Vol 16 No 10, October 2007
1009-1963/2007/16(10)/2862-05
Chinese Physics
© 2007 Chin. Phys. Soc.
and IOP Publishing Ltd

Unconditional secure two-way quantum dense key distribution*

Lü Hua(吕 桦)[a)c)d)†], Chen Ai-Xi(陈爱喜)[b)], and Yan Xu-Dong(闫旭东)[a)]

[a)] *Department of Mathematics and Physics, Hubei University of Technology, Wuhan* 430068, *China*
[b)] *Department of Physics, East China Jiaotong University, Nanchang* 330013, *China*
[c)] *Wuhan Institute of Physics and Mathematics, Chinese Academy of Sciences, Wuhan* 430071, *China*
[d)] *University of the Chinese Academy of Science, Beijing* 100049, *China*

(Received 9 November 2006; revised manuscript received 13 April 2007)

In this paper, we present a two-way quantum dense key distribution protocol. With double check modes, our scheme is secure regardless of the presence of noises. And with a quantum teleportation process, secret message can be encoded deterministically even if the quantum channel is highly lossy. Therefore, our scheme can be used in a realistic quantum channel regardless of the presence of noises and channel losses.

Keywords: quantum cryptography, security, two-way communication
PACC: 0365, 0367

1. Introduction

Quantum key distribution (QKD) is a physically secure method of creating a private key that can be created between two partners, Alice and Bob, who share a quantum channel and a public-authenticated channel.[1] The key bits can be used to implement a classical private key cryptosystem, or more precisely called one-time pad algorithm, to empower the partners to communicate securely. The pioneer QKD protocol was presented by Bennett and Brassard in 1984,[2] of which the security has been studied deeply.[3−7]

In 1992, Bennett and Wiesner[8] presented a well-known dense coding protocol in which a two-bit message can be encoded by a unitary operation. However, as pointed out by Bennett and Wienser, the intrinsic security of dense coding protocol is illusory, for an eavesdropper could effectively tap into the channel by intercepting all the particulars on their way to and from Bob, and substituting others in such a way as to impersonate Alice to Bob and Bob to Alice. In Ref.[9], Boström and Felbinger have announced that the dense coding feature has to be abandoned in favour of the secure transmission. After that, Cai and Li[10] showed that dense coding character could be implemented in a perfect channel with a check mode. However, the tolerable noise was not quantified. Furthermore, if we consider that the realistic quantum channels are highly lossy, the recent quantum secure deterministic communication (QSDC) protocols may not be implemented.[9−17] In message mode, Alice will perform an encoding operation every time. However, if the quantum channel is lossy, Alice may encode her message in an empty pulse. Therefore, the QSDC protocols can not be used in the lossy channel without being modified.

In this paper, we present a two-way dense key distribution protocol which is unconditionally secure in the presence of noise, and an improved scheme of QSDC protocols, which can be used in a highly lossy quantum channel to encode the secret message with unitary probability. We show that our scheme can be used regardless of the presence of noises and quantum channel losses.

2. Bennett-Wiesner dense coding protocol

Two qubits can be entangled only in one way so that four Bell states $|\psi^{\pm}\rangle$, $|\phi^{\pm}\rangle$, which are mutually orthogonal to each other, can be transformed into each other only by local unitary operations. Usually, these four Bell states can be written as

$$|\phi^{+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle),$$

*Project supported by the National Natural Science Foundation of China (Grant No 10504039).
†E-mail: lvhuahg@163.com

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle),$$
$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle),$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \quad (1)$$

Now we assume that Bob prepares an Einstein-Podolsky-Rosen (EPR) pair in the state $|\psi^-\rangle$. He sends one qubit (travel qubit) to Alice and keeps another one (home qubit) in her laboratory. Having received Bob's travel qubit, Alice performs a unitary operation U_{ij} on it to encode her information, where U_{ij} are

$$U_{00} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U_{01} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$U_{10} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad U_{11} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (2)$$

Clearly, these four operations U_{ij} can transform the state $|\psi^-\rangle$ into $|\psi^-\rangle$, $|\psi^+\rangle$, $|\phi^-\rangle$, and $|\phi^+\rangle$, respectively. As a rule, Alice's four operations correspond to her codes 00, 01, 10, and 11, respectively. Then Alice returns the travel qubit to Bob. Having received the back qubit, Bob performs a Bell-basis measurement on two qubits to decode Alice's information. In this way, one travel qubit can transmit two classical bits, which is the well-known dense coding protocol. However, such a protocol cannot be used directly in realistic communication because of the potential eavesdropping. Furthermore, practical communication channels are noisy so that a QKD protocol should be of tolerable noise.

3. Two-way quantum dense key distribution with double check modes

In the dense coding protocol, the travel qubit is sent from Bob to Alice first. Then it will be sent back to Bob after Alice's encoding operations. Thus, an eavesdropper may attack the travel qubit either in the line $B \to A$ or in the line $A \to B$. In this case, security of the communication has to be ensured both in line $B \to A$ and in line $A \to B$. That is, double check modes are necessary to ensure the security of the communication.

In order to improve the security of communication, we have to modify the communication with two additional check modes. The modified protocol is described as follow (See Fig.1.):

(1) Bob creates n EPR pairs in the state $(|\psi^-\rangle)^{\otimes n}$.

(2) Bob selects a random m-bit string b, and selects m EPR pairs. He performs a Hadamard transform on the travel qubit of each selective EPR pair in which b is 1.

(3) Bob sends each travel qubit of his n EPR pairs to Alice.

(4) Alice receives n qubits and announces this fact.

(5) Bob announces the bit string b, and which m EPR pairs are the bits to be checked.

(6) Alice performs Hadamard transform on the qubits where b is 1.

(7) Bob and Alice each measure their half of m check EPR pairs in $|0\rangle$ and $|1\rangle$ basis. If there are too many of these measurements to agree with each other, they abort the protocol (This is the first check mode: verify the fidelity of the EPR pair.)

(8) Alice encodes her information on the encoding qubits and returns them to Bob.

(9) Bob performs Bell-basis measurement on each EPR pair to draw Alice's information.

(10) Alice publishes some of her key bits. Bob compares Alice's announced measurements with his measurements to obtain the quantum bit error rate (QBER). If the QBER is higher than the threshold d_0, they abort the protocol (This is the second check mode.). If both the fidelity and the QBER are normal, Alice and Bob will use their encoding bits to generate a raw key. Having made error-correcting and privacy amplification, they can obtain the secure final key. The threshold d_0 will be calculated later.

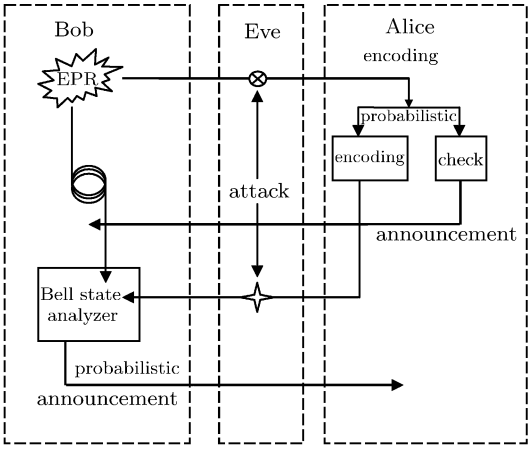


Fig.1. Sketch of our two-way communication scheme.

4. Security proof

We now prove that this double check communication protocol described above is a secure QKD protocol. Since $\rho_A^{\pm} := \mathrm{tr}_B\{|\psi^{\pm}\rangle\langle\psi^{\pm}|\} = \mathrm{tr}_B\{|\phi^{\pm}\rangle\langle\phi^{\pm}|\}$, the eavesdropper-Eve cannot distinguish each of Bell states if she attacks the travel qubit only after Alice's encoding operation. So she has to attack the travel qubit in the line $B \to A$ first. After Alice's encoding operation, she performs a measurement attack in the line $A \to B$ to obtain Alice's encoding message. The most general idea of Eve's attack in the line $B \to A$ can be described as follows. When a qubit propagates from Bob to Alice, Eve can let a system chosen by her, called a probe (ancilla), interact with this qubit. Eve can freely choose the initial state of the probe, and the interaction. But she should obey the laws of quantum mechanics. After the interaction, Eve forwards the qubit to Alice. Then the EPR pair is entangled with Eve's probe. Suppose that the state of the EPR pair Bob and Alice share becomes ρ under Eve's interactions (ρ is a mixed state now.). In the line $A \to B$, Eve will perform a joint measurement on the travel and her probe to draw Alice's encoding information. It has been proven that information Eve can gain I_{E} in the line $A \to B$ is determined by the fidelity f of the state $|\psi^-\rangle$ and ρ.[10] Suppose

$$F(|\psi^-\rangle, \rho)^2 = \langle\psi^-|\rho|\psi^-\rangle = f, \tag{3}$$

where $F(|\psi^-\rangle, \rho)$ is the fidelity of $|\psi^-\rangle$ and ρ; $0 \le f \le 1$. Therefore, the entropy of ρ is bounded by the entropy of a diagonal density matrix $\rho_{\max}$ with diagonal entries f, $(1-f)/3$, $(1-f)/3$, and $(1-f)/3$.[10] The entropy of $\rho_{\max}$ is

$$S(\rho_{\max}) = -f\log_2 f - (1-f)\log_2\frac{1-f}{3}. \tag{4}$$

Thus, we can conclude that information Eve can gain $I_{\mathrm{E}}(f)$ is tightly bounded by $S(\rho_{\max})$, i.e. $I_{\mathrm{E}}(f) \le S(\rho_{\max})$. Hence, the information Eve can gain is determined by the fidelity f.

Alice and Bob can verify the fidelity $F(|\psi^-\rangle, \rho)$ by using their local measurements and classical communication. One property of $|\psi^-\rangle$ is that $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|+\rangle|-\rangle - |-\rangle|+\rangle)$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. In the realistic channel, noises will cause bit flip and phase flip of the travel qubit. The bit flip could be found out when Alice and Bob measure their qubits in the basis $|0\rangle$, $|1\rangle$ directly. Note that for the EPR pairs where $b = 1$ in our protocol. Alice and Bob can effectively measure them in the basis $|+\rangle$, $|-\rangle$ rather than the $|0\rangle$, $|1\rangle$ basis. From the relations

$$\begin{aligned}&|\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-| = |00\rangle\langle 00| + |11\rangle\langle 11|,\\ &|\psi^+\rangle\langle\psi^+| + |\phi^+\rangle\langle\phi^+| = |++\rangle\langle++| + |--\rangle\langle--|,\end{aligned} \tag{5}$$

we know that the rates of bit flip errors and of phase flip errors that Alice and Bob estimate from their measurements on check qubits are the same as those estimated by using Bell-basis measurements.[6]

Now we consider the security authentication in the second check mode. Bob's mean information gain on Alice's bit, I_{AB}, equals their relative entropy decrease: $I_{AB} = H_{\text{a priori}} - H_{\text{a posteriori}}$.[1] The a posteriori entropy must be averaged over all possible results r:

$$H_{\text{a posteriori}} = \sum_r p(r)H(i|r), \tag{6}$$

where

$$H(i|r) = -\sum_i p(i|r)\log_2[p(i|r)],$$

$$p(i|r) = \frac{p(r|i)p(i)}{p(r)},$$

with $p(r) = \sum_i p(r|i)p(i)$. In practice, probabilities of Alice's four encoding operations are identical. In this case, Alice's a priori bits are two, i.e. $H_{\text{a,priori}} = 2$. Consequently, information Bob can draw from his measurements is that

$$I_{AB} = 2 - H_{\text{a posteriori}}. \tag{7}$$

A realistic quantum channel is noisy. The presence of noises can cause bit errors. So Alice and Bob should estimate the QBER in the second check mode. After Bob's decoding measurements, Alice should publish some of her key bits to obtain the QBER. Suppose the verified QBER to be d. Thus, Bob can obtain Alice's correct message with probability $1-d$, and he gains the wrong message with probability d. The maximal value of $H_{\text{a posteriori}}$ is that

$$H^{\max}_{\text{a posteriori}} = -(1-d)\log_2(1-d) - d\log_2\frac{d}{3}. \tag{8}$$

Thus, the mutual information between Alice and Bob is

$$I_{AB}(d) = 2 - \left[-(1-d)\log_2(1-d) - d\log_2\frac{d}{3}\right]. \tag{9}$$

In QKD, privacy amplification can be implemented if and only if $I_{AB}(d) > I_{\mathrm{E}}(f)$.[1] Consequently, the necessary and sufficient condition for the secure final key is

$$-(1-d)\log_2(1-d) - d\log_2\frac{d}{3}$$

$$-f\log_2 f-(1-f)\log_2\frac{1-f}{3}<2, \qquad (10)$$

where $0 \le d \le 1$ and $0 \le f \le 1$. This is the necessary and sufficient condition of the security of the final key. We show a numerical solution of Eq.(10) in Fig.2. Thus, we have presented an unconditional secure condition for the double check communication protocol with dense coding feature.

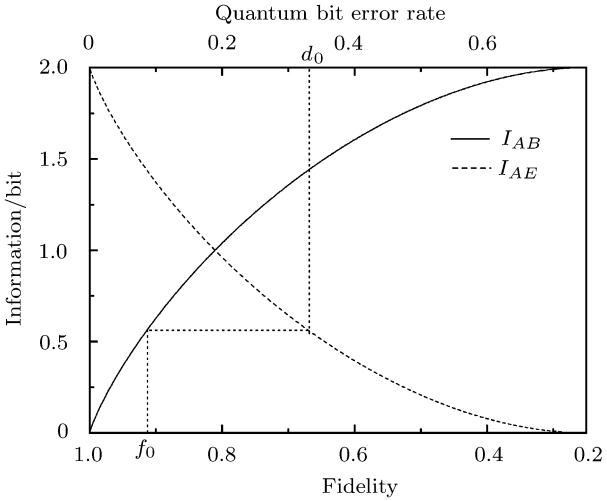


Fig.2. Security authentication. Security of the communication is ensured by Eq.(10), $I_{AB}(f) > I_E(d)$. For example, when the QBER in the second check is d_0, it requires that $f > f_0$ to ensure the security of the communication. In other words, if Alice and Bob find out the fidelity to be f_0, they will continue their protocol if and only if the QBER in the second check mode is $d \le d_0$.

5. Deterministic encoding in lossy channel

In fact, our scheme can be modified as a QSDC protocol which is similar to that in Ref.[10]. Consider that realistic quantum channels are lossy so that a QSDC scheme may not be used. In QSDC protocols,[9−12,18] having received Bob's photon, Alice performs an encoding operation in message mode. However, if the quantum channels are lossy, it is difficult for Alice to encode her message accurately. Eve if Alice knows the exact time when Bob sends the travel photon and the time when the travel photon should arrive, she cannot judge whether an arriving photon pulse is empty or not for the quantum channel losses. Thus, Alice's encoding operation is unsuccessful when the photon pulse is empty. This implies that information transmission is not "deterministic" any longer. However, this problem can be overcome with quantum teleportation (QT) or entanglement swapping (ES). In Fig.3, when an arriving photon pulses arrives, Alice performs Bell basis measurement in message mode. If the arriving pulse is empty, then Alice's Bell basis measurement will fail so that she does not perform the encoding operations. Only when the Bell basis measurement is successful can Alice encode her message. Therefore, with the QT or ES, Alice can encode her message with unitary probability, i.e. information can be transmitted in a deterministic way even if the quantum channel is highly lossy.

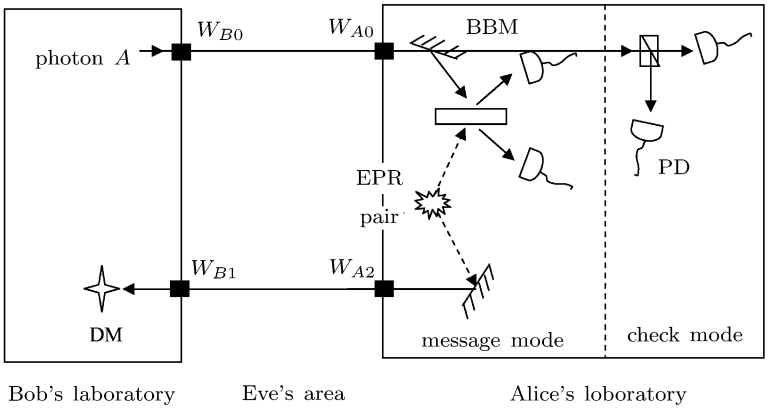


Fig.3. The simplest scheme of the probabilistic Bell state measurement with a beam splitter and two single-photon detectors. Only when the travel is detected in the Bell basis measurement can Alice encode her secret message.

6. Summary and discussion

Our scheme is an improvement on the one in Ref.[10]. Reference [10] indicates that dense coding can be used as quantum secure direct communication in an ideal channel, and it only presents the relation between the fidelity in the first check mode and the information Eve can gain. In fact, both Refs.[10]

and [13] offer the secure direct communication protocols that can be used only in ideal quantum channels. However, we have presented a two-way QKD scheme with dense coding character. Having compared our scheme with those in Refs.[10] and [13], we should point out that our scheme can be used in a noisy and lossy channel.

In summary, we have presented a double check mode quantum dense coding protocol. Our scheme needs quantum information storage which has been discussed in Ref.[19]. We have shown that our communication scheme is secure in the presence of noise. We have presented a modified scheme which can help us to encode the secret message with unitary probability when the quantum channel is lossy. Therefore, our two-way quantum dense coding scheme with double check modes is secure and deterministic regardless of the presence of noises and channel losses.

Acknowledgment

We thank Qing-yu Cai for useful discussion.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[2] Bennett C H and Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* Bangalore, India, (New York: IEEE) pp175-179

[3] Mayers D 2001 *J. of ACM* **48** 351

[4] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 *Proc. of the Thirty-Second Annual ACM Symposium on Theory of Computing* (Portland, OR) pp715–724

[5] Lo H K and Chau H F 1999 *Science* **283** 2050

[6] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[7] Gottesman D, Lo H K, Lükenhaus N and Preskill J 2004 *Quant. Inf. Comp.* **5** 325

[8] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881

[9] Boström K and Felbinger T, 2002 *Phys. Rev. Lett.* **89** 187902
Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801

[10] Cai Q Y and Li B W 2004 *Phys. Rev.* A **69** 054301

[11] Cai Q Y and Li B W, 2004 *Chin. Phys. Lett.* **21** 601
Lucamarini M and Mancini M 2005 *Phys. Rev. Lett.* **94** 140501
Ji X and Zhang S 2006 *Chin. Phys.* **15** 1418

[12] Deng F G and Long G L 2004 *Phys. Rev.* A **69** 052319

[13] Deng F G, Long G L and Liu X S, 2003 *Phys. Rev.* A **68** 042317

[14] Wang C, Deng F G, Li Y S, Liu Y S and Long G L 2005 *Phys. Rev.* A **71** 044305

[15] Yan F L and Zhang X 2004 *Eur. Phys. J.* B **41** 75

[16] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893 313

[17] He G Q and Zeng G H 2006 *Chin. Phys.* **15** 1284

[18] Li X H, Deng F G, Li C Y, Liang Y J, Zhou P and Zhou H Y 2006 *J. Korean Phys. Soc.* **49** 1354

[19] Deng F G, Long G L, Wang Y and Xiao L 2004 *Chin. Phys. Lett.* **21** 2097