Parametric down-conversion with local operation and two-way classical communication*

Liu Qiang(刘 强)† and Tan Yong-Gang(谭勇刚)‡

Physics and Information Engineering Department, Luoyang Normal College, Luoyang 471022, *China*

(Received 1 October 2010; revised manuscript received 9 November 2010)

The decoy-state quantum key distribution protocol suggested by Adachi *et al.* (*Phys. Rev. Lett.* **99** 180503 (2007)) is proven to be secure and feasible with current techniques. It owns two attractive merits, i.e., its longer secure transmission distance and more convenient operation design. In this paper, we first improve the protocol with the aid of local operation and two-way classical communication (2-LOCC). After our modifications, the secure transmission distance is increased by about 20 km, which will make the protocol more practicable.

Keywords: parametric down-conversion, local operation and two-way classical communication, B step

PACS: 03.65.–w, 03.67.–a **DOI:** 10.1088/1674-1056/20/4/040303

1. Introduction

Differing from traditional cryptography, quantum key distribution (QKD) uses the fundamental principles of quantum mechanics to guarantee secure communication. It enables two parties (generally called Alice and Bob) to produce a shared random bit string only known to them, which can be used as the key to encrypt and decrypt messages. The first QKD protocol was proposed in 1984 by Bennett and Brassard, which is known as BB84 protocol.[1] In the first BB84 protocol, ideal single-photon source is required. However, in practical implementation of this protocol, weak coherence pulses (WCPs) are the usual candidate as photon sources.[2−7] Nevertheless, an eavesdropper (hence Eve) is assumed to be limited with quantum principles in QKD. Then the WCP is invoke apt to the attack of photon-number splitting (PNS).[8] It is now known that decoy state protocol is an efficient tool to combat this attack.[9−12] In decoy state protocol, multiple optical sources are used as signal sources and decoy sources. As every optical source has its unique character, Eve may make use of this to differentiate between the sources. Theoretically, only one optical source is expected and it is tailored into different intensity for different usage. Whereas, in practical implementation of decoy state protocol, the efficiency of this switch is comparably low. The passive decoy state protocol,[13,14] where the legitimate users choose their decoy states after their measurements, can remedy this drawback. The protocol presented by Adachi *et al.*[14] (hence AYKI protocol) is especially interesting because all their experimental apparatuses are based on present technology. How to improve the AYKI protocol is an interesting topic. In this paper, we consider this protocol with two-way classical communication (2-LOCC)[15−18] which can tolerate a higher initial error rate and extend longer secure transmission distance than 1-LOCC. This paper is arranged as follows: First, we review the AYKI protocol, then we apply the 2-LOCC theory to it. Secondly, we give numerical simulation on the performance of the improved AYKI protocol. Finally, we give some discussions and conclusions.

2. AYKI protocol with 2-LOCC

In the AYKI protocol, a parametric down-conversion (PDC) source is used.[19] As a pumping laser illuminates on a nonlinear crystal, some photons are converted into new photon-pairs. The state of the photons generated in both modes by PDC source can

*Project supported by the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 10905028/A050104), the Natural Science Foundation of Henan Province, China (Grant No. 092300410188), the Science Foundation of Hennan Provincial Education Department (Grant No. 2010A140010) and Youth Fund of Luoyang Normal College.

†Corresponding author. E-mail: qliu@lynu.edu.cn

‡Corresponding author. E-mail: ygtan@lynu.edu.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

be mathematically described as[20]

$$|\Psi\rangle = \sum_{n=0}^{\infty} \sqrt{p_n}|n\rangle|n\rangle. \quad (1)$$

Here $|n\rangle$ represents the photon number state. And p_n is the probability state $|n\rangle|n\rangle$ that occurs, and is given by

$$p_n \equiv \frac{\mu^n}{(1+\mu)^{n+1}}, \quad (2)$$

where μ is the average intensity of the photon-pairs. In the AYKI protocol, the PDC source is in Alice's Lab. She takes the photons in one mode and operates the polarization of the photons in the opposite mode as that in BB84 protocol and transfers them to Bob. Alice triggers the photons in her mode by a detector D_A with efficiency η_A and dark count rate d_A. The probability of detection (triggering) at D_A can be written as

$$\gamma_n = 1 - (1-d_A)(1-\eta_A)^n, \quad (3)$$

and with probability $1-\gamma_n$ Alice's detector misses the photons. Then the n-photon emission events from Alice's Lab can be divided into triggering events (at $p_n^{(t)}$) and non-triggering events (at $p_n^{(nt)}$), where $p_n^{(t)} = p_n\gamma_n$ and $p_n^{(nt)} = p_n(1-\gamma_n)$.

When the emission photons reach Bob's Lab, he measures them by two threshold detectors after a polarizing beam splitter (PBS). Supposing that the transmission efficiency of the quantum channel is $\eta_c = 10^{-\alpha l/10}$ and the detecting efficiency of Bob's detectors is η_B, with probability $\eta = \eta_c\eta_B$ a photon emitted from Alice's Lab will be detected by Bob's detectors. Here l is the length of the quantum channel, and α is its lossy rate coefficient. Let p_d be the dark count rate of Bob's detectors, with probability $Q_n = p_n[1-(1-\eta)^n(1-p_d)^2]$ Bob's detectors will gain an n-photon pulse. Bob's detecting events can be divided into two groups: Those registering on Alice's detector with probability $Q_n^{(t)} = Q_n\gamma_n$ and those missed by her detector with probability $Q_n^{(nt)} = Q_n(1-\gamma_n)$. In PDC protocol, a well prepared signal by Alice may hit on an erroneous detector, which causes the so-called quantum bit error rate (QBER). The overall detection rate $Q^{(t)}$ and the QBER $E^{(t)}$ with triggering and the overall detection rate $Q^{(nt)}$ and the QBER $E^{(nt)}$ without triggering can be achieved by

$$Q^{(t)} = \sum_{n=0}^{\infty} Q_n^{(t)}, \quad Q^{(nt)} = \sum_{n=0}^{\infty} Q_n^{(nt)}, \quad (4)$$

$$E^{(t)} = \sum_{n=0}^{\infty} \frac{Q_n^{(t)} e_n}{Q^{(t)}}, \quad E^{(nt)} = \sum_{n=0}^{\infty} \frac{Q_n^{(nt)} e_n}{Q^{(nt)}}, \quad (5)$$

where e_n is the QBER of an n-photon pulse. If Bob's detectors have the same characters, they will have the same background. Then the QBER on vacuum pulses e_0 can be assumed to be $\frac{1}{2}$ for the simplicity of discussion.

The relation between Alice's triggering and non-triggering events can be expressed as

$$Q_n^{(t)} = r_n Q_n^{(nt)}. \quad (6)$$

Here

$$r_n \equiv \frac{\gamma_n}{1-\gamma_n} = \frac{p_n^{(t)}}{p_n^{(nt)}}. \quad (7)$$

From Eq. (3), we can obtain the relationship

$$0 \le r_0 < r_1 < r_2 < r_3 \cdots. \quad (8)$$

Then we have $r_2 Q_n^{(nt)} \le Q_n^{(t)}$ for $n \ge 2$. Applying Eq. (4) leads to $r_2(Q^{(nt)} - Q_0^{(nt)} - Q_1^{(nt)}) \le Q^{(t)} - Q_0^{(t)} - Q_1^{(t)} = rQ^{(nt)} - r_0 Q_0^{(nt)} - r_1 Q_1^{(nt)}$. Here r is defined as $r \equiv Q^{(t)}/Q^{(nt)}$. If defining $x \equiv Q_0^{(nt)}/Q^{(nt)}$, one then has the lower bound on the ratio of $Q_1^{(nt)}$ and $Q^{(nt)}$

$$\frac{Q_1^{(nt)}}{Q^{(nt)}} \ge \frac{r_2 - r - (r_2 - r_0)x}{r_2 - r_1} \equiv \xi(x), \quad (9)$$

which is a function of x. The upper bound of QBER on single photon pulse can be estimated from

$$e_1 \le \frac{Q^{(t)}E^{(t)} - Q_0^{(t)} e_0}{Q_1^{(t)}} \le \frac{2rE^{(t)} - r_0 x}{2r_1\xi(x)} \equiv \epsilon_t(x). \quad (10)$$

In a similar way, one can have its other bound

$$e_1 \le \frac{2E^{(nt)} - x}{2\xi(x)} \equiv \epsilon_{nt}(x). \quad (11)$$

Combining the two bounds, one has

$$e_1 \le \epsilon(x) \equiv \min\{\epsilon_t(x), \epsilon_{nt}(x)\}. \quad (12)$$

Then, it is easy to have

$$0 \le x \le \min\{2E^{(t)}(r/r_0), 2E^{(nt)}\}. \quad (13)$$

Consequently, the low bound of the secure keys which Alice and Bob can obtain from Alice's detecting events is given by[14,21,22]

$$R^{(t)} = q\{Q^{(nt)} \min\{r_0 x + r_1\xi(x)[1 - H_2(\epsilon(x))]\} - Q^{(t)} f(E^{(t)}) H_2(E^{(t)})\}. \quad (14)$$

As presented in the AYKI protocol,[14] if the transmission distance is not very far, Alice and Bob can also generate the secure keys from the Alice's non-triggering events. The key generation rate from the non-triggering events is written as

$$R^{(nt)} = q\{Q^{(nt)} \min\{x + \xi(x)[1 - H_2(\epsilon(x))]\} - Q^{(nt)} f(E^{(nt)}) H_2(E^{(nt)})\}. \quad (15)$$

When the transmission distance is short, the key generation rate for both groups is nonnegative, then Alice and Bob can both generate their secure final keys. When the transmission distance is large, Alice and Bob can only generate their secure final keys from Alice's triggering events. That is, the key generation rate $R^{(\mathrm{both})}$ on both groups obeys

$$R^{(\mathrm{both})} = \max\{R^{(t)}, 0\} + \max\{R^{(nt)}, 0\}. \quad (16)$$

Now we would like to extend the AYKI protocol with 2-LOCC theory. As mentioned before, the 2-LOCC based on post-processing can tolerate a higher initial error rate and extend longer secure transmission distance than 1-LOCC.[15,16,18] The crux of this method is B steps. The process of PDC with 2-LOCC is as follows: Alice and Bob perform a sequence of B steps to the sifted keys. That is, Alice and Bob perform a bilateral XOR (BXOR) between pairs of the shared sifted keys and measure the target bits in Z basis. If their measurement outcomes disagree, they discard both of the control and target bits. Otherwise, they only keep the control bits.[15,18] So in the B step process, only the events that Bob's results coincide with those of Alice's can survive. Then after one B step, the survival events will have the probability

$$\tau = e^2 + (1 - e)^2, \quad (17)$$

where e is the error bit rate on Alice and Bob's sifted keys. In the AYKI protocol, Alice and Bob's sifted keys are divided into two parts: triggering and non-triggering events. Then the probability of the survival events can also be divided into two parts accordingly

$$\tau^{(t)} = (E^{(t)})^2 + (1 - E^{(t)})^2,$$
$$\tau^{(nt)} = (E^{(nt)})^2 + (1 - E^{(nt)})^2. \quad (18)$$

In the AYKI protocol, e_n is the same for all n-photon emission events theoretically, whether or not they are registered on Alice's detector. Then the probability for the survival probability untagged event and the vacuum event can be written as

$$\tau^1 = e_1^2 + (1 - e_1)^2,$$

$$\tau^0 = e_0^2 + (1 - e_0)^2. \quad (19)$$

Though the B step can lower the bit error rates of the AYKI protocol, it lowers the efficiency of key generation rate at the same time. The residue ratio of the key for the triggering events and non-triggering events after one B step is respectively expressed by

$$\rho_{\mathrm{B}}^{(t)} = \frac{1}{2}\tau^{(t)}, \quad \rho_{\mathrm{B}}^{(nt)} = \frac{1}{2}\tau^{(nt)}. \quad (20)$$

Here the factor 1/2 given is because Alice and Bob only keep the control bits in the XOR process. So the key generation rate can be written as

$$R^{(t)'} = \rho_{\mathrm{B}}^{(t)} R^{(t)}, \quad R^{(nt)'} = \rho_{\mathrm{B}}^{(nt)} R^{(nt)}. \quad (21)$$

The changes of the overall QBER of the triggering events and non-triggering events are respectively given by

$$E^{(t)'} = \frac{E^{(t)^2}}{E^{(t)^2} + (1 - E^{(t)})^2},$$
$$E^{(nt)'} = \frac{E^{(nt)^2}}{E^{(nt)^2} + (1 - E^{(nt)})^2}. \quad (22)$$

The bit error rate of the untagged pulses after one B step is given as

$$e_1' = \frac{e_1^2}{e_1^2 + (1 - e_1)^2}. \quad (23)$$

Substituting these parameters from Eqs. (17)–(23) into Eq. (16), one can obtain the key generation rate and the secure transmission distance of the AYKI protocol with one B step. If more B steps are required, one only needs to repeat this procedure. In the following numerical simulation, one can see that the B step can indeed improve the performance on the secure transmission distance apparently.

3. Numerical simulations

In the following numerical simulation, the efficiency of Alice's detector is fixed at $\eta_{\mathrm{A}} = 0.5$, and its background is assumed to be $d_{\mathrm{A}} = 1.0 \times 10^{-6}$. The parameters of the quantum channel and the apparatus on Bob's side take those of the GYS experiment,[2] where the loss coefficient of the quantum channel is $\alpha = 0.21$ dB/km, the detecting efficiency of Bob's detectors is $\eta_{\mathrm{B}} = 4.5$ and its dark counts rate is $p_{\mathrm{d}} = 8.5 \times 10^{-7}$. We also assume that with probability $e_{\mathrm{d}} = 3.3\%$ a pulse will hit on an erroneous detector because of basis misalignment between Alice and Bob. Substituting these parameters into Eq. (16),

one can obtain the numerical relationship between the key generation rate and the secure transmission distance, which is illustrated in Fig. 1. The dotted curve refers to the key generation rate of AYKI protocol with 1-LOCC, whose maximal transmission distance is about 170 km. And the solid curve is the improvement with 2-LOCC on the key generation rate of the former. With one B step, we can see that the maximal transmission distance can be enlarged about 20 km.

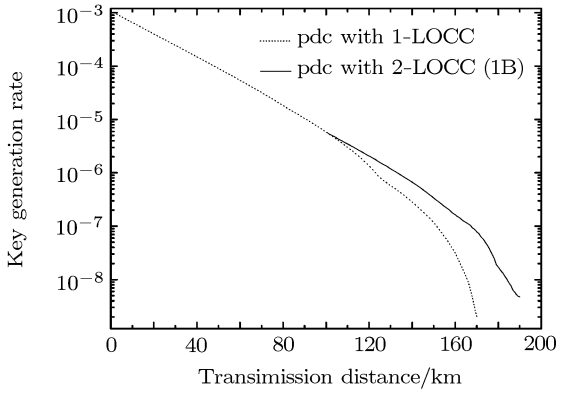


Fig. 1. The key generation rate versus the transmission distance, calculated by 1-LOCC AYKI protocol and 2-LOCC AYKI protocol (one B step). Our result of 1-LOCC AYKI protocol fits with that of AYKI protocol well[14] and the result of 2-LOCC protocol can improve that of the former by about 20 km.

As illustrated in the figure, the maximal transmission distance for the AYKI protocol with 2-LOCC can reach almost 190 km. It confirms us that the 2-LOCC can greatly improve the performance of the AYKI protocol.

4. Discussions and conclusions

QKD is aimed to generate a secure key between the legitimate users. Then the maximal transmission distance and the secure key generation rate are very important factors for it. As the security of AYKI protocol is based on the practical devices. In particular, it does not need any modulation on the apparatus during the experiment to generate decoy states, which is more efficient compared with the active decoy state. It is an interesting issue to consider whether one can still improve it with present technology. In this paper, we have shown that the 2-LOCC method is an efficient way for improving the performance of this protocol. Our numerical simulation showed that by about 20 km the secure transmission distance can be enlarged when one B-step is carried out. Our results may be useful for practical implement of the AYKI protocol.

Acknowledgement

We thank X. Ma for his helpful discussion.

References

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

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

[3] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41

[4] Kimura T, Nambu Y, Hatanaka T, Tomita A, Kosaka H and Nakamura K 2004 *Jpn. J. Appl. Phys.* **43** L1217

[5] Zhao Y, Qi B, Ma X, Lo H K and Qian L 2006 *Phys. Rev. Lett.* **96** 070502

[6] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B and Pan J W 2007 *Phys. Rev. Lett.* **98** 010505

[7] Hiskett P A, Rosenberg D, Peterson C G, Hughes R J, Nam S W, Lita A E, Miller A J and Nordholt J E 2006 *New J. Phys.* **8** 193

[8] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330

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

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

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

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

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

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

[15] Gottesman D and Lo H K 2003 *IEEE Transactions on Information Theory* **49** 457

[16] Chau H F 2002 *Phys. Rev.* A **66** 060302(R)

[17] Gerd K, Vollbrecht H and Verstraete F 2005 *Phys. Rev.* A **71** 062325

[18] Ma X, Fung C H F, Dupuis F, Chen K, Tamaki K and Lo H K 2006 *Phys. Rev.* A **74** 032330

[19] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[20] Yurke B and Potasek M 1987 *Phys. Rev.* A **36** 3464

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

[22] Lo H K 2005 *Quantum Information Comput.* **5** 413