Vol 15 No 7, July 2006
1009-1963/2006/15(07)/1418-03

Chinese Physics

© 2006 Chin. Phys. Soc.
and IOP Publishing Ltd

Secure quantum dialogue based on single-photon*

Ji Xin(计 新)† and Zhang Shou(张 寿)‡

Department of Physics, College of Science, Yanbian University, Yanji 133002, *China*

(Received 5 January 2006; revised manuscript received 9 February 2006)

In this paper a quantum dialogue scheme is proposed by using N batches of single photons. The same secret message is encoded on each batch of single photons by the sender with two different unitary operations, and then the N batches of single photons are sent to the receiver. After eavesdropping check, the message is encoded on the one remaining batch by the receiver. It is shown that the intercept-and-resend attack and coupling auxiliary modes attack can be resisted more efficiently, because the photons are sent only once in our quantum dialogue scheme.

Keywords: quantum dialogue, single photon, unitary operation
PACC: 0365

As is known, quantum key distribution based on quantum mechanics allows two remote legitimate users to establish a shared secret key through the transmission of quantum signals and use this key to encrypt secret messages. Since Bennett and Brassard proposed the standard BB84 QKD protocol[1] in 1984, the development of quantum key distribution[2−11] has attracted the attention of many researchers.

Recently, quantum secure direct communication (QSDC) was proposed.[12−20] This is to transmit the secret message directly without first establishing a key to encrypt them. Boström and Felbinger[12] presented a ping-pong QSDC scheme by using Einstein–Podolsky–Rosen (EPR) pairs. Deng and Long[18] proposed a QSDC scheme by using four single photon states. Whereas, their schemes are only one-way communication. In order to realize bidirectional communication, Nguyen[21] presented a quantum dialogue scheme which enables both legitimate parties to exchange their secret messages directly by using EPR pairs. However, in his scheme, an eavesdropper who adopts the intercept-and-resend attack strategy can steal the secret messages without being detected. Then Man *et al*[22] modified the scheme, i.e. in the control mode, the intercept-and-resend attack can be detected by introducing and randomly choosing two sets of measuring bases. Nevertheless, there is still a hidden danger in the above schemes:[21,22] if there were an eavesdropper in the quantum channel when the message qubit is being sent, the messages would be leaked inevitably to the eavesdropper who adopts the intercept-and-resend attack strategy or coupling auxiliary modes attack strategy.[23]

In this paper, we present a quantum dialogue scheme based on N batches of single photons. In our scheme, the sender Bob encodes the same message on each batch of N batches of single photons, and sends them to the receiver Alice in one go. Then Alice selects randomly $N-1$ batches of single photons to check, together with Bob, the security of quantum channel by using two different measuring bases. After assuring the safety of the quantum channel, Bob encodes his message on the remaining one batch to complete the quantum dialogue. In Ref.[18], they send photons twice to realize one-way communication, while in our scheme, we can realize bidirectional communication with photons being sent only once. Our scheme can resist the intercept-and-resend attack and coupling auxiliary modes attack more efficiently than that in Refs.[21] and [22], because the photons are sent only once and simultaneously in our scheme.

Initially, we write the four single photon states as

$$|\alpha\rangle = |0\rangle, \qquad |\beta\rangle = |1\rangle,$$
$$|\gamma\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\delta\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the horizontal and vertical polarization states respectively. $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, and $i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ are two unitary operations acting on one single photon, for example, $I|\alpha\rangle = |\alpha\rangle$, $I|\gamma\rangle = |\gamma\rangle$, $i\sigma_y|\alpha\rangle = |\beta\rangle$, $i\sigma_y|\gamma\rangle = |\delta\rangle$. Alice and Bob agree on that the two unitary operations are encoded

*Project supported by the Science Foundation of Yanbian University of China (Grant No 2005-20).
†E-mail: jixin@ybu.edu.cn
‡E-mail: szhang@ybu.edu.cn

information as

$$I \longrightarrow 0, \qquad i\sigma_y \longrightarrow 1. \tag{2}$$

Now we describe the quantum dialogue process in detail.

(1) Bob initially prepares N batches of single photons. Suppose each batch of single photons is composed of many photons which are randomly in one of the four states $|\alpha\rangle$, $|\beta\rangle$, $|\gamma\rangle$, and $|\delta\rangle$. Bob encodes the same message on each batch of the N batches of single photons by performing unitary operations I or $i\sigma_y$, and sends them to Alice. The number of photons in each batch is determined by the length of the message. For instance, if the message that Bob wants to transmit is 0010, there should be four photons in each batch of the N batches. Bob needs to encode the message 0010 by performing four unitary operations of $I, I, i\sigma_y, I$ on the four photons in each batch respectively. Thus, the states of the photons in each batch all carry the message that Bob wants to transmit.

(2) Alice informs Bob that she has received the N batches of photons. Then Alice and Bob check eavesdropping by the following procedures. Firstly, Alice selects randomly $N-1$ batches of photons from the N batches and measures them by using one of the two measuring bases $\{|0\rangle, |1\rangle\}$ and $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ randomly. Then Alice informs Bob of the position, the measuring bases and measurement result for each photon she has measured via a classical channel. According to Alice's measuring bases and measurement results, Bob can know whether the eavesdropper is in the line. If the error rate is higher than the threshold, Bob concludes that the channel is not secure, and aborts the quantum dialogue. Otherwise, Alice and Bob continue to the next step.

(3) Alice encodes her message on the remaining one batch. Then Bob informs Alice of the initial states of each photon in the batch. Alice measures them by using one of the two measuring bases in terms of the initial state which Bob has told her and she reads out Bob's secret message.

(4) Alice announces her measurement results to Bob. According to Alice's measurement results and the unitary operations performed by himself, Bob reads out Alice's secret message directly.

For example, if Bob initially prepares a single photon state in $|\gamma\rangle$, and performs the unitary operation $i\sigma_y$, then Alice performs the unitary operation I on it, so the single photon state becomes $|\delta\rangle$, namely $I \otimes i\sigma_y|\gamma\rangle = |\delta\rangle$. So Alice gets the measurement result $|\delta\rangle$ of the single photon state. After knowing the initial state that Bob has told her, Alice reads out Bob's secret message $i\sigma_y$(or 1) directly based on her measurement result $|\delta\rangle$ and the unitary operation I performed by herself. Also, Bob can read out Alice's secret message I(or 0) directly based on Alice's measurement result $|\delta\rangle$ and the unitary operation $i\sigma_y$ performed by himself. So the quantum dialogue is completed successfully.

Now, we discuss the security of our scheme. In our scheme, the initial state of each photon is randomly prepared in one of the four states. After having encoded his message on each batch of the N batches, Bob sends them to Alice. If the eavesdropper intercepts the photons, sent from Bob to Alice, he cannot get any useful message and his behaviour can be detected undoubtedly, due to our introducing and randomly choosing two sets of measuring bases to check eavesdropping. We now consider another eavesdropping attack which we call subsection intercepting attack here. We suppose that the eavesdropper is so superior that he knows the length of the message (or the number M of the photons in each batch). If we happen to prepare the initial state of the same sequence number photon in each batch in the same state, then the eavesdropper may intercept the first photon, the second photon, the third photon, ..., the Mth photon from different $M(M < N)$ batches respectively, when the N batches of photons, on which the same message has been encoded by Bob, are being sent from Bob to Alice. Then the eavesdropper sends M false photons, prepared randomly in one of the four states, to Alice (the error rate caused by the eavesdropper may be concealed in the noise). After Alice's encoding on the remaining one batch of photons, Bob announces the initial state of the photons, then the eavesdropper measures the photons and she obtains Bob's message. After Alice's measuring the batch of photons encoded by herself and announcing the measurement results, the eavesdropper obtains Alice's message. Therefore, in our scheme, the initial state of each photon in each batch should be prepared in one of the four states randomly to avoid this kind of eavesdropping.

In summary, we have proposed a quantum dialogue scheme for two legitimate parties to exchange their secret messages directly by using single photons. Compared with the previous dialogue schemes[21,22] in which the photons are sent back and forth, our scheme decreases the opportunity of being attacked in a noisy

channel when the eavesdropper takes the intercept-and-resend strategy or coupling auxiliary modes strategy, because each batch of single photons is encoded on with the same message respectively and sent only once and simultaneously. So our scheme can resist the intercept-and-resend attack and coupling auxiliary modes attack more efficiently than the previous dialogue schemes. In addition, our scheme can also resist the subsection intercepting attack discussed above. It should be pointed out that single photons are more difficult to prepare than entangled photons in the present technique. Furthermore, the single-photon resource is a decaying laser which is an approximate single-photon resource. Therefore, in order to assure the security of our scheme, it is not easy for us to prepare, encode and send a great deal of single photons simultaneously.

References

[1] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (New York: IEEE) p175
[2] Cabello A 2000 *Phys. Rev.* A **61** 052312
[3] Long G L and Liu X S 2002 *Phys. Rev.* A **65** 032302
[4] Xue P, Li C F and Guo G C 2002 *Phys. Rev.* A **65** 022317
[5] Zhang Q, Tang C J and Zhang S Q 2002 *Acta Phys. Sin.* **51** 1439 (in Chinese)
[6] Zhang Q and Zhang E Y 2002 *Acta Phys. Sin.* **51** 1684 (in Chinese)
[7] Song D 2004 *Phys. Rev.* A **69** 034301
[8] Wang X B 2004 *Phys. Rev. Lett.* **92** 077902
[9] Yang Y G, Wen Q Y and Zhu P C 2005 *Acta Phys. Sin.* **54** 3995 (in Chinese)
[10] Ma H Q, Li Y L, Zhao H and Wu L A 2005 *Acta Phys. Sin.* **54** 5014 (in Chinese)
[11] Yang Y G, Wen Q Y and Zhu P C 2005 *Acta Phys. Sin.* **54** 5544 (in Chinese)
[12] Boström K and Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902
[13] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317
[14] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 18
[15] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[16] Gao T, Yan F L and Wang Z X 2004 *Nuovo Cimento* B **119** 313
[17] Gao T, Yan F L and Wang Z X 2005 *J. Phys.* A **38** 5761
[18] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319
[19] Zhu A D, Xia Y, Fan Q B and Zhang S 2006 *Phys. Rev.* A **73** 022338
[20] Jang S S and Lee H W 2005 *Phys. Lett.* A **339** 430
[21] Nguyen B A 2004 *Phys. Lett.* A **328** 6
[22] Man Z X, Zhang Z J and Li Y 2005 *Chin. Phys. Lett.* **22** 22
[23] Wôjcik A 2003 *Phys. Rev. Lett.* **90** 157901