Journal of Southeast University (English Edition) Vol. 26, No. 4, pp. 532 – 536 Dec. 2010 ISSN 1003—7985

Revised quantum direct communication scheme with mutual authentication

Liu Wenjie[1,2] Chen Hanwu[1] Xu Juan[1] Liu Zhihao[1]

([1] School of Computer Science and Engineering, Southeast University, Nanjing 210096, China)
([2] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China)

Abstract: Based on mutual authentication and dense coding, a novel revised efficient quantum direct communication scheme is proposed. It is composed of two phases: the quantum state distribution process and the direct communication process. The purpose of the former is to authenticate Trent and users to each other, and let the two legitimate users (Alice and Bob) safely share the Bell states. While the latter aims to make direct communication to transmit a secret message between Alice and Bob. In order to prevent from Eve's eavesdropping as well as to authenticate each other simultaneously, a decoy photon checking technique is applied. Compared with other analogous protocols, the quantum state distribution process is more simple and feasible and the proposed scheme is more efficient; i. e., the total efficiency is almost 100%. Security analysis shows that the proposed scheme is secure against the eavesdropping attacks, the impersonation attacks, and some special Trent's attacks, including the attacks by using different initial states.

Key words: quantum direct communication; mutual authentication; decoy-photon checking; impersonation attack; special Trent's attack

With the development of quantum technology, quantum cryptography has become a hot research topic in the field of information security. As an important branch of quantum cryptography, quantum direct communication (QDC) has attracted much attention [1-6]. With the principles in quantum mechanics, such as no-cloning theorem, uncertainty principle, entanglement, etc., QDC provides some interesting ways for secure communication.

Recently, Lee et al. [7] proposed two QDC protocols with authentication (LLY protocols), which first introduced the authentication mechanism to resist the impersonators' attacks. However, Zhang et al. [8] indicated that these protocols were insecure against the authenticator's (Trent's) attacks, and put forward two modified protocols (ZLW protocols) by utilizing the Pauli σ_z operation instead of the original bit-flip operation σ_x. And we put forward two efficient protocols (LCL protocols) by using four Pauli operations $\{I, \sigma_x, i\sigma_y, \sigma_z\}$ in Ref. [9]. Qin et al. [10] pointed out that in LCL protocols Trent and the eavesdropper Eve can elicit half of the information about the secret message from the public declaration. Simultaneously, Yen et al. [11] also pointed out that ZLW protocols are still insecure when Trent prepares different initial states, and presented a new protocol with mutual authentication and entanglement swapping (YHG protocol) to make up for this kind of security leakage. However, it wastes too much quantum state resource and the efficiency is a little low. The motivation of this paper is to promote the efficiency and guarantee the security against all kinds of known attacks.

Received 2010-04-08.

Biographies: Liu Wenjie(1979—), male, doctor, lecturer, wenjiel@163.com; Chen Hanwu (corresponding author), male, doctor, professor, hw_chen@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 60873101), the Natural Science Foundation of Jiangsu Province (No. BK2008209), the Research Foundation of Nanjing University of Information Science and Technology (No. 20080298).

Citation: Liu Wenjie, Chen Hanwu, Xu Juan, et al. Revised quantum direct communication scheme with mutual authentication [J]. Journal of Southeast University(English Edition), 2010, 26(4): 532 – 536.

1 Preliminaries

1.1 Some notations

The quantum-mechanical analog of the classical bit is the qubit, a two-level quantum system, and it can be written as

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

where $|0\rangle$ represents the horizontal polarization; $|1\rangle$ represents the vertical polarization; α and β are complex numbers that specify the probability amplitudes of the corresponding states, and $|\alpha|^2 + |\beta|^2 = 1$. $\{|0\rangle, |1\rangle\}$ consists of the rectilinear orthogonal basis, Z-basis, and the diagonal orthogonal basis, namely X-basis, is composed of $\{|+\rangle, |-\rangle\}$, where $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$.

In this paper, we utilize the following four Bell states (i. e., EPR pairs) as the carrier of imformation:

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),\ |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{2}$$

Besides, four Pauli unitary operations $\{U_0, U_1, U_2, U_3\}$ and a Hadamard operation H are used to encode messages or authenticate the anticipators. They are defined as

$$\left.\begin{aligned} U_0 &= I = |0\rangle\langle 0| + |1\rangle\langle 1| \\ U_1 &= \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| \\ U_2 &= i\sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0| \\ U_3 &= \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned}\right\} \tag{3}$$

and

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| - |1\rangle\langle 1| + |0\rangle\langle 1| + |1\rangle\langle 0|) \tag{4}$$

1.2 Generation of authentication keys

Similar to that in Ref. [7], a one-way hash function h is used to generate the authentication keys of the users in our protocol.

$$h: \{0, 1\}^{*} \times \{0, 1\}^{l} \rightarrow \{0, 1\}^{c} \tag{5}$$

where the asterisk $*$, l and c represent an arbitrary length, the length of a counter, and a fixed number, respectively. Thus the user's authentication key can be expressed as $AK_{user} = h(ID_{user}, c_{user})$, where c_{user} is the counter of calls on the hash function.

In our scheme, we denote the authentication keys of Alice and Bob as $AK_A = h(ID_A, c_A)$, $AK_B = h(ID_B, c_B)$. And the users' identity number $ID_A(ID_B)$ is only known to Trent besides Alice (Bob).

2 Revised QDC Scheme with Mutual Authentication

Inspired from the YHG protocol, we improved the LCL protocol and proposed a novel revised QDC schema (RQDC), where the Bell states were utilized as the message carriers instead of the GHZ states, and Trent acted as a "genuine" authenticator who only authenticated the users and would not directly take part in the message communication. In order to prevent the eavesdroppers from stealing the secret message as well as authenticate each other, a simple and feasible decoy-photon checking technology is applied.

The RQDC is composed of two parts: the quantum state distribution process with mutual authentication and the direct communication process with identity authentication and dense coding.

2.1 Quantum state distribution process with mutual authentication

The purpose of this process is to authenticate Trent and users for each other, and let the two legitimate users (Alice and Bob) safely share the Bell states. Suppose that Alice wants to send a message to Bob, then the brief procedures are described as follows (see Fig. 1):

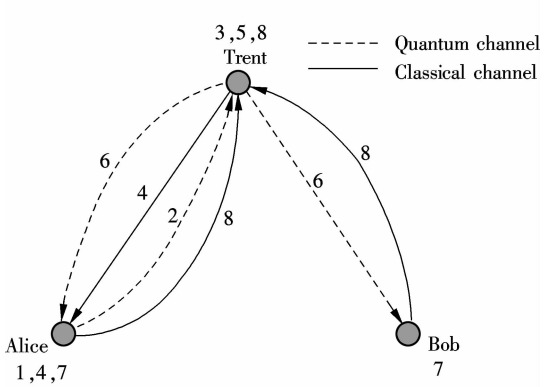

Fig. 1 Procedures of the quantum state distribution process

1) Alice prepares an ordered v-length decoy photon sequence, namely a V_A sequence, each of which is randomly chosen in $\{|0\rangle, |1\rangle\}$. V_A will be used for verifying Trent's identity, and the length $v \gg l_A$, where l_A is the length of AK_A. According to AK_A, Alice performs an operation H or I on each particle of V_A sequence,

$$V'_{Ai} = \begin{cases} HV_{Ai} & AK_{Ai} = 1 \\ IV_{Ai} & AK_{Ai} = 0 \end{cases} \quad 1 \leqslant i \leqslant v \tag{6}$$

Since the number v is normally greater than the length l_A of AK_A, the key bits of AK_A is regenerated by ID_A and a new c_A for operation performing. The process is repeated until all v particles in V_A sequence are encoded. The new sequence is named V'_A sequence.

2) Alice then sends V'_A sequence to Trent.

3) After receiving V'_A sequence, Trent performs a reverse operation of Eq. (6) according to AK_A. If this "Trent" is true, he knows the value of AK_A, so the states of V'_A will return to its initial states of V_A. Trent then measures these encoded decoy photons in the Z-basis $\{|0\rangle, |1\rangle\}$, and publishes the outcomes to Alice.

4) Alice is going to authenticate Trent as well as check the presence of Eve. She compares her initial states in the V_A sequence with Trent's outcomes. If they have a sufficiently large number of results that are the same, Alice will accept that Trent is true and proceeds with the following steps. Otherwise, she just stops the procedure.

5) Trent prepares the Bell states for Alice and Bob. At first, Trent chooses an ordered N Bell state, each of which is one of the Bell states defined in Eq. (2). For example, the state is $|\varphi\rangle = |\phi^{+}\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)_{AB}$, where the subscripts A and B represent the two particles of the Bell state. Trent divides particles A and B into S_A and S_B sequences. Simultaneously, Trent also prepares three ordered v-length decoy photon $\{|0\rangle, |1\rangle\}$ sequences, namely, V_{TA}, V_{AB} and V_{TB}. He then encodes the V_{TA}, V_{AB} and V_{TB} sequences according to AK_A, AK_B and AK_B, respectively, as described in step 1). It should be noted that $N \gg v \gg l_i$, where i = A, B. Finally, Trent inserts V_{TA} and V_{AB} into S_A, V_{TB} into S_B with random positions, and keeps these positions secretly.

6) Trent sends encoded $V_{TA} \parallel V_{AB} \parallel S_A$ and $V_{TB} \parallel S_B$ sequences to Alice and Bob, respectively.

7) After Alice and Bob make sure that they have received $V_{TA} \parallel V_{AB} \parallel S_A$ and $V_{TB} \parallel S_B$, respectively, Trent will authenticate Alice as well as check the security of the channels. Taking Alice as an example, Trent tells Alice the positions of V_{TA}, and Alice decodes V_{TA} by the operations $\{H, I\}$ according to AK_A as Trent did in step 4). If this "Alice" is the real user Alice, then the state of each decoy photons in V_{TA} will return to Alice's initial state. And then she measures those decoy photons of V_{TA} in the Z-basis. At the same time, Bob performs the same procedure on V_{TB} with AK_B as Alice does.

8) Alice and Bob tell Trent their outcomes over the public channel, respectively. Then, Trent can evaluate the error rate by comparing his initial states of $V_{TA}(V_{TB})$ with Alice's (Bob's) outcomes. If the error rate exceeds the expectation, they abort the procedure. Otherwise, Trent confirms that Alice (Bob) is legitimate and the quantum channel is safe.

In the process, Trent is verified by Alice in step 4); Alice and Bob are also verified in step 8). If the error rates are all under the expectation, the EPR pairs (Bell states) are safely distributed to Alice and Bob, and they continue the next phase, direct communication process.

2.2 Quantum direct communication process with identity authentication

After the quantum state distribution process, the Bell states are safely shared between Alice and Bob, and they make direct communication to transmit the secret message. It should be noted that Trent will do nothing but verify the receiver's identity in this process. The detailed procedures are described as follows (see Fig. 2):

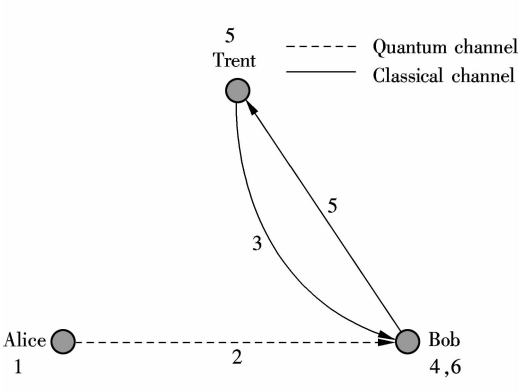

Fig. 2 Procedures of quantum direct communication process among Trent, Alice and Bob

1) The remaining particles in Alice's hand consist of the $V_{AB} \parallel S_A$ sequence. Alice encodes the secret message on S_A by performing operations as follows: $00 \rightarrow U_0$, $01 \rightarrow U_1$, $10 \rightarrow U_2$, and $11 \rightarrow U_3$.

$$\left.\begin{aligned} U_0 \mid \varphi\rangle &= I_A \mid \varphi\rangle = \frac{1}{\sqrt{2}}(\mid 00\rangle_{AB} + \mid 11\rangle_{AB}) = \mid \phi^+\rangle_{AB} \\ U_1 \mid \varphi\rangle &= \sigma_{xA} \mid \varphi\rangle = \frac{1}{\sqrt{2}}(\mid 10\rangle_{AB} + \mid 01\rangle_{AB}) = \mid \psi^+\rangle_{AB} \\ U_2 \mid \varphi\rangle &= i\sigma_{yA} \mid \varphi\rangle = \frac{1}{\sqrt{2}}(\mid 01\rangle_{AB} - \mid 10\rangle_{AB}) = \mid \psi^-\rangle_{AB} \\ U_3 \mid \varphi\rangle &= \sigma_{zA} \mid \varphi\rangle = \frac{1}{\sqrt{2}}(\mid 00\rangle_{AB} - \mid 11\rangle_{AB}) = \mid \phi^-\rangle_{AB} \end{aligned}\right\} \quad (7)$$

2) Alice sends all the particles to Bob.

3) After Bob receives the $V_{AB} \parallel S_A$ sequence, Trent announces the positions of V_{AB}. Note that Trent can compute the new positions of V_{AB} since V_{TA} has been drawn out from the initial sequence Trent prepared in the previous process.

4) According to AK_B and the positions of V_{AB}, Bob performs the corresponding H or I operations on the particles of V_{AB}. If this "Bob" is the real receiver Bob, then the states of V_{AB} sequence will recover their initial states. Finally, Bob measures V_{AB} in the Z-basis.

5) Bob tells Trent the outcomes of V_{AB}, and Trent verifies Bob's identity as well as checks the channel security. Trent compares the outcomes and the original states he prepared, and evaluates the error rate. If the error rate is under the expectation, it shows that the receiver Bob is true and the transmission is safe; thus Alice and Bob continue the next step. Otherwise, they abort the process, and restart the communication.

6) Bob performs Bell basis measurement on pairs of particles consisting of S_A and S_B sequences. From the measurement outcomes, Bob can deduce the probable operations performed by Alice (see Tab. 1).

Tab. 1 Relationships of Alice's operation, secret message, and Bob's measurement in direct communication process

Bob's measurement	Alice's operation	Secret message
$\mid \phi^+\rangle_{AB}$	$U_0(I_A)$	00
$\mid \psi^+\rangle_{AB}$	$U_1(\sigma_{xA})$	01
$\mid \psi^-\rangle_{AB}$	$U_2(i\sigma_{yA})$	10
$\mid \phi^-\rangle_{AB}$	$U_3(\sigma_{zA})$	11

For example, if Bob's measurement outcome is $\mid \psi^+\rangle$, Bob can infer that Alice has performed a $U_1(\sigma_x)$ operation; that is, the bits of message are 01.

3 Security and Efficiency Analysis

3.1 Security analysis

● **Eavesdropping attacks** In both the quantum state distribution process and the direct communication process, the present scheme exploits the ideas of decoy photon checking techniques to ensure the security of the process. Because these decoy photons, such as V_{TA}, V_{AB} and V_{TB}, will be performing H or I operations according to the authentication keys (i. e., AK_A, AK_B and AK_B). It can be viewed that these photons are produced randomly in one of the two bases, i. e., Z-basis $\{\mid 0\rangle, \mid 1\rangle\}$ or X-basis $\{\mid +\rangle, \mid -\rangle\}$, which is essentially the same as that in the BB84 QKD scheme[12]. The difference between this scheme and the BB84 QKD scheme is that, the receiver measures each particle randomly using Z-basis or X-basis in the BB84 QKD scheme, while in our scheme participators measure each decoy-photon particle using the Z-basis after the operations according to the authentication key. BB84 has been proven unconditionally secure against all kinds of the eavesdropper Eve's attacks[13-14]; therefore, our scheme is also secure against the eavesdropping attacks.

● **Impersonation attacks** By introducing the mutual authentication mechanism, i. e., steps 4) and 7) in the quantum state distribution process as well as step 5) in the direct communication process, the RQDC ensures the participators (Alice, Bob and Trent) are legitimate, and no impersonator can imitate users to steal message. That is to say, our RQDC scheme holds the same resistibility as that in LLY protocols against the impersonator attack or man-in-the-middle attack.

● **Some special Trent's attacks** First, we consider the Trent's attack proposed by Zhang et al.[8] (ZLW attack). In this kind of attack, Trent intercepts all the particles transmitted from Alice to Bob, and attempts to make a certain measurement in the direct communication process for obtaining the secret message. Since there is no redundant particle of each EPR pairs to be kept in Trent's hand, the RQDC is immune to this kind of attack.

As analyzed in Ref. [10], half of the information is leaked from the public declaration in our original protocols[9]. Through guaranteeing that Trent keeps out of the direct communication process, our RQDC avoids this flaw.

Finally, we take account of another special Trent's attack by using different initial states, which is proposed by Yen et

al.[11] (YHG attack). Under this attack, Trent prepares different initial states $1/\sqrt{2}(|+0\rangle + |-1\rangle)$ (noted as $|\varphi'\rangle$) instead of $1/\sqrt{2}(|00\rangle + |11\rangle)$, and measures the transmitted qubits with Z-basis (or X-basis) in the direct communication process to gain some information about the message. In the RQDC, the Bell state before transmission is one of the following:

$$|\varphi''\rangle = \begin{cases} U_0|\varphi'\rangle = \frac{1}{\sqrt{2}}(|+0\rangle_{AB} + |-1\rangle_{AB}) = \\ \quad \frac{1}{\sqrt{2}}(|0+\rangle_{AB} + |1-\rangle_{AB}) \\ U_1|\varphi'\rangle = \frac{1}{\sqrt{2}}(|+0\rangle_{AB} - |-1\rangle_{AB}) = \\ \quad \frac{1}{\sqrt{2}}(|0-\rangle_{AB} + |1+\rangle_{AB}) \\ U_2|\varphi'\rangle = \frac{1}{\sqrt{2}}(|-0\rangle_{AB} + |+1\rangle_{AB}) = \\ \quad \frac{1}{\sqrt{2}}(|0+\rangle_{AB} - |1-\rangle_{AB}) \\ U_3|\varphi'\rangle = \frac{1}{\sqrt{2}}(|-0\rangle_{AB} - |+1\rangle_{AB}) = \\ \quad \frac{1}{\sqrt{2}}(|0-\rangle_{AB} - |1+\rangle_{AB}) \end{cases} \quad (8)$$

From Eq. (8), we can see that Trent cannot obtain any information about the secret message by performing the Z-basis (or X-basis) measurement. That is, the present scheme is immune to the YHG attack.

3.2 Efficiency analysis

Recently, Li et al.[15] presented a useful efficiency coefficient to describe the total efficiency of a quantum communication: $\eta_{total} = m_u/(q_t + b_t)$, where m_u, q_t, b_t are the numbers of messages transmitted, the total qubits used and the classical bits exchanged, respectively. In the RQDC, the anticipators do not need classical information except for decoy-photon checking, and two bits of quantum information (i.e., a two-qubit Bell state) carry three bits of the secret message; that is, $m_u = 2$, $q_t = 2$ and $b_t = 0$. Then, $\eta_{our} = 2/(2+0) = 100\%$. In this way, the efficiency of other analogous protocols also can be calculated (see Tab. 2).

It is clear that our RQDC is more efficient than the other analogous protocols.

Tab. 2 Security and efficiency of other analogous protocols and our protocol

Protocol name	Impersonation attacks	ZLW attacks	YHG attack	Total efficiency/%
LLY	Yes	No	No	25
ZLW	Yes	Yes	No	25
LCL	Yes	No	Yes	50
YHG	Yes	Yes	Yes	25 or 50
RQDC	Yes	Yes	Yes	100

4 Conclusion

Based on mutual authentication and decoy-photon checking, a novel revised efficient QDC scheme is presented. In contrast to our original scheme (i.e., LCL protocol), the RQDC expresses powerful security, which is immune to present attacks. On the other hand, the RQDC shows outstanding efficiency, which is obviously more efficient than the analogous protocols (see Tab. 2). Compared with the YHG protocol, the quantum state distribution process is more simple and feasible.

References

[1] Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with single-photon two-qubit states [J]. *J Phys A: Math Gen*, 2002, **35**(28): 407 - 413.

[2] Boström K, Felbinger T. Deterministic secure direct communication using entanglement [J]. *Phys Rev Lett*, 2002, **89**(18): 187902.

[3] Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block [J]. *Phys Rev A*, 2003, **68**(4): 042317.

[4] Deng F G, Long G L. Secure direct communication with a quantum one-time pad [J]. *Phys Rev A*, 2004, **69**(5): 052319.

[5] Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state [J]. *Opt Commun*, 2005, **253**(1): 15 - 20.

[6] Lu X, Ma Z, Feng D G. Quantum secure direct communication using quantum Calderbank-Shor-Steane error correcting codes [J]. *Journal of Software*, 2006, **17**(3): 509 - 515. (in Chinese)

[7] Lee H, Lim J, Yang H. Quantum direct communication with authentication [J]. *Phys Rev A*, 2006, **73**(4): 042305.

[8] Zhang Z J, Liu J, Wang D, et al. Comment on "quantum direct communication with authentication" [J]. *Phys Rev A*, 2007, **75**(4): 026301.

[9] Liu W J, Chen H W, Li Z Q, et al. Efficient quantum secure direct communication with authentication [J]. *Chin Phys Lett*, 2008, **25**(7): 2354 - 2357.

[10] Qin S J, Wen Q Y, Meng L M, et al. High efficiency of two efficient QSDC with authentication is at the cost of their security [J]. *Chin Phys Lett*, 2009, **26**(2): 020312.

[11] Yen C A, Horng S J, Goan H S, et al. Quantum direct communication with mutual authentication [J]. *Quantum Information and Computation*, 2009, **9**(5): 0376 - 0394.

[12] Bennett C H, Brassard G. Quantum cryptography: public-key distribution and tossing [C]//*Proc of IEEE International Conference on Computers, Systems and Signal Processing*. Bangalore, India, 1984: 175 - 179.

[13] Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances [J]. *Science*, 1999, **283**(5410): 2050 - 2056.

[14] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol [J]. *Phys Rev Lett*, 2000, **85**(2): 441 - 444.

[15] Li X H, Deng F G, Li C Y, et al. Deterministic secure quantum communication without maximally entangled states [J]. *J Kerean Phys Soc*, 2006, **49**(4): 1354 - 1360.

一种基于互认证的改进型量子直接通信协议

刘文杰[1,2] 陈汉武[1] 许 娟[1] 刘志昊[1]

([1] 东南大学计算机科学与工程学院,南京 210096)
([2] 南京信息工程大学计算机与软件学院,南京 210044)

摘要:基于互认证和量子超密编码思想,提出了一种改进型量子直接通信协议. 该协议由量子态分发过程和直接通信过程 2 部分组成,前者的主要目的是实现分发者 Trent 与用户之间的相互认证,并让 2 个合法用户(Alice 和 Bob)共享 Bell 态;后者将进行 Alice 与 Bob 的量子直接通信,以实现两者的消息传递. 为了抵抗 Eve 窃听并同时进行相互身份认证,引入了一种诱骗光子检测方法. 与其他同类型协议相比,本协议的量子态分发过程显得更加简单和实用,并且协议本身也更加高效,总效率接近 100%. 安全分析表明,该协议可有效抵抗窃听攻击、伪装攻击及一些特殊的 Trent 攻击,包括采用不同初始态的 Trent 攻击.

关键词:量子直接通信;互认证;诱骗光子检测;伪装攻击;Trent 特殊攻击
中图分类号:TN918. 1