Journal of Computers Vol. 27, No. 3, 2016, pp. 33-40
doi:10.3966/199115592016102703004

TCP Three-Way Handshake Protocol based on Quantum Entanglement

Qin-Min Ma[1,2] Shou-Yin Liu[2] Xiao-jun Wen[1]

[1] Department Of Computer, Shenzhen Polytechnic, Shenzhen 518055, China
maqinmin@126.com

[2] College of Physical Science and Technology, Central China Normal University, Wuhan 430079, China
syliu@phy.ccnu.edu.cn

Received 1 July 2015; Revised 27 July 2015; Accepted 10 August 2015

Abstract. After analyzing the two defects existed in the TCP three-way handshake protocol, namely ACK frustration and SYN attack, we provide a revised TCP three-way handshake protocol using the quantum entanglement features, which moves the transmission of the third time handshake to the quantum entanglement channel instead of classic way. Instantaneity and unstoppable property of quantum information transmission thoroughly solves ACK frustration problem. Meanwhile length of timeout decreases by half, which greatly reduces the risk of server being attacked by SYN flood and improves TCP connection performance.

Keywords: EPR entangled state, quantum communication, quantum entanglement, three-way handshake protocol

1 Introduction

In computer network, reliable communication from end to end of both of the two Host s depends on transport layer for realization. Therefore, the transport layer is the core of the entire network architecture. TCP (Transmission Control Protocol) is a connection-oriented reliable communication protocol which operates in the transport layer based on Byte stream [1]. TCP hands the segment of transport layer to IP layer. However IP layer only tries to transmit as much as possible, and can not ensure reliability of data transmission. Therefore, TCP needs to provide assurance for itself. What TCP provides is a connection-oriented service, and the two sides involved in communication need to establish a reliable connection between them which, then is used to transmit the data. TCP applies three-way handshake protocol to ensure safety of the connection establishment process. There exists an unsurmountable problem of delay in network, which provides opportunity for attackers who can send many connection requests to the server in a short time, and easily conduct SYN flood attack to the server and cause the server to refuse to serve [2-3]. This is an unavoidable safety problem in front of computer network.

The new research achievement of entangled state in quantum mechanics provides a solution for this problem. For two microscopic particles, no matter how far they are from each other, the measurement to one of the particles will absolutely trigger changes to quantum state of the other particle [4]. This fantastic physical phenomenon is now leading people to find another easier way to solve some classical problems which can not be solved in conventional sense. The thesis combines with EPR (Einstein-Podolsky-Rosen) entangled state peculiar to quantum mechanics and transmission characteristics of quantum information to modify TCP three-way handshake protocol and propose the TCP three-way handshake protocol based on entanglement, which can greatly improve system safety and provide a new method to solve inherent defects of TCP/IP.

2 Classical TCP three-way handshake protocol

2.1 TCP segment data format

TCP is a connection-oriented protocol, and connection establishment and release are necessary processes in every connection-oriented communication. It is necessary to solve the following three problems in the connection establishing process:

(1) Make sure that both of the two communication parties clearly know the existence of the other party.

(2) The two parties should coordinate some parameters, such as sending and confirming sequence number, maximum segment length and maximum window size, etc.

(3) Can transport physical resources (such as size of buffer area, projects in connection table, etc.) for allocation.

All the above information is encapsulated in TCP segment in the format as shown in Fig.1, which is divided into head part and data. The former 20 bytes in the head part is necessary, and the latter 4N (N is integer) bytes are dispensable. Therefore, the minimum length of TCP head part is 20-Byte [5].

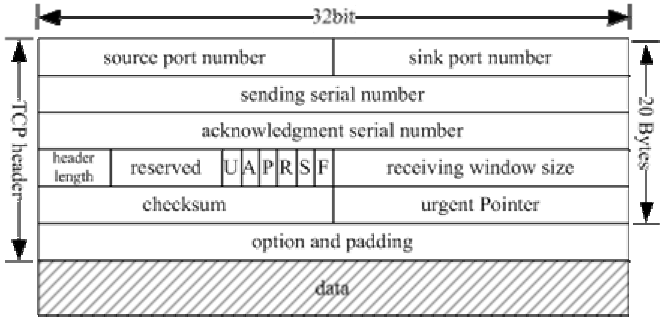


Fig. 1. Format of TCP segment

Sending sequence number is the number of the first byte of the data to be sent; and confirming sequence number is the byte number of the data which the other party is told to hope to receive. The field length of sending and confirming sequence number is 32bit, and one can number the 4GB data.

The UAPRSF in the figure are six identification bits, and their relationship with the three-way handshake is:

A: ACK bits, namely confirming identification bits. When ACK = 1, it represents the previous data received correctly, and then “receiving sequence number” has significance; when ACK = 0, “receiving sequence number” has no significance.

S: SYN bits, namely synchronization identification bits. When SYN = 1 and ACK = 0, it represents one connection request segment; when SYN = 1 and ACK = 1, it represents that the previous connection request has been passed, and the data is a connection receiving segment fed back to connection initiator.

In the option field, TCP currently has only regulated one option, namely the maximum MSS (Maximum Segment Size) to tell the other party the maximum number of bytes that its buffer can receive.

2.2 Connection establishing process of three-way handshake protocol

Connection establishing process of classical TCP three-way handshake protocol is as shown in Fig.2.

The first handshake. TCP of Host A sends connection request (SYN) segment to TCP of Host B, SNY = 1 and ACK = 0 in the head part of segment. Meanwhile select a sequence number x, which means that the sequence number of the first byte of the data transmitted in the following is x.

The second handshake. After receiving the connection request segment, if TCP of Host B agrees to establish connection, it will send “SYN + ACK” segment for confirmation, wherein SYN = 1, ACK = 1 and confirming sequence number = x+1 in the head part of the segment. Meanwhile send its sending sequence number y, with the same significance as the above step.

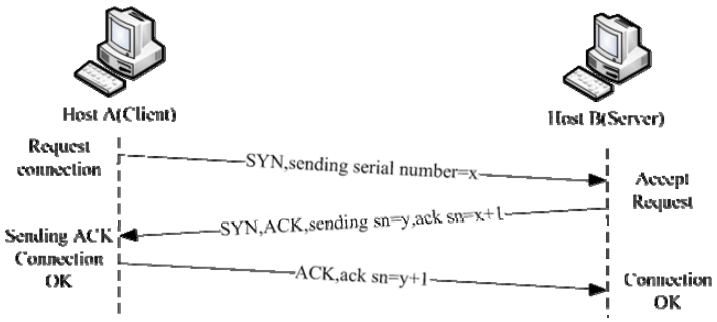


Fig. 2. Three-way handshake to establish TCP connection

The third handshake. After receiving this confirming segment, TCP of Host A will send confirming (ACK) segment to Host B, wherein ACK = 1 and confirming sequence number = y + 1. Meanwhile, TCP of Host A notifies the upper application procedure that connection has been established. And after receiving confirmation of Host A, TCP of Host B will also notify its upper applications.

2.3 Problems of the three-way handshake protocol

The first and second handshakes have completed connection request and response, and the reason to conduct the third handshake is to prevent the expired connection request segment from A suddenly reaching Host B, which makes B believe that A wants to establish new connection and send "SYN + ACK" segment again, but after receiving A will ignore since it does not send new connection request. While B believes that the connection has been established and will be waiting for the data sent from A and enter a deadlock state, which causes resource waste. Just because there is the third confirmation, after sending "SYN + ACK", B does not believe that the connection has been established, but enters a half-connection state, waiting ACK segment from A, and if it does not receive when time exceeds, B will decisively release the prepared connection resources.

However, there still exist the following problems even the third handshake is adopted:

Firstly, in case of not considering loss or delay of ACK segment in the third handshake. If the (ACK) segment to B from A is lost or seriously blocked, A does not know about this and believes that connection has already been established and it can begin to send data; meanwhile, B is still in the half-connection state since it does not receive ACK, and ignores the received data from A. And after A sends the data which is not confirmed by B in a long term, it believes that there is error, and will re-send the previous data information, which will cause a vicious circle.

Secondly, some malicious hosts (take network delay as excuse) do not send back ACK confirming segment on purpose, and Host B, as the server will be helpless, which will easily cause DDoS (Distributed Denial of Service) [6]. According to regulations in TCP protocol: if the server does not receive the ACK confirmation in the third step, it will stay in half-connection state all the time, add client IP in the waiting list, and re-send the "SYN + ACK" segment of the second step. Generally resend for 3~5 times, and polling interval is about 30 seconds, waiting the list to re-test all the clients. Therefore, the server will maintain a huge waiting list, re-send "SYN + ACK" segment in polling, and will occupy large amount of resources which can not be released. On the other hand, after sending "SYN + ACK" segment, the server will pre-allocate resources to make preparation for information storage for the TCP connection to be soon established, and this resource will be maintained during the period of waiting for retest. However, server resources are limited, and will not receive new SYN segment and refuse to establish new TCP connection if it exceeds the limit of maintainable half-connection state.

The above problems can be concluded that: the ACK segment of client that the server waits for might be delayed or might not be passed back maliciously, as shown in Fig.3. ACK delay is unavoidable in classical network and blocking possibility still exists no matter how the network communication quality is improved. For vicious SNY attackers of the returned ACK, the situation of pretending to have not received "SYN+ACK" or pretending as ACK delay can be controlled by shortening server's expiration time and reducing re-sending times [7].

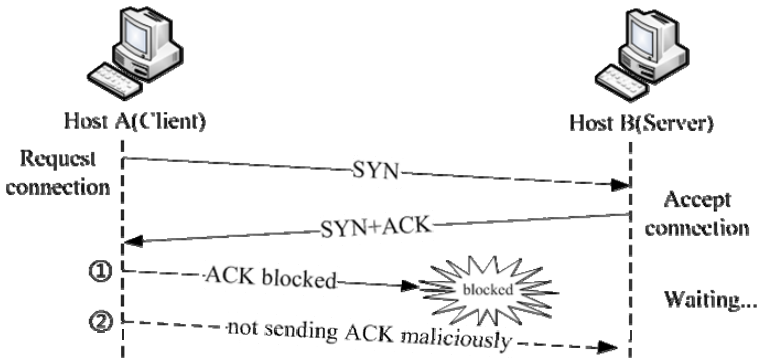


Fig. 3. Problems of classical TCP three-way handshake

From the above description, it can be easily seen that traditional methods might not solve this problem well, while quantum mechanics provides us with a new thought. The thesis proposes a method which can well solve the above problems with quantum entanglement characteristics.

3 Quantum TCP three-way handshake protocol

3.1 Quantum entangled state

Quantum entanglement is an important part of quantum information, which is a special relevance containing two or more particle systems which influence each other. It is firstly proposed by Albert Einstein to criticize the incompleteness of quantum mechanics theory in 1935, and named by Erwin Schrödinger [8]. Particle A and particle B respectively in quantum state of $|\psi\rangle_A$ and $|\psi\rangle_B$ constitute the system AB, and if its quantum state $|\psi\rangle_{AB}$ can not express the direct product form of subsystem state, and one can say that the two particles are in entangled state:

$$|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$$

All the single particle after coupling lose their own unique attribute, but devotes the entanglement characteristic of the entire system: when measuring any one of them, it will absolutely cause wave packet collapse to the other particle. This process is instantaneous, is not constrained by the law of causality in relativity theory [9].

For the superposition state of the two particles $|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle)$, since they can be written as $|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle$, they are not entangled state. Obviously the state of the second particle is always $|1\rangle$, and its state will not change due to any change of state of the first particle, namely that the two particles are independent from each other. While $|\phi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ is entanglement, and the two particles are always opposite to each other. Measurement to one of the two particles causes compound system quantum state collapses to $|01\rangle$ or $|10\rangle$ (each with 50% possibility), and as long as the state of one particle is known, one can deduce the state of the other particle. This is the EPR entanglement revealed by Albert Einstein, and he describes it as “spooky action in a distance” [10]. Both the excellent experiments of remote quantum communication and entanglement exchange have verified this incomprehensible situation, and it has three common characteristics as following:

(1) Transition is completed in a short moment;
(2) There is no need to know where the other party is in advance for transition;
(3) Transition will not be blocked by any obstacle.

In other words, except for the time to establish quantum channel, transition of quantum information

does not need time, and will absolutely cause no error [11]. The thesis uses this characteristic in quantum mechanics to initiate the third handshake through quantum channel to send confirming data segment for TCP connection, which can shorten connection establishing process and effectively avoid safety problems resulted from classical connection methods. It should be noted that the above action at a distance will cause appearance of super velocity of light. Actually for this velocity measured in the test, relativity theory does not exclude the existence of super velocity of light, but existence of signal of super velocity of light (including physical movement with information). Actual TCP is divided into busy and idle time, and we send EPR relevance particle pair during idle time to establish quantum entanglement channel and send TCP confirmation by passing quantum information during busy time, which increases passage efficiency and improves communication safety at the same time.

3.2 Using teleportation to transmit confirming information

It is assumed that the quantum information which is agreed by the two parties to establish TCP connection to be used for confirmation is in a quantum state of $|\phi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$, and the EPR relevance particle pair shared by the two parties to establish TCP connection in idle time is in entangled state of $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. After receiving "SYN+ACK" confirmation of Host B (namely the server terminal of TCP), the Host A (namely the initiating terminal of TCP connection) in Fig.2 conducts confirmation to this segment, prepares a particle in the above confirming quantum state of $|\phi\rangle$, and conducts joint measurement (BSM: Bell-State Measurement) to the newly prepared particle $|\phi\rangle$ and the pre-shared EPR particle with the measuring devices to identify Bell-state [12-13]. Results are as following:

$$|\varphi\rangle_m \otimes |\psi^-\rangle = \frac{1}{2}\left[|\psi^-\rangle\left(-\frac{1}{\sqrt{5}}|0\rangle - \frac{2}{\sqrt{5}}|1\rangle\right) + |\psi^+\rangle\left(-\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle\right) + |\phi^-\rangle\left(\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle\right) + |\phi^+\rangle\left(-\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle\right)\right] \quad \textbf{(1)}$$

Bell-state measuring result has to be one of the Bell-states, and respective probability is 1/4. Once the set measuring time comes, Host B measures the EPR entangled particle corresponding to Host B. If Host A sends confirming information, and the quantum state of the EPR entangled particle of the receiver (namely Host B) has to be:

$$-\frac{1}{\sqrt{5}}|0\rangle - \frac{2}{\sqrt{5}}|1\rangle \ 、\ -\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle \ 、\ \frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle \ 、\ -\frac{2}{\sqrt{5}}|0\rangle + \frac{1}{\sqrt{5}}|1\rangle \quad \textbf{(2)}$$

Probability for one of them is always 1/4, and when any one of the above four states appears, it means that the data segment of the second handshake has been correctly received and TCP connection has been successfully established [14]. It should be noted that the four quantum states are non-orthogonal, and though non-orthogonal quantum states can not be distinguished, it is feasible to distinguish non-orthogonal quantum states as long as it is allowed to break down quantum state [15].

On the contrary, if Host B measuring result is $|0\rangle$ or $|1\rangle$, it means that Host A does not send confirming frame. Since the protocol regulates that it is necessary to unconditionally send quantum confirming frame after receiving "SYN + ACK", it can conclude that "SYN + ACK" segment has not safely arrived at Host A according to the above. Therefore Host B promptly re-sends "SYN + ACK" segment.

3.3 Quantum TCP three-way handshake protocol

According to transmission and inspection method of the above TCP connection three-way handshake information, quantum TCP three-way handshake protocol process is as shown in Fig.4. The horizontal line in the figure realizes quantum confirmation with EPR entangled state. Since the process is completed instantaneously, can not be located and causes no error, there is no delay existing. The entire connection establishing process is described as following:

The two parties which established connection firstly have shared one pair of ERP entangled particle pare in advance before establishing connection, namely that the two parties have established quantum entanglement channel to prepare for connection.

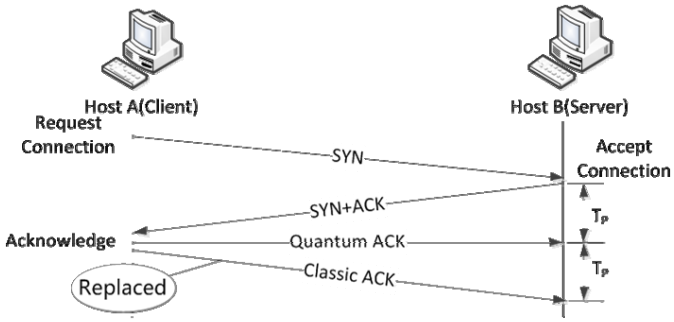


Fig. 4. Quantum TCP three-way handshake process

Connection requesting party (Host A):

A0: Possess particle a which has EPR entanglement relationship with Host B;

A1: Select its own sending sequence number x, and send the connection segment SYN to B through classical information channel;

A2: Receive the "SYN+ACK" segment send by Host B through classical information channel;

A3: Prepare confirming quantum state of $|\phi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|1\rangle$, and conduct joint measurement to EPR entangled particle a, which will absolutely cause changes to quantum state of particle b, namely that realize the third handshake and send quantum confirmation through quantum entanglement channel, and the connection is successfully established.

Service provider (Host B):

B0: Possess particle b which has EPR entanglement relationship with Machine A

B1: Waiting for client connection request;

B2: After receiving connection request segment form A, set SYN, select one sequence number y as its own sending sequence number, take x + 1 as confirming sequence number, and generate TCP "SYN + ACK" segment;

B3: Send "SYN+ACK" segment to A through classical channel, and set waiting timer to begin work, set the re-sending timer as 0;

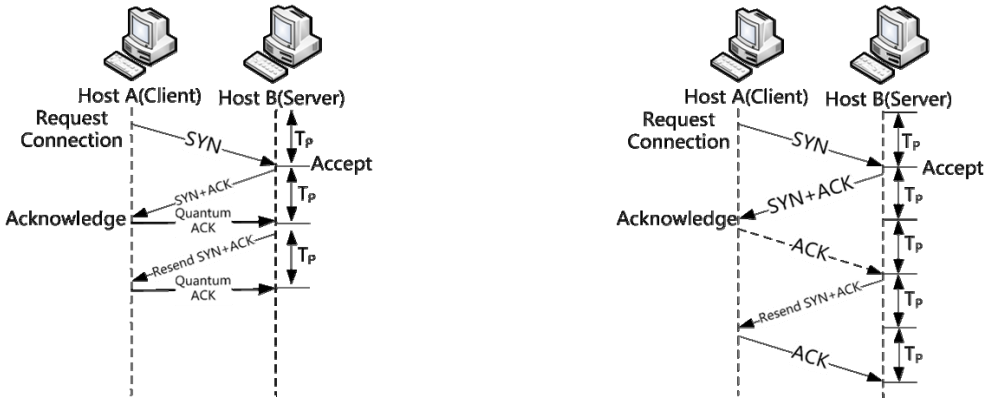
B4: When time is out, conduct quantum measurement to the shared EPR entangled particle B, and as long as the result is one of the Expression (2), it can be determined that quantum confirming segment has been sent back and connection has been established; otherwise, connection fails, re-sending times should be added with 1. If re-sending time is less than 2, goto B2 to re-send, and if it is more than 2, immediately release previously occupied system resources and goto B1.

3.4 Analysis on protocol efficiency and safety

The difference with classical three-way handshake protocol lies in the third handshake, the classical ACK is replaced with quantum confirming process, and since EPR quantum entanglement characteristics ensures that this information will not be blocked or delayed, and possibility of ACK segment being blocked in network can be eliminated. However it should be noted that it also needs some time to establish quantum channel. Therefore the protocol pre-establishes quantum channel in idle time to save time in classical communication phase [16-17].

In case of A not sending "quantum confirmation(namely ACK)" maliciously, after sending "SYN + ACK" confirmation and after T_p (sending time + processing time), B does not receive "quantum confirmation" information from A and will re-send "SYN + ACK", after which if it still does not receive ACK again, it is promptly determined that there is malicious attack in A, and decisively release the system resources consumed to maintain the half-connection state. There, of course, might be erroneous judgement since "SYN+ACK" segment might be blocked twice. A needs to re-send connection request, which can greatly reduce possibility of server being attacked and improve system safety. Since the connection state that the server can bear is much higher than the half-connection state, this method can effectively

alleviate attack to the server. By contract, in the classical three-way handshake protocol, B's overtime length is 2 times of quantum confirmation length, and it is necessary to re-pass "SYN + ACK" and wait. Repeat as this for 2~5 times, which determined by the system where TCP locates, with lower efficiency, and it needs to maintain in half-connection state for a long time.



Left Fig.: Quantum confirming method Right Fig.: Classical confirming method

Fig. 5. Re-sending comparison of the two confirming methods

If network sending time is t_a, classical processing time is t_{pr}, quantum processing time is t_{Qpr}, and classical processing and quantum processing can be conducted at the same time. Therefore, the total processing time $T_{pr} = \max(t_{pr}, t_{Qpr})$, and the above waiting time $T_p = (t_a + T_{pr})$.

Table 1. Comparison of connection establishing times of the two different three-way handshake methods

ACK Method	First Confirm	Second Confirm	Third Confirm
Quantum ACK	$2T_P$	$3T_P$	$4T_P$
Classical ACK	$3T_P$	$5T_P$	$7T_P$

It can be seen from the above that if there is no error, quantum confirming efficiency is 1.5 times of that of classical method. If re-send for one time, it is 1.67 times; if re-send twice, it is 1.75 times. It should be noted that efficiency improvement is not the main target of this protocol, what is more important is to greatly reduce the risk of server resource exhaustion by saving time of the server, and then prevent various DDoS attacks.

4 Conclusion

It utilizes entanglement relevance and quantum information transition instantaneity in quantum mechanics to propose the TCP three-way handshake protocol based on EPR entanglement quantum state. The protocol completes EPR entangled state distribution and establish quantum channel in idle time of the line. The third handshake of TCP, the final sending confirmation, is passed through quantum channel in form of quantum. Since EPR quantum entanglement characteristics ensure that the process will not be blocked or delayed, this completely solves the problem of ACK being blocked in network in the classical three-way handshake protocol. Meanwhile since the overtime length at the connection accepting terminal is reduced by half, it greatly reduces the occupied resources to maintain half-connection state and greatly reduces the risk of suffering from SYN Flood attack.

Acknowledgements

The work is supported by the Guangdong Provincial Natural Science Foundation(Grant No. S2013010015471), and the Shenzhen Basic Research Project(Grant No.JCYJ20120617140737337, Grant No. JCYJ20130331151803073).

References

[1] Tanenbaum., A. S. (2004). *Computer networks* (4th ed.). Beijing, China: Tsinghua University Press.

[2] Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.

[3] Bellovin, S. M. (1989). Security problems in the TCP/IP protocol suite. *Computer Communications Review, 19*(2), 32-48.

[4] Zhang, Y.-D. (2006). *Principles of quantum information physics*. Beijing, China: Science Press.

[5] Xie, X.-R. (2008). *Computer networks*. Beijing, China: Electronic Industry Press.

[6] Yan, F., Wang, J.-J., Zhao, J.-F., & Yin, X.-C. (2008). Survey of detection on DDoS attack. *Application Research of Computer, 25*(4), 966-969.

[7] Mirkovic, J., Prier, G., & Reiher, P. (2002, November). *Attacking DDoS at the source*. Paper presented at the Proceedings of the ICNP, Paris, France.

[8] Einstein, A., Podolsky, B., & Rosen, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Physical Review, 47*, 777-780.

[9] Bennett, C. H., & Brassard, G. (1984, December). *Quantum cryptography: Public key distribution and coin tossing*. Paper presented at Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India.

[10] Riebe, M., Häffner, H., Roos, C. F., Hänsel, W., Benhelm, J., Lancaster, G. P. T., Körber, T. W., Becher, C., Schmidt-Kaler, F., James, D. F. V., & Blatt, R. (2004). Experimental quantum teleportation with atoms. *Nature, 429*, 734-737.

[11] Wen, X.-J., & Chen, Y.-Z. (2012). *Quantum signature and application*. Beijing, China: Aviation Industry Press.

[12] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical Review Letter, 67*, 661-663.

[13] Guo, G.-C. (1996). Entangled state and application. *Acta Sinica Quantum Optica,* 164.

[14] He, G.-P. (2012). *Popular quantum information science*. Beijing, China: Science Press.

[15] Zhou, N.-R., Zeng, G.-H., Zhu, F. C., & Liu, S. Q. (2006). The quantum synchronous communication protocol for two-army problem. *Journal of Shanghai Jiaotong University, 40*, 1885-1889.

[16] Zhou, N.-R., Zeng, B.-Y., & Gong, L.-H. (2010). ARQ quantum synchronous communication protocol based on entanglement. *Acta Physica Sinica, 59*(4), 2193-2199.

[17] Huang, Y.-F., Guo, G.-C. (2009). Experimental preparation and manipulation of quantum entangled states. *Journal of the Graduate School of the Chinese Academy of Sciences, 26*(4), 569-576.