A Quantum Identity Authentication Protocol Based on Optical Transmission & Face Recognition

https://doi.org/10.3991/ijoe.v14i04.8374

Dexin Zhu, Xiaohui Li
Changchun University, Changchun, Jilin Province, China

Xiaohong Li
Jilin Province Economic Management Cadre College, Changchun, Jilin Province,China

Rongkai Wei, Jianan Wu
Changchun University, Changchun, Jilin Province, China

Lijun Song(✉)
Jilin Engineering Normal University, Changchun, Jilin Province, China
Jilin Engineering Laboratory for Quantum Information Technology, Changchun, Jilin Province, China
ccdxslj@126.com

Abstract—Specific to security issues concerning identity authentication of mobile applications, a quantum identity authentication protocol based on optical transmission and face recognition is put forward in this paper with consideration of the unconditional security characteristic of quantum key. As for this protocol, optical transmission technology is adopted to acquire quantum key and identity authentication encrypted by quantum key can thus be realized, for which key feature points of face image and user password serve as dual authentication factors. Experimental result and security analysis indicate that this protocol can resist illegal attack and ensure security of identity authentication of mobile applications, which also has great operating efficiency.

Keywords—Optical Transmission, Face Image, Quantum Key, Identity Authentication

1 Introduction

With rapid development of digitization of information in recent years, modern internet technology has been changing people's lifestyle gradually: Various web services such as social network, long-distance education, instant messaging and e-commerce have been integrated into people's work, study and life. However, not only did such web services bring convenience to people's life, they also brought about challenges concerning various Internet security and privacy protection issues. Serving as the first line of defense for Internet interaction, identity authentication is the basis

of all security issues and plays a very important role in overall Internet security. Identity authentication is used by both sides in communications to recognize each other's identity in order to prevent illegal user from using network information system and prevent any user from using such system illegally. At present, identity authentication technologies mainly include static password-based authentication technology, dynamic password-based authentication technology, biological characteristic-based authentication technology, PKI-based authentication technology, etc.Griffin [1] describes biometric-based cryptographic techniques for providing confidential communications and strong, mutual and multifactor authentication on the Internet of Things, Anamonye [2] put forwardthe designing and implementing a stand-alone identity authentication device using fingerprint technique, Tabassum [3] suggests the authentication mechanism of Kerberos protocol under HDFS and provide security to the communication channel with help of RSA, YU [4] aims to design a face recognition system that can be used in the exam identity authentication system.Although various researches provided some relatively feasible plans for identity authentication, the currently used keys are generated by computers in a pseudo-random way and thus follow a certain rule. With rapid development of computer technology, especially emergence of quantum computer, it becomes very difficult for the method of classic key generation and encryption to meet requirements of identity authentication in those occasions requiring a high class of confidentiality.

Basic thought of quantum communication was successively put forward by Bennett et al. in the 1980s and 1990s, mainly including quantum key distribution (QKD) [5] and quantum teleportation [6]. Quantum key distribution can establish secure quantum password and realize point-to-point secure classic communication through the "one-time pad" encryption method. Security described herein refers to security strictly proved by mathematical method, which can't be done by classic communication so far. At present, Sharma [7] proposes a quantum identity based authentication and key agreement scheme for cloud server architecture, Tanizawa [8] proposes a new solution for developing secure network infrastructure based on QKD technology to accommodate multiple applications. The proposed solution introduces 3 functions: (1) a directory mechanism to manage multiple applications hosted on the QKD network, (2) a key management method to share and to allocate the keys for multiple applications, and (3) a cryptography communication library enabling existing cryptographic communication software to be ported to the QKD network easily. However, quantum keys are currently acquired via wired network.

Therefore, a quantum identity authentication protocol based on optical transmission and face recognition is put forward in this paper, for which quantum key can be acquired via wireless network instead of wired network. By using optical transmission technology, this protocol can convert a quantum key in a wired network into a QR code firstly and the user can acquire the quantum key by scanning the QR code with a mobile device. Based on a characteristic of face recognition, namely requiring no field collection of a user's information, key feature points of a facial image and user password are used as two factors in two-factor authentication in order to realize two-factor authentication of a user's identity and further ensure safety of network information.

2 Protocol Architecture

The architecture of a quantum identity authentication protocol based on optical transmission and face recognition is indicated in Figure 1 and the protocol is composed of Mall (Shopping Mall) and PP (Payment Platform), in which type of network for Mall is local area network, for which participants include QGW_A（QuantumGateWay Alice）, MS (Mall Server), QKWD (Quantum Key Write Device) and USER; type of network for Payment Platform is local area network, for which participants include QGW_B（QuantumGateWay Bob） and PPS (Payment Platform Server). QGW_A and QGW_B can generate symmetrical quantum keys via a quantum optical fiber link. Quantum key at the QGW_A side is stored in MS, while quantum key at the QGW_B side is stored at PPS; QKWD is used to convert quantum key into QR code.

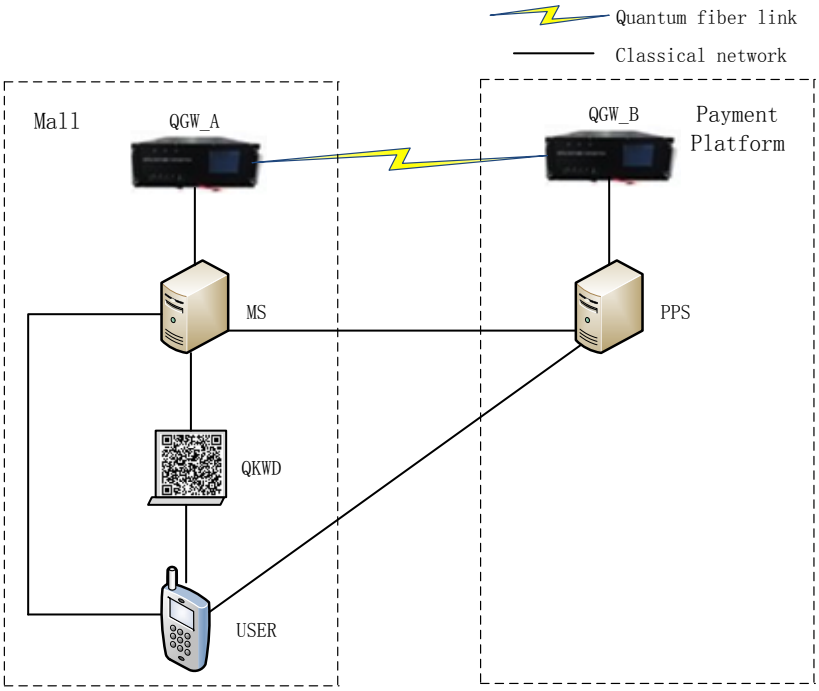

Fig. 1. Protocol Architecture

Design requirements of this identity authentication should be considered from three perspectives: Firstly, networks of Mall and PP should be trusted networks; secondly, it should be ensured that identity authentication data provided by USER will not be illegally attacked; finally, high efficiency of the system should be guaranteed. Authentication services of this system include the following functions:

1. Quantum key distribution. QGW of Mall and PP realizes quantum key distribution through quantum optical fiber link and generates quantum key.
2. Quantum key management. Quantum keys generated by QGW_A and QGW_B are stored in MS and PPS and managed by MS and PPS based on use of quantum keys.
3. Quantum key writing. Based on optical transmission technology, QKWD can acquire quantum key from MS and PPS based on quantum key required by identity authentication. Embedded technology is adopted to convert quantum key into the form of QR code.
4. Identity authentication. USER at the Mall side can collect facial feature information through camera, acquire quantum key by scanning QKWD based on such facial feature information, encrypt data by adopting "one-time pad" scheme and send such data to PP side finally. PPS at the PP side should verify validity of identity of USER.

3 Protocol Scheme

This quantum identity authentication protocol is established at system application layer based on conceptual design, including two phases, namely registration and identity authentication. Registration phase refers to the phase in which a new user uses the system and each user only has one registration process. Identity authentication is the critical operation in which a user logs on to the system, for which system will determine validity of user's identity based on result of identity authentication.

3.1 User Registration Phase

User registration refers to the process in which USER applies for a valid identity, for which the process is indicated in Figure 2.

Major steps are described as follows:

Step 1: QGW_A and QGW_B conduct quantum key distribution through quantum optical fiber line. Quantum key distribution protocol adopts BB84 protocol [5], which selects a certain physical quantity of single photon to carry single-bit information and uses two different groups of orthogonal bases for two-dimensional Hilbert space of single-photon polarization state, for which two groups of bases have the following relation:

$$\left|\pm\right\rangle = 1/\sqrt{2}\left(\left|H\right\rangle \pm \left|V\right\rangle\right) \tag{1}$$

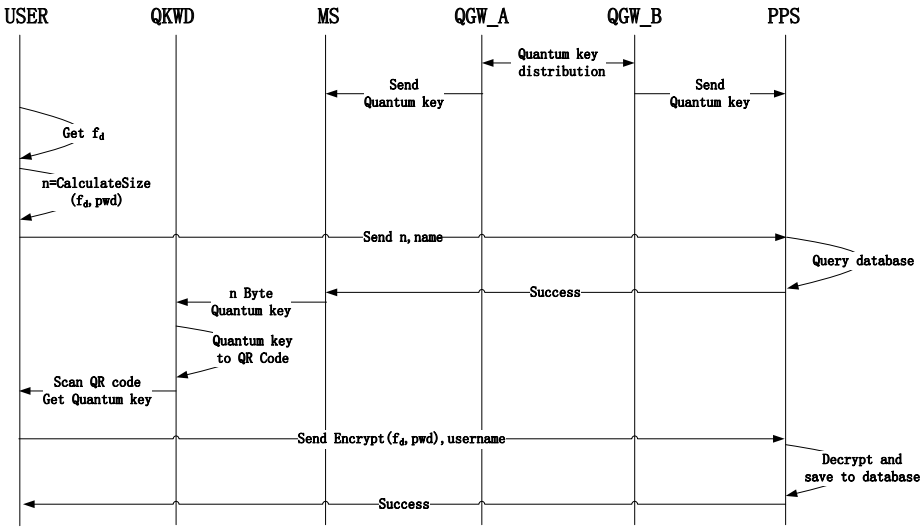

Fig. 2. User Registration Process

Step 2: QGW_A and QGW_Bgenerate quantum keys qk_a and qk_b, in which qk_a is stored into MS and qk_b is stored into PPS. Herein qk_a and qk_b are binary symmetric keys and expressed as:

$$\begin{aligned} qk_a &= \left\{qk_{a1}, qk_{a2}, \cdots, qk_{ai}, qk_{a(i+1)}, \cdots, qk_{an}\right\}, qk_{ai} \in \{0,1\}, (i = 1,2,\cdots,n) \\ qk_b &= \left\{qk_{b1}, qk_{b2}, \cdots, qk_{bi}, qk_{b(i+1)}, \cdots, qk_{bn}\right\}, qk_{bi} \in \{0,1\}, (i = 1,2,\cdots,n) \end{aligned} \tag{2}$$

Step 3: USER can analyze information about key feature points of face images f_d captured by mobile phone by using face recognition technology.

Step 4: USER enters name and pwd and then calculates number of bytes occupied by f_d and pwd. Herein: Unit of n is byte; pwd is user's password; name is user's name; f_d is information about key feature points of face images, which can be expressed as $f_{di}(i = 1,2,3,\cdots)$.

Step 5: USER sends n and name to PPS.

Step 6: PPS makes an inquiry in personnel database of payment platform in order to check whether the "name" exists. If such "name" is valid, MS success status will be returned; otherwise, failure status will be returned.

Step 7: MS should make a judgment on return status of PPS. If return status is success, MS should send quantum key qk_a with n bytes to QKWD.

Step 8: QKWD converts quantum key qk_a with n bytes into a QR code.

Step 9: USER activates QR code scanning program and scans the QR code displayed by QKWD in order to acquire encryption quantum key qk_a.

Step 10: Through encryption formula $En\_Info = qk_a \oplus (\mathrm{f}_d, pwd)$, USER can encrypt key feature points of face image f_d and user's password pwd by using quantum key and send encrypted data and name to PPS through classic optical fiber line, in which En_Info represents encrypted data.

Step 11: PPS reads quantum key qk_b with n bytes and acquires decrypted information De_Info through decryption formula $De\_Info = qk_a \oplus En\_Info$, in which decrypted information De_Info includes information about key feature point of face image f_d and user's password pwd. PPS inserts name, f_d and pwd into personnel database of payment platform.

Step 12: PPS returns status of successful registration to USER.

3.2 Identity Authentication Phase

Identity authentication is a process in which USER and PPS recognize each other's valid identity and require encryption of data through using quantum key in order to ensure data security. Process of user identity authentication is indicated in Figure 3.

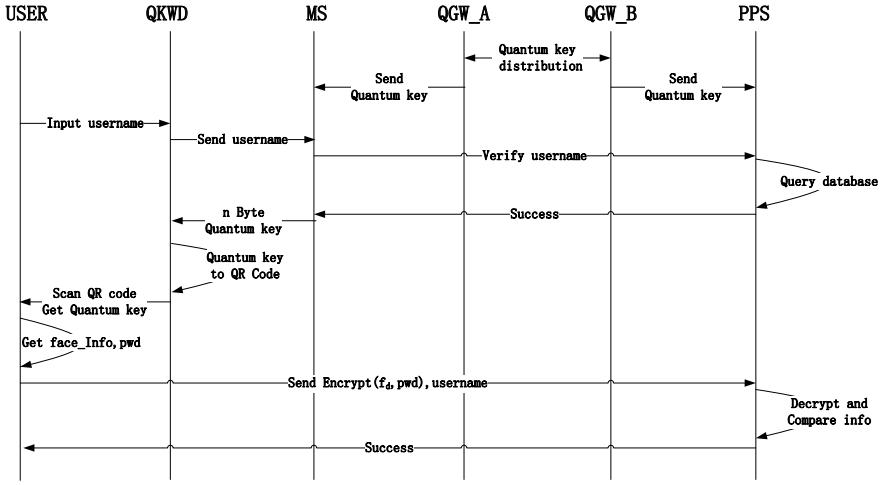

Fig. 3. Process of User Identity Authentication

Steps are described as follows:

Step 1: QGW_A and QGW_B distribute quantum key and generate real-time quantum keys qk_a and qk_b.

Step 2: qk_a is stored into MS and qk_b is stored into PPS.

Step 3: In order to acquire quantum key qk_a, USER should enter name into QKWD and click the button GetQKey to acquire quantum key.

Step 4: QKWD sends the name entered by USER to MS in order to determine whether the user is a valid user.

Step 5: MS sends name to PPS and then PPS makes an inquiry in the personnel database of payment platform in order to check whether the user exists. If the user exists, quantum key number n of this user and Success will be returned to MS; otherwise, "Failed" should be returned.

Step 6: MS sends quantum key with n bytes to QKWD.

Step 7: QKWD converts quantum key with n bytes into QR code.

Step 8: USER activates QR code scanning program and scans the QR code displayed by QKWD in order to acquire encryption quantum key qk_a.

Step 9: USER analyzes information about key feature point of face image f_d captured by mobile phone by using face recognition technology. Encryption formula $En\_Info = qk_a \oplus (f_d, pwd)$ is adopted to conduct quantum key encryption of information about key feature point of face image f_d and user's password pwd, and encrypted data and name should be sent to PPS through classic optical fiber link.

Step 10: PPS reads quantum key qk_b with n bytes and acquires decrypted information De_Info through decryption formula $De\_Info = qk_a \oplus En\_Info$. PPS then makes a comparison between decrypted f_d and pwd and information about this user in the personnel database of payment platform. If such information comparison is successful, then go to Step (k); otherwise, identity authentication fails.

Step 11: Identity authentication is successful.

4 Security Analysis

This protocol has a relatively high degree of security, for which specific analysis is provided as follows.

4.1 Security of Quantum Key

As for quantum key distribution, BB84 protocol is adopted. This protocol is based on special laws of quantum physics, Heisenberg's Uncertainty Principle and Quantum

Non-cloning Theorem [9]. This protocol enables both sides to acquire secure shared key and can realize absolutely secure secret communication under strict mathematical proof.

4.2 Brute Force Attack

Security of this protocol depends on secure sharing of quantum key and the "one-time pad" encryption mechanism. In this mechanism, quantum key with a length equal to message is used to generate random output without any statistical relation with the original text and such quantum key can only be used for once. Shannon proves that: "One-time pad" mechanism can realize perfect confidentiality and has been deemed as unbreakable [10].

5 Experimental Result & Analysis

5.1 Experimental Scheme

In this experiment, quantum key distribution device adopts quantum security gateway with a working frequency of 40M and 1*4 matrixed photon switcher. Topological structure of network is indicated in Figure 4. Herein: KJCS represents key generation control server, which is used to control quantum key distribution process for the entire quantum optical fiber link; SIP represents SIP server, which is used to establish SIP user; Log represents log server, which is used to check operating state of the entire quantum optical fiber line.

Quantum key distribution device generates quantum key through quantum optical fiber link and classic optical fiber link can store quantum keys of both sides into PPS and MS.

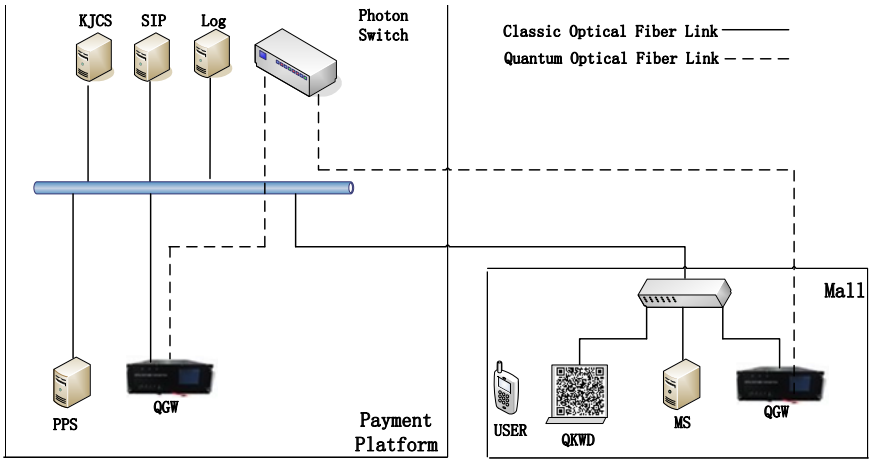

Fig. 4. Topological Structure of Network

QKWD uses ARM9 mini2440 development board and major parameters of equipment are indicated in Table 1. See Table 2 for major parameters of USER's mobile device.

Table 1. Major Parameters of QKWD

Parameters ofHardware				
OS	***CPU***	***SDRAM***	***Nand Flash***	***Touch screen***
Fedora14	S3C2440	64M	256M	4.3Inch

Table 2. Major Parameters of USER's Mobile Device

Major Parameters of USER's Mobile Device		
OS	***CPU***	***RAM***
Android5.1	8-core, 1.5GHz	2.0GB

5.2 Result & Analysis

QKWD converts quantum key of different bytes into QR code, for which the relation between number of bytes of quantum key and time of QR code generation is indicated in Figure 5.

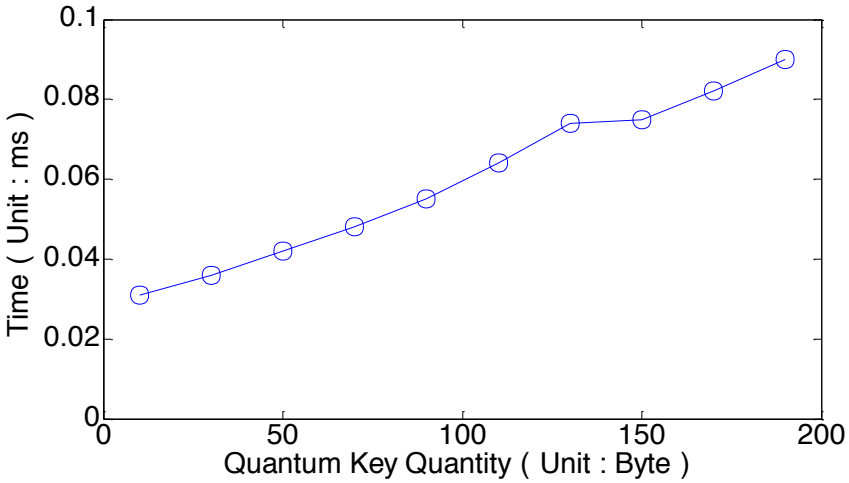

Fig. 5. Time of QR code generation

Mobile device should be positioned at the place 200mm directly above quantum key writing device and QR code should be scanned, based on which the time relationship between quantum key of different bytes and QR code scanning is indicated in Figure 6.

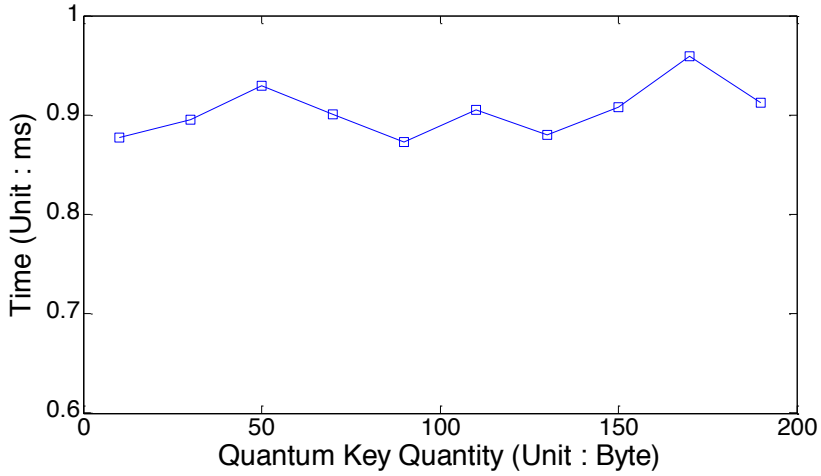

Fig. 6. Time of QR code scan

As for this protocol, four eye corners of two eyes, tip of nose, two corners of mouth, points of intersection between extension line of two corners of mouth and facial contour in a face image are selected as 9 key feature points, and length of user's password should be 6 characters. According to the "one-time pad" encryption scheme, 78 bytes of quantum key are needed. For the purpose of making an assessment on operating efficiency of this protocol, the following symbols are adopted in this paper to represent time needed by each operation: T_K represents time needed by QKWD for acquiring quantum key from MS; T_Q represents time needed for realizing conversion of quantum key into QR code; T_M represents time needed by mobile device for scanning QR code; T_I represents time needed for completing authentication of user's identity. Overhead time of each phase is indicated in Table 3. It can be seen that life cycle of the entire protocol is 1ms, so this protocol has very high operating efficiency.

Table 3. Overhead Time of Protocol

Process	Time (ms)
T_K	0.003
T_Q	0.049
T_M	0.898
T_I	0.008

As indicated in Table 4, through comparison between this paper and some existing reference papers such as Griffin [1], Yu [4] and Sharma [7], only the author of this paper put forward the method of acquiring quantum key via optical transmission technology and conducting absolutely safe identity authentication.

Table 4. Comparison between This Paper & Other Reference Papers

	Reference Papers[1] & [4]	***Reference Paper [7]***	***Ours***
Key Generation	Pseudo-random Generation	Quantum Key Distribution	Quantum Key Distribution
Safety of Key	Non-absolutely Safe	Theoretically Absolutely Safe	Theoretically Absolutely Safe
Type of Network	Wireless Network	Wired Network	Wireless Network

6 Conclusion

In this paper, a quantum identity authentication protocol based on optical transmission and face recognition is put forward, which integrates various technologies such as optical transmission, face recognition and quantum key. As for this protocol, optical transmission technology is adopted to acquire quantum key and face recognition technology can recognize 9 key feature points of face image. Based on the "one-time pad" encryption scheme, quantum key is used to encrypt and decrypt key feature points of face image and user's password. This protocol can ensure authenticity and confidentiality of user's information during registration phase and authentication phase and can achieve a relatively high degree of security against illegal attack. Meanwhile, this protocol has great operating efficiency.

7 Acknowledgment

This work is supported by the Science and technology of Jilin province development plan projectswith grants No. 20170204023GX.

8 References

[1] GriffinPhillip, H. (2013). Secure authentication on the Internet of Things. Southeastcon, pp1-5.
[2] Anamonye, U. G., Eyenubo, O. J. (2017). DESIGN OF EMBEDDED IDENTITY AUTHENTICATION SYSTEM. JOSTE, 5(1):81–86.
[3] Tabassum, R., Tyagi, D. N. (2017). Hadoop Identity Authentication using Public Private Key Concept. IJETT, 45(9): 436–442. https://doi.org/10.14445/22315381/IJETT-V45P283
[4] Yu, L. J., Li, K.F. (2017). Application of Face Recognition Technology in the Exam Identity Authentication System. 2017 3rd International Conference on Social Science and Management.

[5] Bennett, C. H., Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. Proceedings of theIEEE International Conference on Computers, Systems, and SignalProcessing, 175-179.
[6] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W. K.(1993). Teleporting an unknown quantum state via dual classical and EinsteinPodolsky-Rosen. Phys Rev Lett, 70(13):1895–1899. https://doi.org/10.1103/PhysRevLett.70.1895
[7] Sharma, G., Kalra, S. (2016). Identity based secure authentication scheme based on quantum key distribution for cloud computing. Peer-to-Peer Netw. Appl., 1-15.
[8] Tanizawa, Y., Takahashi, R., Sato, H., Dixon, A. R., Kawamura, S. (2016). A Secure Communication Network Infrastructure Based on Quantum Key Distribution Technology. Ieice Transactions on Communications, 99(5):1054-1069. https://doi.org/10.1587/transcom.2015AMP0006
[9] Wootters, W. K., Zurek, W. H. (1982). Asinglequantum cannot be cloned. Nature, 299(5886): 802-803. https://doi.org/10.1038/299802a0
[10] Shannon, C. E. (2014). Communication theory of secrecy systems. Bell System Technical Journal, 28(4):656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

9 Authors

Dexin Zhu is lecturer at the School of College of Computer Science and Technology, Changchun University, Changchun 130021, China, with the research fields of Computer applications and Quantum communication. Email address is 38925023@qq.com.

Xiaohui Li is associate professor at the School of College of Computer Science and Technology, Changchun University, Changchun 130021, China, with the research fields of Computer applications and Quantum communication.

Xiaohong Li is associate professor at the School of Public Teaching Department, Jilin Province Economic Management Cadre College, Changchun 130021, China, with the research fields of Computer test.

Rongkai Wei is lecturer at the School of College of Computer Science and Technology, Changchun University, Changchun 130021, China, with the research fields of Computer networking technology.

Jianan Wu is associate professor at the School of College of Computer Science and Technology, Changchun University, Changchun 130021, China, with the research fields of Computer networking technology.

Lijun Song is professor at the School of Institute for Interdisciplinary Quantum Information Technology, Jilin Engineering Normal University, Changchun 130021, China, with the research fields of Quantum information.

Article submitted 07 February 2018. Resubmitted 15 March 2018. Final acceptance 31 March 2018. Final version published as submitted by the authors.