In the following study, we will focus on these untagged bits m ($m \in [(1-\delta)N, (1+\delta)N]$), where δ is the fluctuation of the source caused by the control of Eve. The overall gain $Q_{\rm e}$ and the overall qubit error rate (QBER) $E_{\rm e}$ can be measured experimentally. Though the gain Q and the QBER E of the untagged bits cannot be measured directly, the upper and lower bounds of Q and E can be estimated.[13] The upper and lower bounds of Q are given respectively by

$$\overline{Q} = \frac{Q_{\rm e}}{1-\Delta-\varepsilon}, \quad \underline{Q} = \max\left(0, \quad \frac{Q_{\rm e}-\Delta-\varepsilon}{1-\Delta-\varepsilon}\right), \quad (1)$$

and the upper and lower bounds of E can be obtained, respectively as

$$\overline{E} = \frac{Q_{\rm e}E_{\rm e}}{1-\Delta-\varepsilon}, \quad \underline{E} = \max\left(0, \frac{Q_{\rm e}E_{\rm e}-\Delta-\varepsilon}{1-\Delta-\varepsilon}\right). \quad (2)$$

In order to obtain tighter bounds on Q and E, $\Delta = 1-\mathrm{erf}(\sqrt{N\delta/2})$ should be made as small as possible. For simplicity, we only consider the asymptotic case in the following studies, that is, the ε can be considered to tend to 0. Considering m ($m \in [(1-\delta)N, (1+\delta)N]$) photons entering Alice's laboratory, we find that the conditional probability n photons emitted by Alice's laboratory obeys a binomial distribution given by[13]

$$p_n(m) = C_m^n \lambda^n (1-\lambda)^{m-n}. \quad (3)$$

When the statistical fluctuation of the internal transmittance is taken into account, that is, λ ($\lambda \in [(1-\sigma)\lambda_{\rm o}, (1+\sigma)\lambda_{\rm o}]$), the upper and lower bounds of $p_n(m)$ for untrusted source can be obtained respectively as follows:

$$\overline{p}_n = \begin{cases} [1-(1-\sigma)\lambda]^{(1-\delta)N}, & \text{if } n=0, \\ C^n_{(1+\delta)N}[(1+\sigma)\lambda]^n[1-(1+\sigma)\lambda]^{(1+\delta)N-n}, & \text{if } n \le (1+\delta)N, \\ 0, & \text{if } n \ge (1+\delta)N; \end{cases} \tag{4}$$

$$\underline{p}_n = \begin{cases} [1-(1+\sigma)\lambda]^{(1+\delta)N}, & \text{if } n=0, \\ C^n_{(1-\delta)N}[(1-\sigma)\lambda]^n[1-(1-\sigma)\lambda]^{(1-\delta)N-n}, & \text{if } n \le (1+\delta)N, \\ 0, & \text{if } n \ge (1-\delta)N. \end{cases} \tag{5}$$

Under the condition $\lambda_o(1+\sigma)N(1+\delta) < 1$, the expected outputted photon number of any untagged bits should be lower than 1. In order to obtain tighter bounds on $p_n(m)$, we need to obtain δ and σ as small as possible. Reducing δ and σ would narrow the bound of the untagged bits, however, which would widen the bound of Q and E. Therefore, we need to achieve a balance between the tightness of the bounds of $p_n(m)$ and that of the bounds of Q and E. The optimal choice of δ and σ depends on the practical system and can be calculated by numerical simulation.

We can implement the above analysis into some QKD proposals and study the effects of δ and σ on the maximum transmission distance and the key generation rate for the cases of the Gottesman *et al* (GLLP)[1] without-decoy method, the one-decoy proposal, and the weak+vaccum proposal, respectively.

Case I We consider the effects of the transmittance fluctuation on the results of GLLP without-decoy method. The secure key generation rate of a standard BB84 protocol[17] with untrusted sources is given as[13]

$$R \ge 0.5\Big\{ -Q_e f(E_e) H_2(E_2) + (\underline{Q}_e + \underline{p}_0 + \overline{p}_1 - 1) \times \left[1 - H_2\left(\frac{Q_e E_e}{Q_e + \underline{p}_0 + \overline{p}_1 - 1}\right)\right]\Big\}, \tag{6}$$

where $f(E_e)$ is the bidirectional error correction inefficiency. In experiments, $f(E_e) = 1.22$ is usually used. The $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy. The gain Q_e and the qubit error rate E_e of the signals based on the BB84 protocol can be obtained as follows:[18]

$$Q_e = Y_0 + 1 - \exp(-\eta\eta_{Bob}N\lambda), \tag{7}$$

$$E_e = \frac{0.5Y_0 + e_{dec}[1-\exp(-\eta\eta_{Bob}N\lambda)]}{Q_e}, \tag{8}$$

where $\eta = 10^{-\alpha l/10}$ is the channel transmittance, α is the fibre attenuation, l is the distance between Alice and Bob, η_{Bob} is the detection efficiency of Bob's setup, Y_0 is the background rate and e_{dec} is the probability that a photon will hit the erroneous detector. In our numerical simulations, the parameters used are as follows: $\alpha = 0.2$, $Y_0 = 1.7 \times 10^{-6}$, $\eta_{Bob} = 0.45$, $e_{dec} = 0.33$, reported by Gobby, Yuan and Shieldds (GYS).[19]

Substituting Eqs. (4) and (5) into Eq. (6), one can obtain the key generation rate in the GLLP without-decoy method easily. The simulation results with $\delta = 0.01$ are shown in Fig. 2(a). It can be seen that the three cases provide almost the same final key generation rate and maximum transmission distance, the latter being around 40 km. Observing the subtle details of the figure, we show that neglecting the internal transmittance fluctuation has a slight advantage in gain compared with the cases of $\sigma = 0.05$ and $\sigma = 0.1$. That is, the effect of the fluctuation of $\sigma = 0.1$ on the key generation rate is weak for the GLLP protocol without-decoy method. Furthermore, the optimal λ_o of the maximum transmission distance are 2.6×10^{-9}, 2.9×10^{-9}, and 3.1×10^{-9} for the cases with $\sigma = 0$, $\sigma = 0.05$, and $\sigma = 0.1$, respectively.

Case II We consider the effect of the transmittance fluctuation on the results of the one-decoy method. The decoy state idea was first proposed by Hwang *et al.*,[20] which allows the users to place a rigorous lower bound on the single-photon channel transmittance, including the receiver's losses. It is now known that the decoy state scheme is efficient in fighting against the PNS attack. In the protocol,[21–23] Bob emits a signal state with an average photon number of μ and a decoy state with an average photon number of ν ($\nu < \mu$). The decoy state is used for the purpose of detecting eavesdropping attacks only, whereas the standard BB84 state is used for key generation. Considering the fluctuation of the transmittance, we find that Alice's signal state transmittance is $\lambda_s \in ((1-\sigma)\lambda_{os}, (1+\sigma)\lambda_{os})$, where λ_{os} is the optimal transmittance, and the transmittance of the decoy state is $\lambda_d \in ((1-\sigma)\lambda_{od}, (1+\sigma)\lambda_{od})$, for which $\lambda_{os} > \lambda_{od}$ is required.[13] The key generation rate in standard BB84 protocol is given by[13]

$$R \geq 0.5\{-Q_{\rm e}^{\rm s} f(E_{\rm e}^{\rm s}) H_2(E_{\rm e}^{\rm s}) + (1-\Delta-\varepsilon)\underline{Q}_1^{\rm s}[1-H_2(\overline{e}_1^{\rm s})]\}. \tag{9}$$

The lower bound of $Q_1^{\rm s}$ and upper bound of $e_1^{\rm s}$ for the untrusted source can be obtained respectively as[13]

$$\underline{Q}_1^{\rm s} = \underline{p}_1^{\rm s}\frac{\underline{Q}^{\rm d}\underline{p}_2^{\rm s} - \overline{Q}^{\rm s}\overline{p}_2^{\rm d} + (\underline{p}_0^{\rm s}\overline{p}_2^{\rm d} - \overline{p}_0^{\rm d}\underline{p}_2^{\rm s})\overline{E}^{\rm s}/p_0^{\rm s}E^{\rm v} - [2N\delta(1-\lambda_D)^{2N\delta-1}\underline{P}_2^{\rm s}]/[(1-\delta)N+1]!}{\overline{p}_1^{\rm d}\underline{p}_2^{\rm s} - \underline{p}_1^{\rm s}\overline{p}_2^{\rm d}}, \tag{10}$$

$$\overline{e}_1^{\rm s} = \frac{\overline{E}^{\rm s}}{\underline{Q}_1^{\rm s}}. \tag{11}$$

Substituting Eqs. (4), (5), (10), and (11) into inequality (9), one can obtain the key generation rate of the one-decoy protocol. The results of the key generation rate are presented in Fig. 2(b), in which the transmittance fluctuations are set as $\sigma = 0, \sigma = 0.02$, and $\sigma = 0.03$, respectively. It can be seen that the one-decoy protocol is very sensitive to transmittance fluctuation. There is no way to generate a secure final key for the one-decoy protocol since the σ is greater than 0.04. The maximum transmission distance of the one-decoy without transmittance fluctuation σ is obviously greater than that of the one-decoy protocol with transmittance fluctuation. The maximum transmission distance can reach 114 km for an untrusted source without transmittance fluctuation. However, the maximum transmission distance is reduced to 82 km with $\sigma = 0.02$ and 15 km with $\sigma = 0.03$, respectively. The optimal $\lambda_{\rm os}$ and $\lambda_{\rm od}$ of the maximum transmission distance are 1.8×10^{-7} and 1.1×10^{-7} for the case without the transmittance fluctuation, and 1.9×10^{-7} and 1.2×10^{-7} for the case with $\sigma = 0.02$ and $\sigma = 0.03$.

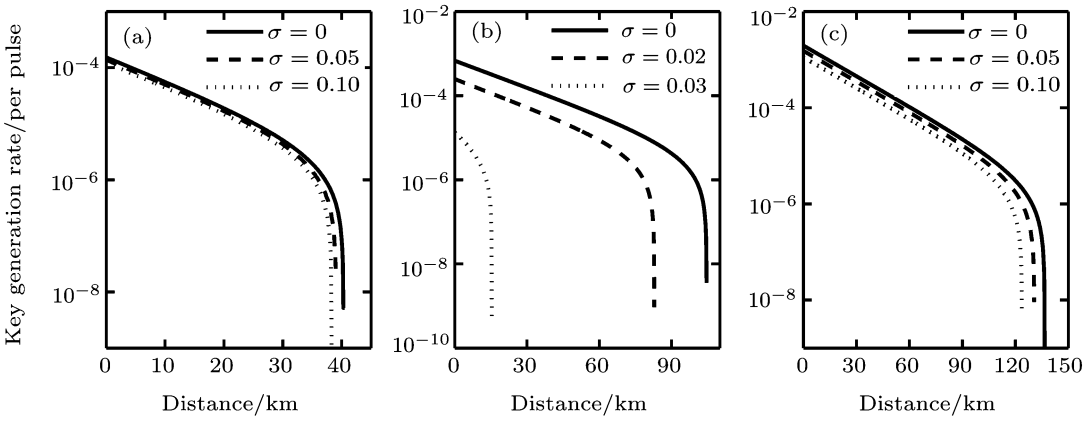


Fig. 2. Simulation results for (a) the GLLP protocol without-decoy method, (b) the one-decoy protocol, and (c) the weak+vacuum protocol with different values of Alice's internal transmittance fluctuation σ, and source fluctuation $\delta = 0.01$.

Case III We consider the effect of the transmittance fluctuation on the results of the weak+vacuum protocol.[24–27] The weak+vacuum protocol was first presented in Wang's 3-intensity decoy-state,[24] in which one can use three randomly different intensities (average photon numbers) for each pulse ($\mu^{\rm s}$, $\mu^{\rm d}$, ν). The signal state is used to generate the final key, the decoy state is used to test the channel property, and the vacuum state is used to detect the background count rate. Considering the fluctuation of Alice's internal transmittance, the signal state transmittance in Alice's laboratory can be written as $\lambda_{\rm s} \in ((1-\sigma)\lambda_{\rm os}, (1+\sigma)\lambda_{\rm os})$, where $\lambda_{\rm os}$ is the optimal transmittance value for the signal state. The transmittance of the weak decoy state in Alice's laboratory is $\lambda_{\rm d} \in ((1-\sigma)\lambda_{\rm od}, (1+\sigma)\lambda_{\rm od})$, and the vacuum state's transmittance is 0, where $\lambda_{\rm od}$ is the optimal transmittance value for the weak decoy state; also, $\lambda_{\rm os} > \lambda_{\rm od}$ is required.

The lower bound of $Q_1^{\rm s}$ and upper bound of $e_1^{\rm s}$ for the untagged bits are given by[13]

$$\underline{Q}_1^{\rm s} = \underline{p}_1^{\rm s}\frac{\underline{Q}^{\rm d}\underline{p}_2^{\rm s} - \overline{Q}^{\rm s}\overline{p}_2^{\rm d} + (\underline{p}_0^{\rm s}\overline{p}_2^{\rm d} - \overline{p}_0^{\rm d}\underline{p}_2^{\rm s})\overline{Q}^{\rm v} - [2N\delta(1-\lambda_D)^{2N\delta-1}\underline{P}_2^{\rm s}]/[(1-\delta)N+1]!}{\overline{p}_1^{\rm d}\underline{p}_2^{\rm s} - \underline{p}_1^{\rm s}\overline{p}_2^{\rm d}}, \tag{12}$$

$$\overline{e}_1^{\rm s} = \frac{\overline{E}^{\rm s} - \underline{P}_0^{\rm s}\underline{E}^{\rm v}}{\underline{Q}_1^{\rm s}}. \tag{13}$$

Substituting Eqs. (4), (5), (12), and (13) into inequality (9), one can obtain the key generation rate in the weak+vacuum protocol. The simulation results with $\delta = 0.01$ are presented in Fig. 2(c). It is shown that the influence of such a small fluctuation of the internal transmittance on the key generation rate can be neglected. The maximum transmission distance can reach 140 km for the case without the transmittance fluctuation. The optimal $\lambda_{\rm os}$ and $\lambda_{\rm od}$ of the maximum transmission distance are 3.3×10^{-7} and 1.0×10^{-8} for the case without the transmittance fluctuation, 3.4×10^{-7} and 1.0×10^{-8} for the case with $\sigma = 0.05$, 3.5×10^{-7} and 1.0×10^{-8} for the case with $\sigma = 0.1$. From the above analysis, it can be seen that the optimal transmittance of the maximum transmission distance in the weak+vacuum protocol is much greater than that of the GLLP state without-decoy method and the one-decoy proposal. That is, more photons would be encoded in the system of the weak+vacuum protocol, leading to a higher final key generation rate and longer transmission distance.

In order to obtain a more detailed view of the transmittance fluctuation on the final key generation rate and transmission distance, we analyse the most general case, that is, the sources controlled by Eve, and Alice's internal transmittance fluctuation controlled in a receivable bound. Surprisingly, it is shown that even in this practical case, the security of the QKD system can be rigorously obtained. In the following numerical simulations, we consider Alice's internal transmittance fluctuation as $\sigma = 0.01$ and δ can be chosen differently. Figure 3 shows numerical results of $\delta = 0.01$, $\delta = 0.05$, and $\delta = 0.1$ for the three protocols, respectively. It can be seen that the one-decoy protocol is very sensitive to the fluctuation of the source. However, the influences of the untrusted source on the weak+vacuum proposal and the GLLP without-decoy method are much weaker. From Fig. 3(a), we can see that the result of the GLLP without-decoy method with $\delta = 0.01$ is very close to that of $\delta = 0.05$ and $\delta = 0.1$. The maximum transmission distance is close to 40 km. Figure 3(b) shows that the maximum transmission distance of the one-decoy protocol with $\delta = 0.01$ is greater than that of one-decoy with $\delta = 0.05$ and $\delta = 0.1$. The maximum transmission distance can reach 96 km with $\delta = 0.01$, 94 km with $\delta = 0.05$, and only 73 km with $\delta = 0.1$. That is, the maximum transmission distance is reduced for about 23 km due to the influence of relative fluctuation. It can be seen that the maximum transmission distances of the weak+vacuum protocol with different δ are very close to each other from Fig. 3(c). In addition, the advantage of the weak+vacuum protocol over the GLLP without-decoy and one-decoy protocols is shown by the fact that the maximum secure transmission distance is about 140 km. In order to increase the secure transmission distance and the key generation rate, one should choose the relevant parameters appropriately. Different proposals have different sensitivity to δ and σ, and choosing δ and σ too large or too small will make the security analysis less optimal.

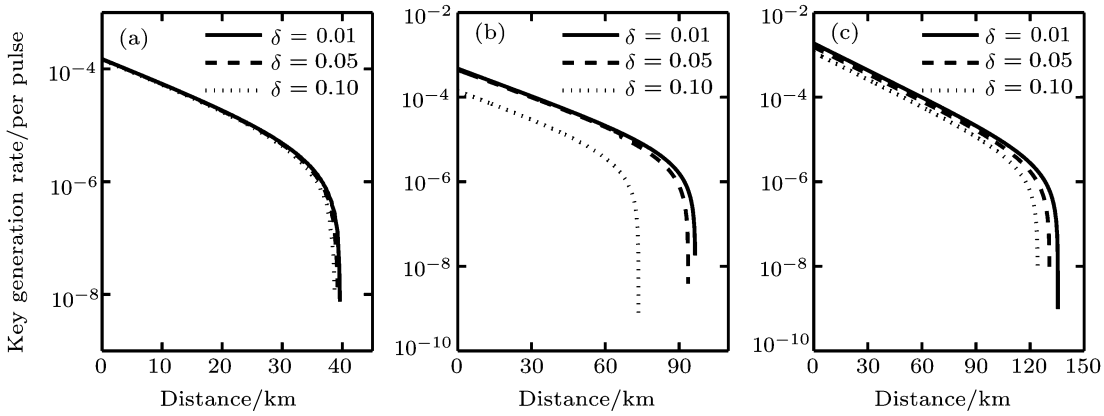


Fig. 3. Simulation results for (a) the GLLP protocol without decoy method, (b) the one-decoy protocol, and (c) the weak+vacuum protocol with different values of source fluctuation δ and Alice's internal transmittance fluctuation $\sigma = 0.01$.

To control σ is difficult; different σ can produce different maximum possible transmission distances. The maximum transmission distance of the weak+vacuum protocol for different σ is studied, as shown in Fig. 4. It can be seen that the maximum transmission distance slowly decreases with the growth of σ as $\sigma < 0.2$. However, it decreases quickly when $\sigma > 0.2$. It cannot obtain a secure final key for the case of $\delta = 0.01$ when $\sigma > 0.255$, and for the case of $\delta = 0.05$ when $\sigma > 0.222$.

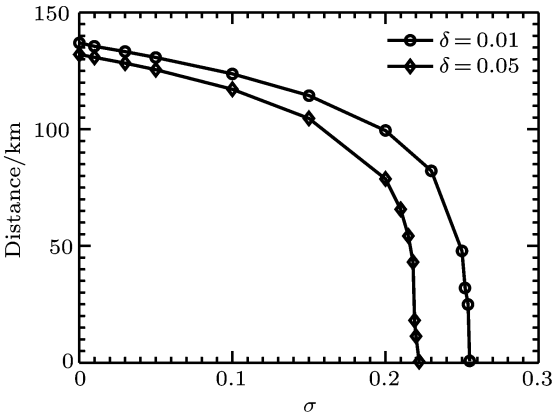


Fig. 4. Maximum transmission distances of the weak + vacuum protocol for various choices of σ.

3. Conclusions

In summary, we have applied the p & p system to practical experiments with untrusted sources. It is shown that the weak+decoy state method is more favourable for enhancing the secure transmission distance and the key generation rate in comparison with the one-decoy proposal and the GLLP state without-decoy method within relative statistical fluctuations. It is also shown that the one-decoy state is much more sensitive to statistical fluctuation. However, further numerical simulations show that the three protocols give similar evolution with statistical fluctuation. The secure transmission distance and the key generation rate can be increased by choosing optimal values of the parameters. In practice, imperfect devices in the QKD system may allow potential eavesdropping on the final key and influence maximum secure transmission distance, which needs to be considered seriously.

Acknowledgements

The authors thank Sun S H and Zhao Y for their helpful advice and comments.

References

[1] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inform. Comput.* **4** 325
[2] Inamori H, Lütkenhaus N and Mayers D 2007 *Eur. Phys. J.* D **41** 599
[3] Zhao F, Fu M X, Lu Y Q and Liu S H 2007 *Chin. Phys.* **16** 3402
[4] Jiao R Z, Feng C X and Ma H Q 2009 *Chin. Phys.* B **18** 915
[5] Muller A, Herzog T, Hutter B, Tittle W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793
[6] Zbinden H, Gautier J D, Gisin N, Hutter B, Muller A and Tittel W 1997 *Electron. Lett.* **33** 586
[7] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New. J. Phys.* **4** 41
[8] Zhao Y, Qi B, Ma X F, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502
[9] Lü H, Chen A X and Yan X D 2007 *Chin. Phys.* **16** 2862
[10] Sun S H, Ma H Q, Han J J, Liang L M and Li C Z 2010 *Opt. Lett.* **35** 1203
[11] Liu Q and Tan Y G 2011 *Chin. Phys.* B **20** 040303
[12] Wang X B, Peng C Z, Zhang J, Yang L and Pan J W 2008 *Phys. Rev.* A **77** 042311
[13] Zhao Y, Qi B and Lo H K 2008 *Phys. Rev.* A **77** 052327
[14] Peng X, Jiang H, Xu B, Ma X F and Gou H 2008 *Opt. Lett.* **33** 2077
[15] Peng X, Xu B and Gou H 2010 *Phys. Rev.* A **81** 042320
[16] Lütkenhaus N and Jahma M 2002 *New. J. Phys.* **4** 44
[17] Bennett C H and Brassard G 1984 *Proceedings of IEEE, International Conference on Computers, Systems, and Singal Processing* (New York: IEEE) p. 175
[18] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326
[19] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[20] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[21] Hu H P, Wang J D, Huang Y X, Liu S H and Lu W 2010 *Acta Phys. Sin.* **59** 287 (in Chinese)
[22] Mi J L, Wang F Q, Lin Q Q and Liang R S 2008 *Chin. Phys.* B **17** 1178
[23] Xu F X, Wang S, Han Z F and Guo G C 2010 *Chin. Phys.* B **19** 100312
[24] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[25] Wang X B 2005 *Phys. Rev.* A **72** 012322
[26] Sun S H, Liang L M and Li C Z 2009 *Phys. Lett.* A **373** 2533
[27] Jiao R Z and Zhang W H 2009 *Acta Phys. Sin.* **58** 2189 (in Chinese)