A quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation*

LI Jian(李剑)[1] SONG Dan-Jie(宋丹劼)[1;1)] GUO Xiao-Jing(郭晓静)[1] JING Bo(景博)[1,2]

[1] School of Computer, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Department of Computer Science, Beijing Institute of Applied Meteorology, Beijing 100029, China

Abstract: In order to transmit secure messages, a quantum secure direct communication protocol based on a five-particle cluster state and classical XOR operation is presented. The five-particle cluster state is used to detect eavesdroppers, and the classical XOR operation serving as a one-time-pad is used to ensure the security of the protocol. In the security analysis, the entropy theory method is introduced, and three detection strategies are compared quantitatively by using the constraint between the information that the eavesdroppers can obtain and the interference introduced. If the eavesdroppers intend to obtain all the information, the detection rate of the original ping-pong protocol is 50%; the second protocol, using two particles of the Einstein-Podolsky-Rosen pair as detection particles, is also 50%; while the presented protocol is 89%. Finally, the security of the proposed protocol is discussed, and the analysis results indicate that the protocol in this paper is more secure than the other two.

Key words: QSDC, XOR operation, five-particle cluster state, eavesdropping detection, protocol security

PACS: 03.67.Dd, 03.67.Hk, 03.67.-a **DOI:** 10.1088/1674-1137/36/1/005

1 Introduction

Quantum mechanics offers some unique capabilities for the processing and transmission of quantum information. Over the past decade, scientists have made dramatic progress in the field of quantum communication. Since Bennett and Brassard [1] proposed the pioneer quantum key distribution (QKD) protocol in 1984, in which two remote authorized users (Alice and Bob) can create a shared private key, many quantum information security processing schemes have been presented [2–13].

Subsequently, a new concept, quantum secure direct communication (QSDC), was put forward and actively pursued [14–34]. Different from QKD, whose goal is to establish a common random key between the two remote parties of communication, QSDC's goal is to transmit the secret message directly without first creating a private key to encrypt the secret message. In 2002 Beige et al. proposed a QSDC scheme based on single-photon two-qubit states [14]. In this scheme, the message can be read after the transmission of an additional classical bit for each qubit. Subsequently, Boström and Felbinger put forward a ping-pong protocol using Einstein-Podolsky-Rosen (EPR) pairs as quantum information carriers [15]. But this proved to only be a deterministic QKD scheme rather than a QSDC scheme. Long et al. proposed a theoretical two-step QKD scheme using EPR pairs [16], which is the first QSDC protocol. This introduced the method of quantum data block transmission for the security in QSDC based on error rate analysis. To guard the secret message, one has to ensure the security of a block of quantum data [14, 16–19] before encoding the secret message. When errors exist, error correction and quantum privacy amplification can be used to maintain its security. In 2003, modifying the basic idea in Ref. [16], Deng et al. proposed a two-step secure QSDC scheme with EPR pairs [17] also transmitted in blocks.

Received 28 March 2011, Revised 3 May 2011
* Supported by National Natural Science Foundation of China (61100205)
1) Corresponding author. E-mail: songdj@bupt.edu.cn

Another class of quantum communication protocol [14, 20] used to transmit secret messages is called deterministic secure quantum communication (DSQC). The receiver can only read out the secret message after he exchanges at least one bit of classical information for each qubit with the sender in a DSQC protocol, which is different from QSDC. DSQC is similar to QKD, but can be used to obtain deterministic information, not a random binary string, which is different from QKD protocols in which the user cannot predict whether an instance is useful or not.

In this paper, a QSDC protocol is proposed. The five-particle cluster state is used to detect eavesdroppers and the classical XOR operation, serving as a one-time-pad (OTP), is used to ensure the security of the protocol. In Ref. [19], the original ping-pong protocol is called OPP, and the protocol it proposed is called MPP for convenience. Referring to Ref. [19], the proposed DSQC protocol in this paper is called FWPP. During the security analysis, the entropy theory method is introduced, and three detection strategies are compared quantitatively by using the constraint between the information the eavesdroppers can obtain and the interference introduced. If the eavesdroppers get the full information, the detection rate of OPP is 50%, MPP is also 50%, while FWPP is 89%. Finally, the security of the proposed protocol is discussed. The analysis results show that the proposed protocol in this paper is more secure than the other two.

2 Model and method

2.1 The process of the FWPP protocol

In the protocol in Ref. [16], the transmission is managed in batches of N EPR pairs. One advantage of a block transmission scheme is that we can check the security of the transmission by measuring some of the photons in the first step, where both Alice and Bob contain a particle sequence at hand, which means that an eavesdropper has no access to the first particle sequence, and then no information will be leaked to her whatever she has done to the second particle sequence. Following this method using block transmission, the FWPP scheme is proposed.

Suppose that the message to be transmitted is a sequence $x^N = (x_1,...,x_N)$, where $x_i \in \{0,1\}$, $i = 1,2,...,N$.

Define

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{1}$$

$$|\psi\rangle_5 = \frac{1}{2}(|00000\rangle + |00111\rangle + |11010\rangle + |11101\rangle). \tag{2}$$

Now let us give an explicit process for the FWPP.

(Step (S)1) Bob prepares a large enough number of Bell states, inserts enough five-particle cluster states and dispenses the Bell states.

Bob prepares a large enough number (N) of Bell states $|\Phi^+\rangle$ in sequence. He extracts all the first particles in the Bell states and forms a series of A particles (the travel qubits) in order. The remainder of the particles in the Bell states form a series of B particles (the home qubits) in order. These particles are used to transmit a secure message, and this step corresponds to the message mode in the original ping-pong protocol.

Bob prepares a large number ($cN/(1-c)$) of five-particle cluster states $|\psi\rangle$, of which the last two qubits are contained by himself, while the first three qubits form a series of C particles in order. These particles are used to detect eavesdropping, and this step corresponds to the control mode in OPP. Here, c expresses the probability of the control mode in the OPP. Note that the C particles includes $3cN/(1-c)$ qubits.

Bob inserts the decoy photons [12, 13] C to the A particles randomly. So a new sequence, A, is produced, but only Bob knows the positions of the decoy photons.

Bob stores the B particles and sends the A particles to Alice.

(S2) The detection of eavesdropping.

After Alice receives the A particles, Bob tells her the positions where the decoy photons are located. Alice measures the decoy photons extracted from the A particles and compares the measurement performed by Bob through a public channel. If there is no eavesdropper, every result should be in the five-particle cluster state $|\psi\rangle$, they continue to execute the next step (S3) and the FWPP protocol keeps on. Otherwise, the communication is interrupted and the FWPP protocol is switched to (S1).

(S3) Alice and Bob measure their particles with Z-basis, respectively.

Alice discards the decoy photons and measures the remaining A particles with Z-basis $B_{\rm Z} = \{|0\rangle, |1\rangle\}$ in order, and can form a series of classical numbers $C_{\rm A}$ in order. Bob also measures his B particles with Z-basis $B_{\rm Z} = \{|0\rangle, |1\rangle\}$ in order, and can form a series of classical numbers $C_{\rm B}$ in order. In the ideal cases, $C_{\rm A}$ is the same as $C_{\rm B}$.

(S4) Alice encrypts her secure message with the classical XOR operation and publicly broadcasts her encrypted message.

Suppose that Alice's secure message is a series of classical "0" or "1" numbers C_S in order. She encrypts her secure message C_S with C_A bit by bit using the classical XOR operation in order:

$$C_S \text{ XOR } C_A \rightarrow C_E. \tag{3}$$

The series of encrypted message is C_E. Alice publicly broadcasts the encrypted message C_E.

(S5) Bob decrypts Alice's secure message with the classical XOR operation.

After receiving Alice's secure message C_E, Bob decrypts Alice's secure message C_E with C_B bit by bit using the classical XOR operation in the same order as Alice, and can get Alice's secure message C_S.

(S6) The FWPP protocol is ended.

2.2 An example of the FWPP protocol

(S1) Bob prepares a large-enough number of Bell states, inserts enough five-particle cluster states, and dispenses the Bell states.

Suppose that Bob prepares four Bell states $|\Phi^+\rangle$, and a five-particle cluster state $|\psi\rangle$.

(S2) The detection of eavesdropping.

(Here the detection of eavesdropping is the same as (S2) in the process of the FWPP protocol and will not be discussed.)

(S3) Alice and Bob measure their particles with Z-basis, respectively.

Suppose that Alice's measured result is C_A= "0101", and Bob's measured result is also C_B= "0101".

(S4) Alice encrypts her secure message with the XOR operation and publicly broadcasts the encrypted message.

The classical XOR operation can be described as:

$$\begin{aligned} &0 \text{ XOR } 0 \rightarrow 0;\\ &0 \text{ XOR } 1 \rightarrow 1;\\ &1 \text{ XOR } 0 \rightarrow 1;\\ &1 \text{ XOR } 1 \rightarrow 0. \end{aligned} \tag{4}$$

Suppose that Alice's secure message is C_S="1001", she encrypts her secure message C_S with C_A bit by bit using the classical XOR operation in order, and can get C_E="1100":

$$\text{"1001" XOR "0101"} \rightarrow \text{"1100"}. \tag{5}$$

Alice publicly broadcasts the encrypted message C_E="1100".

(S5) Bob decrypts Alice's secure message with classical XOR operation.

After receiving Alice's secure message C_E, Bob decrypts Alice's secure message C_E with C_B bit by bit using the classical XOR operation in the same order of Alice:

$$\text{"1100" XOR "0101"} \rightarrow \text{"1001"}. \tag{6}$$

(S6) The FWPP protocol is ended.

2.3 The security analysis of the protocol

In the OPP, the author computes the maximal amount of the information ($I(d_{\text{lO}})$) that Eve can eavesdrop and the probability (d_{lO}) that Eve is detected. And the function $I(d_{\text{lO}})$ is provided.

When $p_0 = p_1 = \dfrac{1}{2}$,

$$I(d_{\text{lO}}) = -d_{\text{lO}}\log_2 d_{\text{lO}} - (1-d_{\text{lO}})\log_2(1-d_{\text{lO}}). \tag{7}$$

So the above method can be used to compare the efficiency of eavesdropping detection among the three protocols.

In the MPP, the maximal amount of the information ($I(d_{\text{lM}})$) that Eve can eavesdrop is

$$I(d_{\text{lM}}) = H\left(\frac{1-\sqrt{1-2d_{\text{lM}}}}{2}\right), \tag{8}$$

where

$$H(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{9}$$

and d_{lM} is the probability that Eve is detected.

Now, let us analyze the efficiency of the eavesdropping detection in the FWPP protocol. In order to gain the information that Alice operates on the travel qubits, Eve performs the unitary attack operation $\hat{E}$ on the composed system first. Then Alice performs the coding operation on the travel qubits. And finally, Eve performs a measurement on the composed system. Note that all the transmitted particles are sent together before the detection of eavesdropping. This method is different from OPP. Because Eve does not know which particles are used to detect eavesdropping, she can only perform the same attack operation on all the particles. As for Eve, the state of the travel qubits is indistinguishable from the complete mixture, so all the travel qubits are considered in either of the states $|0\rangle$ or $|1\rangle$ with equal probability p=0.5.

Generally speaking, suppose there is a group of decoy photons [12, 13] in five-particle cluster states $|\psi\rangle$, and we suppose that after performing the attack operation $\hat{E}$, the states $|0\rangle$ and $|1\rangle$ become

$$|\varphi_0'\rangle = \hat{E}\otimes|0x\rangle = \alpha|0x_0\rangle + \beta|1x_1\rangle, \tag{10}$$

$$|\varphi_1'\rangle = \hat{E}\otimes|1x\rangle = m|0y_0\rangle + n|1y_1\rangle, \tag{11}$$

where $|x_i\rangle$ and $|y_i\rangle$ are the pure ancillary states de-

termined by $\hat{E}$ uniquely, and

$$|\alpha|^2+|\beta|^2=1, \quad |m|^2+|n|^2=1. \tag{12}$$

Then let us compute the detection probability. After attack by Eve, the state of the composed system becomes

$$\begin{aligned}|\psi\rangle_{\rm Eve} =& E\otimes E\otimes E\otimes I\otimes I\left[\frac{1}{2}\left(|0x0x0x0x0x\rangle+|0x0x1x1x1x\rangle+|1x1x0x1x0x\rangle+|1x1x1x0x1x\rangle\right)\right]\\ =& \frac{1}{2}\left[(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes|00\rangle\right.\\ &+(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes|11\rangle\\ &+(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(\alpha|0x_0\rangle+\beta|1x_1\rangle)\otimes|10\rangle\\ &\left.+(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes(m|0y_0\rangle+n|1y_1\rangle)\otimes|01\rangle\right].\end{aligned} \tag{13}$$

Obviously, when the measurement is performed on the decoy photons, the probability without eavesdroppers is

$$p(|\psi\rangle_{\rm Eve})=\frac{1}{4}\left(|\alpha^3|^2+|\alpha^2 n|^2+|\alpha n^2|^2+|n^3|^2\right). \tag{14}$$

So the lower bound of the detection probability ($d_{\rm lFW}$) is

$$d_{\rm lFW}=1-p(|\psi\rangle_{\rm Eve}). \tag{15}$$

Now, let us analyze how much information Eve can gain maximally when there is no decoy mode. Suppose $|\alpha|^2=a,\ |\beta|^2=b,\ |m|^2=s,\ |n|^2=t$, where a, b, s and t are positive real numbers and $a+b=s+t=1$. Then

$$\begin{aligned}d_{\rm lFW} =& 1-\frac{1}{4}\left(|\alpha^3|^2+|\alpha^2 n|^2+|\alpha n^2|^2+|n^3|^2\right)\\ =& 1-\frac{1}{4}(a^3+a^2t+at^2+t^3).\end{aligned} \tag{16}$$

In the case of $p_0=p_1=0.5$, when Bob sends $|0\rangle$ to Alice, the maximal amount of information is equal to the Shannon entropy of a binary channel,

$$I_0=-a\log_2 a-(1-a)\log_2(1-a)=H(a). \tag{17}$$

Then assume that Bob sends $|1\rangle$ rather than $|0\rangle$. The above security analysis can be done in full analogy, resulting in the same crucial relations. The maximal amount of information is equal to the Shannon entropy of a binary channel,

$$I_1=-t\log_2 t-(1-t)\log_2(1-t)=H(t). \tag{18}$$

So the maximal amount of information that Eve can obtain is

$$I=\frac{1}{2}(I_0+I_1)=\frac{1}{2}[H(a)+H(t)]. \tag{19}$$

After some simple mathematical calculations, when $a=t$, we can get

$$d_{\rm lFW}=1-a^3, \tag{20}$$

and the maximum I is

$$I(d_{\rm lFW})=H(\sqrt[3]{1-d}). \tag{21}$$

The above analysis shows that functions $I(d_{\rm lO})$, $I(d_{\rm lM})$ and $I(d_{\rm lFW})$ have similar algebraic properties. If Eve wants to gain the full information (I=1), the probabilities of eavesdropping detection are $d_{\rm lO}$ (I=1)=0.5 and $d_{\rm lM}$ (I=1)=0.5 in the OPP and the MPP, separately, and the probability of eavesdropping detection is $d_{\rm lFW}$ (I=1)=0.89 in this paper.

In order to compare the three functions, Fig. 1 is given. As Fig. 1 shows, if Eve wants to gain the same amount of information, she must face a larger detection probability in the FWPP than the other two. This also shows that the FWPP is more secure than the other two.

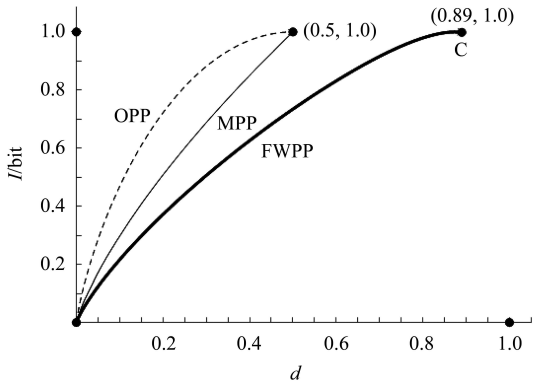

Fig. 1. The comparison of the three detection results.

The dotted line expresses the function $I(d_{\rm lO})$ in the OPP, the thin line expresses the function $I(d_{\rm lM})$ in the MPP, and the thick line expresses the function $I(d_{\rm lFW})$ in the FWPP. Obviously, if Eve wants to get the same amount of information, she must encounter the higher detection efficiency in FWPP. Also, if there

is the same detection efficiency, Eve will eavesdrop less information.

Taking into account the probability c of the control mode, the effective transmission rate, i.e. the number of message bits per protocol run, is $1-c$, which is equal to the probability for a message transfer. So, if Eve wants to eavesdrop one message transfer without being detected, the probability for this event is

$$s(c,d) = (1-c)+c(1-d)(1-c)+c^2(1-d)^2(1-c) +\ldots = \frac{1-c}{1-c(1-d)}. \quad (22)$$

Then the probability of successful eavesdropping $I = nI(d)$ bits is $s(I,c,d) = s(c,d)^{I/I(d)}$. So

$$s(I,c,d) = \left(\frac{1-c}{1-c(1-d)}\right)^{I/I(d)}, \quad (23)$$

where

$$I(d) = H(\sqrt[3]{1-d}). \quad (24)$$

In the limit $I \to \infty$ (a message or key of infinite length) we have $s \to 0$, so the presented protocol in this paper is asymptotically secure. If the security of the quantum channel is ensured, the protocol is completely secure. For example, a choice of the control mode is c=0.5. In Fig. 2, we have plotted the eavesdropping success probability as a function of the information gain I, for c=0.5 and for different detection probabilities d, which Eve can choose. Note that for d <0.5, Eve only gets part of the message right and does not even know which part.

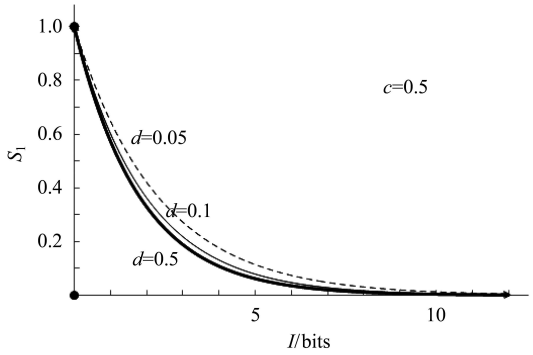

Fig. 2. Eavesdropping success probability as a function of the maximal eavesdropped information, plotted for different detection probabilities, d.

In steps (S4) and (S5) of the FWPP protocol, the secure message is encrypted bit by bit with the classical XOR operation and publicly broadcasts the encrypted message, which can get OTP level security. So the FWPP protocol is secure.

3 Conclusions

In the FWPP protocol presented in this paper, the security message can be securely transmitted to the receiver, and any useful message will not leak to the potential eavesdroppers. Compared with the OPP protocol and the MPP protocol, the FWPP protocol has the following differentia.

(1) The eavesdropper's detection method, using the five-particle cluster state in the FWPP protocol, is similar to the method using the Bell state in MPP.

(2) In the FWPP protocol, Alice performs the classical XOR operation on the secret message and then publicly broadcasts the encrypted message.

(3) The localization of FWPP is that the Bell state $|\Phi^+\rangle$ will collapse and cannot be reused later, after the protocol; while in the OPP protocol and the MPP protocol, the Bell state can be reused.

In summary, we introduced in full detail a novel QSDC protocol based on a five-particle cluster state and the classical XOR operation. The security of the protocol is also analyzed, and detection probability approaches 89%, which is more secure than that in Ref. [19]. In future, the security of the other QSDC protocol and its improvement will be studied.

References

1 Bennett C H, Brassard G. Proc. IEEE Int. Conf. on Computer, Systems, and Signal Processing, Bangalore, India. IEEE, New York, 1984. 175–179
2 Bennett C H, Brassard G, Crepeau C et al. Phys. Rev. Lett., 1993, **70**: 1895–1899
3 Bouwmeester D, Pan J W, Mattle K et al. Nature, 1997, **390**: 575–579
4 Bouwmeester D, Mattle K, Pan J W et al. Appl. Phys. B, 1998, **67**: 749–752
5 Kim Y H, Kulik S P, Shih Y. Quantum Electronics and Laser Science Conference, 2001. 223–226
6 Prakash H. International Conference on Emerging Trends in Electronic and Photonic Devices & Systems, 2009. 18–23
7 Furusawa A. Quantum Electronics and Laser Science Conference, 2010
8 Bennett C H, Wiesner S J. Phys. Rev. Lett., 1992, **69**: 2881–2884
9 Mattle K, Weinfurter H, Kwiat P G et al. Phys. Rev. Lett., 1996, **76**: 4656–4659
10 Hillery M, Buzek V, Berthiaume A. Phys. Rev. A, 1999, **59**: 1829–1834
11 Cleve R, Gottesman D, Lo H K. Phys. Rev. Lett., 1999, **83**: 648–651
12 LI Chun-Yan, ZHOU Hong-Yu, Wang Yan et al. Chinese Physics Letters, 2005, **22**(5): 1049–1052
13 LI Chun-Yan, LI Xi-Han, DENG Fu-Guo et al. Chinese Physics Letters, 2006, **23**(11): 2896
14 Beige A, Englert B G, Kurtsiefer C et al. Acta Phys. A, 2002, **101**: 357–370
15 Boström K, Felbringer T. Phys. Rev. Lett., 2002, **89**: 187902
16 LONG Gui-Lu, LIU Xiao-Shu. Phys. Rev. A, 2002, **65**(3): 032302
17 DENG Fu-Guo, LONG Gui-Lu, LIU Xiao-Shu. Phys. Rev. A, 2003, **68**: 042317
18 DENG Fu-Guo, LONG Gui-Lu. Phys. Rev. A, 2004, **69**: 052319
19 GAO Fei, GUO Fen-Zhuo, WEN Qiao-Yan et al. Sci. China Ser G-Phys Mech. Astron, 2009, **39**(2): 161–166 (in Chinese)
20 LONG Gui-Lu, DENG Fu-Guo, WANG C et al. Front. Phys. China, 2007, **2**(3): 251–272
21 CAi Qing-Yu, LI Bai-Wen. Chinese Physics Letters, 2004, **21**: 601–603
22 LIANG Hao, CHUAN Wang, LONG Gui-Lu. J. Phys. B: At. Mol. Opt. Phys., 2010, **43**: 125502
23 CAI Qing-Yu, LI Bai-Wen. Phys. Rev. A, 2004, **69**: 054301
24 GAO Ting, YAN Feng-Li, WANG Zhi-Xi. Chinese Physics Letters, 2005, **22**: 2473–2476
25 WANG Chuan, DENG Fu-Guo, LONG Gui-Lu. Optical Communications, 2005, **253**: 15–20
26 LI Xi-Han, DENG Fu-Guo, ZHOU Hong-Yu. Phys. Rev. A, 2006, **74**: 054302
27 LI Xi-Han, LI Chun-Yan, DENG Fu-Guo et al. Chinese Physics Letters, 2007, **16**: 2149–2153
28 KAI Wen, LONG Gui-Lu. International Journal of Quantum Information, 2010, **8**(4): 697
29 MAN Zhong-Xiao, XIA Yun-Jie, Nguyen B A. J Phys. B-At Mol. Opt. Phys., 2006, **39**: 3855–3863
30 MAN Zhong-Xiao, XIA Yun-Jie. Chinese Physics Letters, 2006, **23**: 1680–1682
31 JIN Xing-Ri, JI Xin, ZHANG Ying-Qiao et al. Phys. Lett. A, 2006, **354**: 67–70
32 MAN Zhong-Xiao, XIA Yun-Jie. Chinese Physics Letters, 2007, **24**: 15–18
33 CHEN Yan, MAN Zhong-Xiao, XIA Yun-Jie. Chinese Physics Letters, 2007, **24**: 19–22
34 GU Bin, PEI Shi-Xin, SONG Biao et al. Science in China Series G-Physics Mechanics Astronomy, 2009, **52**(12): 1913–1918