Available online at www.ijpe-online.com

International Journal of Performability Engineering

vol. 15, no. 8, August 2019, pp. 2165-2172
DOI: 10.23940/ijpe.19.08.p16.21652172

A Quantum Key-based Mobile Security Payment Scheme

Dexin Zhu[a,c], Xiaohui Li[a,c], Jianan Wu[a,c], and Lijun Song[b,c,*]

[a]*College of Computer Science and Technology, Changchun University, Changchun, 130022, China*
[b]*Institute for Interdisciplinary Quantum Information Technology, Jilin Engineering Normal University, Changchun, 130052, China*
[c]*Jilin Engineering Laboratory for Quantum Information Technology, Jilin Engineering Normal University, Changchun, 130052, China*

Abstract

In view of the safety problem of current mobile security payment encryption schemes, this paper proposed a quantum key-based MSP (mobile security payment) scheme. First, this scheme introduced quantum encryption technology to solve the symmetric key problem between the payment platform server and the commercial supermarket server. Then, the quantum key was safely obtained and the QR (quick response) code was generated by using the proposed quantum key gateway. Finally, the mobile device finished the payment according to the one-time pad encryption scheme. Compared with the existing schemes, the proposed scheme can fully employ the advantages of quantum encryption technology. It can also resist multiple security threats by using the quantum key gateway. Under the real quantum key distribution and quantum key gateway environment, the feasibility and effectiveness of this scheme were proven by experimental results.

Keywords: mobile security payment; quantum key gateway; quantum key distribution; QR (quick response) code

(Submitted on June 11, 2019; Revised on July 10, 2019; Accepted on August 7, 2019)

---

1. Introduction

With the rapid growth of the Internet and the rise of e-commerce, the financial payment pattern has become the bottleneck of the economic development. Therefore, mobile payments have emerged. The mobile payment platform has a solid foundation in electronic shopping and has strong technical support. However, there are still many users who are deeply worried about online payment methods. Thus, how to guarantee the transaction security of mobile e-commerce and information security of both sides of a transaction has become the main problem of the development of mobile e-commerce. An encrypted short message verification code-based two-factor mobile payment system was proposed [1]. The NFC security payment protocol based on CoSE was introduced [2]. Based on the cloud service, the payment platform and virtual service hall were implemented [3]. Authors have designed multiple mechanisms including internet, data, security, and emergency response to improve the security of mobile payments. However, the current existing schemes require frequent transmission of sensitive information of users between the mobile terminal and payment platform. Thus, an actual secure channel is needed to guarantee the transmission security. Otherwise, once the internal information of MSP scheme is stolen or modified, it will result in a huge security threat to the whole scheme. The encryption and decryption key used in the MSP scheme are both pseudo-randomly generated by the computer. There are certain rules to follow, and the possibility of being deciphered exists.

Quantum encryption is a proven safe encryption technology that is based on the physical properties of quantum states and the theory of quantum physics [4]. The safety of the technology relies on the principle of quantum physics rather than the mathematical complexity of traditional cryptography. Therefore, it has the outstanding safety advantages in information transmission. Quantum key encryption has been applied in various fields [5-13], such as Ali cloud, telecommunication providers, and the construction of practical quantum networks including quantum satellite networks, quantum metropolitan area networks, and quantum trunk networks [14-17]. By introducing QKD (quantum key distribution) technology to the existing mobile security payment scheme and fully utilizing the physical characteristics of quantum key, the system security

---

[*] Corresponding author.
E-mail address: ccdxslj@126.com

can be effectively enhanced.

A quantum key-based mobile security payment (QMSP) scheme was proposed in this paper. We adopted the quantum encryption technology to enhance the transmission security between mobile terminals and the payment platform. A safe and efficient MSP scheme was formulated by seamlessly applying the quantum key gateway to MSP.

2. Background

Quantum key distribution technology does not rely on the calculation complexity of the classical communication system. It uses the quantum state of the photon or the phase of the quantum state to carry information. By using quantum measurements, transceivers can detect whether these photonic states are attacked by eavesdroppers during transmission. Once the transceivers confirm that the transmission has been maliciously eavesdropped, they will give up the shared key or terminate the protocol directly. This kind of key sharing mechanism can guarantee the absolute security of quantum key distribution system in theory. The BB84 protocol [18] is the earliest and most mature quantum key distribution protocol. Generally, the BB84 protocol employs a single photon to transmit information and uses photon polarization states as the information coding object. The sender is usually represented by Alice, the receiver is Bob, and the eavesdropper is named Eve. The photon polarization states used are horizontal polarization, vertical polarization, 450 polarization, and 1350 polarization, which respectively correspond to the quantum states of $|\mathrm{H}\rangle$, $|\mathrm{V}\rangle$, $|+\rangle$, and $|-\rangle$. Alice and Bob map the photon polarization to the corresponding binary "01" bit information by the basis comparison and form the shared quantum key $key=\{s_i \mid i=1,2,\cdots,n\},\ s_i\in\{0,1\}$ through the "post-processing" process. This is the quantum key distribution process.

3. Quantum Key-based QMSP Scheme

3.1. Structure of the Scheme

The structure of the quantum key-based QMSP scheme is shown in Figure 1. The scheme consists of the payment platform and the commercial supermarket. The network type of the payment platform is a local area network (LAN) including the QKD device and the payment platform server. The network type of the commercial supermarket is also LAN, which includes the QKD device, commercial supermarket server, switch, quantum key gateway, and mobile device. The network type between the payment platform and the commercial supermarket is a wide area network (WAN) including the quantum key distribution channel and quantum encryption channel.

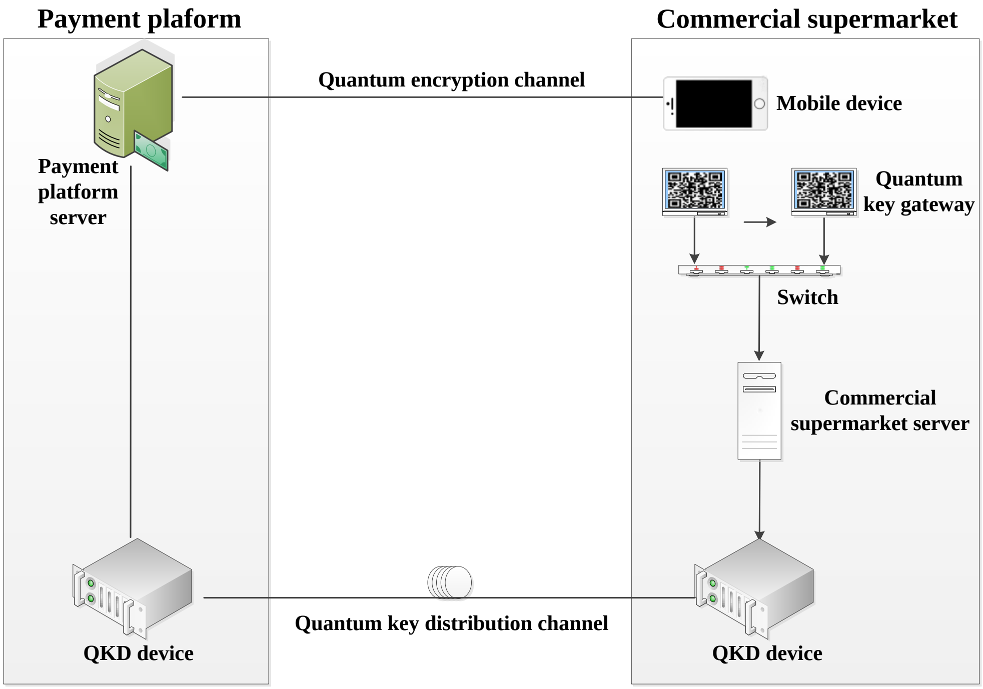

Figure 1. Structure of quantum key-based QMSP scheme

3.2. Role of Related Components

A QKD device is a quantum key distribution device that adopts the mature and widely used single photon decoy state-based BB84 protocol.

The quantum key distribution channel is the link of quantum state transmission and quantum key generation for the QKD devices of the payment sides.

The quantum encryption channel is a secure transmission channel for bit stream-based OTP (one time pad) encryption that uses the quantum key after the payment sides to perform quantum key distribution through the quantum link.

The quantum key is the encryption and decryption key used by each mobile user when it transmits data with the payment platform. It is a symmetric key generated by QKD devices of the payment sides through the quantum key distribution channel. Using quantum key to implement one time pad encryption is a proven secure quantum encryption communication mode at present.

The payment platform server is used to keep the symmetric quantum key generated by the QKD device of the payment platform.

The commercial supermarket server is used to keep the symmetric quantum key generated by the QKD device of the commercial supermarket.

The quantum key gateway applies for the quantum key from the commercial supermarket server and converts it into QR code.

A mobile device scans the QR code and obtains the quantum key to encrypt payment information and transmit it to the payment platform server.

3.3. Main Algorithms of QMSP Scheme

Based on the existing mobile security payment scheme, QMSP introduces quantum key encryption and management-based algorithms to improve the practicability and security. The introduced algorithms mainly include the quantum key gateway setup algorithm and quantum key gateway key acquisition algorithm.

The quantum key gateway setup algorithm: preset the quantum key.

(1) Set the quantum key gateway identifier $GI_i \left\{ i \in 1, 2, \cdots, n \right\}$.

(2) The payment platform server and commercial supermarket server record GI_i.

(3) $Pre(GI_i, 16) = PK_{(GI_i, 16)}$, where Pre is the preset quantum key function, 16 is the number of bytes, and PK is the preset key of the quantum key gateway GI_i.

(4) The payment platform server and commercial supermarket server keep $SPK_{(GI_i, 16)}$, where SPK is the preset key used by servers to keep the quantum key gateway GI_i.

The algorithm for quantum key gateway to obtain quantum key:

(1) The quantum key gateway GI_i applies quantum key from the commercial supermarket server.

(2) The payment platform server and commercial supermarket server apply quantum key $QK_{(GI_i, 1024)}$ with 1024 bytes from the QKD devices.

(3) $DivQ(QK_{(GI_i, x)}, QK_{(GI_i, 16)}, QK_{(GI_i, x-16)})$, where $DivQ$ is the quantum key segmentation function and x is the length of

quantum key, $x <= 1024$.

(4) $En\_AES(PK_{(GI_i,16)}, QK_{(GI_i,x)})$, where En_AES is the encryption quantum key function of the commercial supermarket server that is sent to the quantum key gateway.

(5) $SPK_{(GI_i,16)} = QK_{(GI_i,16)}$.

(6) $De\_AES(PK_{(GI_i,16)}, QK_{(GI_i,x)})$, where De_AES is the decryption quantum key function of the quantum key gateway.

(7) Repeat step (3).

(8) $PK_{(GI_i,16)} = QK_{(GI_i,16)}$.

3.4. Payment Process of QMSP Scheme

Assume that the plaintext length of payment information is 32 bytes. To guarantee the one-time pad encryption, both sides of the payment adopt the XOR algorithm, for which the process is indicated in Figure 2.

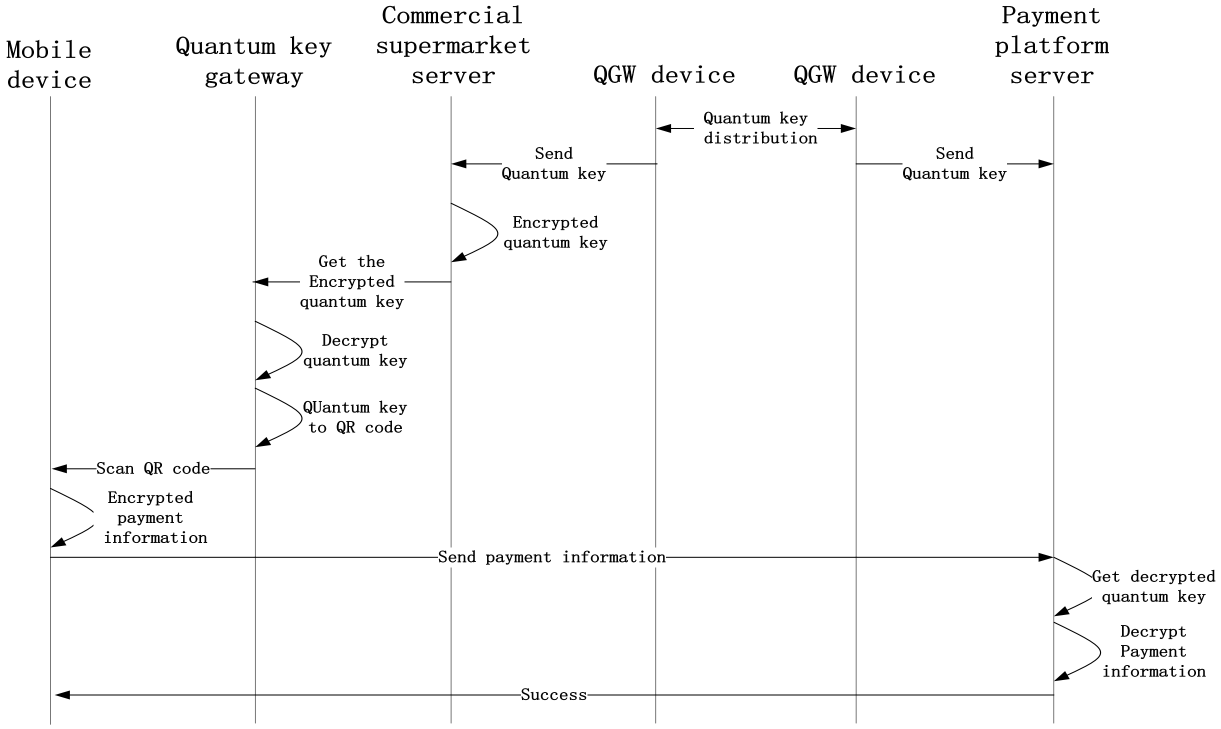

Figure 2. Payment process of QMSP scheme

The payment process is as follows:

(1) The quantum key gateway obtains key $QK_{(GI_i,48)}$.

(2) $DivQ(QK_{(GI_i,48)}, QK_{(GI_i,16)}, QK_{(GI_i,32)})$.

(3) The quantum key gateway converts $QK_{(GI_i,32)}$ into the QR code.

(4) The mobile device cans the QR code to obtain the quantum key.

(5) $En\_Info_{GI_i} = QK_{(GI_i,32)} \oplus M$, where $En\_Info_{GI_i}$ is the encrypted cipher text of the payment information of the mobile device, M is the plaintext of payment information, and $\oplus$ is the XOR operation.

(6) The mobile device transmits $En\_Info_{GI_i}$ to the payment platform server.

(7) The payment platform repeats step (2).

(8) $De\_Info_{GI_i} = QK_{(GI_i,32)} \oplus En\_Info_{GI_i} = M$. The payment platform obtains the plaintext of payment information of the mobile device.

3.5. Security Analysis

Compared with the existing schemes, the proposed QMSP scheme has the advantages of preventing eavesdropping and cracking attacks in the WAN information transmission and internal LAN.

3.5.1. QMSP Scheme Guarantees the Network Transmission Security

Proof: Existing schemes generally use the hypothetical secure channel to transmit the key system parameters. However, in practical applications, security problems such as eavesdropping and cracking due to the complexity of network will threaten the overall security of the MSP scheme. In the proposed QMSP scheme, the quantum key distribution mechanism is introduced. By fully utilizing the security characteristic of the quantum key, the quantum encryption channel is built to encrypt the information between the mobile device and payment platform with one-time pad quantum encryption mode. The physical properties of quantum, such as the Heisenberg uncertainty principle and quantum state non-cloning principle, effectively avoid monitoring and stealing, which enhances the communication security of existing schemes.

3.5.2. QMSP Scheme Guarantees the LAN Internal Security

Existing schemes generally assume that the interior of LAN is a trusted area. However, in practical applications, malicious users can eavesdrop on the transmitted quantum key in the trusted area. The proposed QMSP scheme adopts the preset quantum key strategy to keep $QK_{(GI_i,16)}$ in the quantum key gateway. By using the AES-128 symmetric encryption algorithm, the quantum key sent from the commercial supermarket server to the quantum key gateway is encrypted. Meanwhile, the gateway replaces the preset key with the obtained quantum key to ensure the one-time pad encryption characteristic of the key.

4. Experimental Results and Analysis

To verify the feasibility and efficiency of the proposed QMSP scheme, the algorithm to obtain the key by the quantum key gateway of the commercial supermarket is constructed, and the experimental results are analyzed. The QKD device used is Quantum-CTEK QGW, where the frequency is 40MHz, the signal wavelength is 1550nm, the signal pulse is 200, and the detector dark count is less than or equal to $\leq 5\times10^{-6}$. The topological structure of the network is illustrated in Figure 3. KJCS represents the key generation control server, which is used to control the quantum key distribution process for the entire quantum optical fiber link; SIP represents the SIP server, which is used to establish the SIP user; and Log represents the log server, which is used to check the operating state of the entire quantum optical fiber line.

The quantum key gateway uses the ARM9 demo board of mini2440, Samsung S3C2440 microprocessor, 256M Nand Flash, and 4.3-inch touch screen. The QR code generation software is QT4.7.

The processor of the commercial supermarket server is Inter Core i5-8500 3.0GHz with 8GB memory. The operating system is 64-bit windows7.

First of all, to verify the coding rate of the QKD device, different lengths of the quantum key distribution link are designed and tested where 1550nm single mode optical fiber is used. The results are shown in Figure 4, where the x-axis denotes the quantum key distribution time and the y-axis denotes the coding rate of the QKD device. As shown in Figure 4, the coding rate of the QKD device decreases with the increase in the length of the quantum key distribution link.

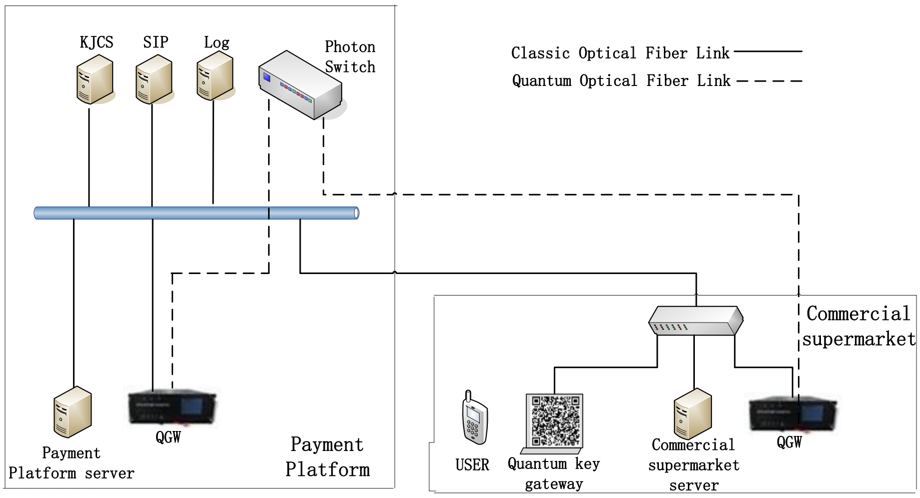

Figure 3. Topological structure of network

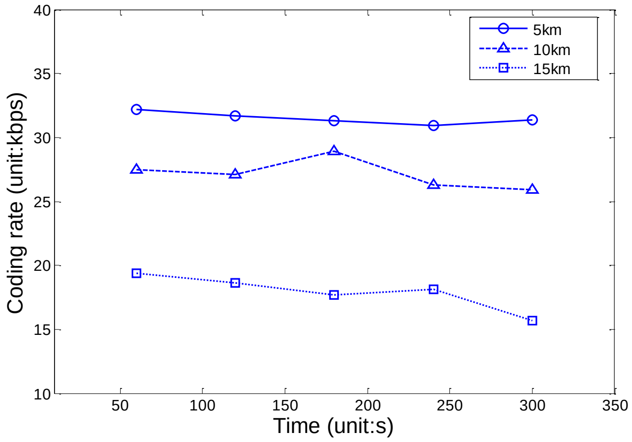

Figure 4. Coding rates of different quantum key distribution link lengths

Next, in order to choose a suitable quantum key encryption algorithm of the QMSP scheme, we test the responding time of the commercial supermarket server with multiple users and different algorithms. The plaintext length of the key is 16 bytes. The x-axis is the number of visits to the quantum key gateway, and the y-axis is the average responding time of the commercial supermarket server. From the comparison results shown in Figure 5, we can see that the time efficiency of the AES-128 encryption and decryption algorithm is better than that of other algorithms. Therefore, the encryption and decryption algorithm to obtain the quantum key adopted in this paper is AES-128.

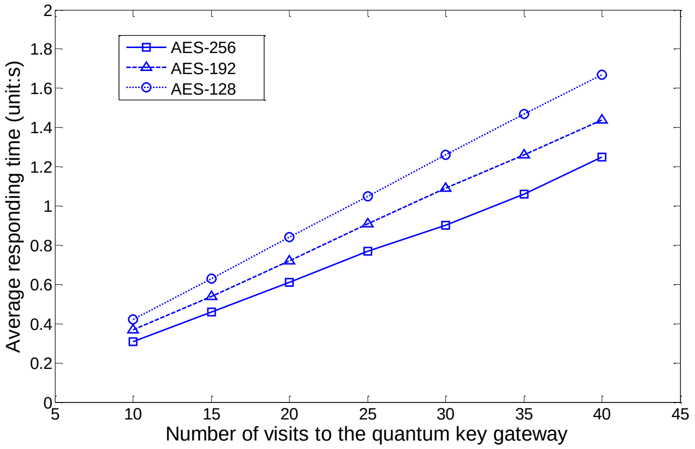

Figure 5. Average responding time of the commercial supermarket server with different algorithms

Finally, in the case of multiple accesses with different users, we verify the average responding time of the commercial supermarket server when the quantum key gateway generates QR codes with different lengths. The encryption and decryption algorithm to obtain the key by the quantum key gateway is AES-128. The results are shown in Tables 1-3. We can see that the average responding time of the commercial supermarket server is in direct proportion to the number of visits to the quantum key gateway. With the same number of visits, the time to obtain QR codes with different key lengths from the commercial supermarket server is roughly the same.

Table 1. 8-byte key plaintext information

Number of visits to the quantum key gateway	10	15	20	25	30	35	40
Average responding time of the commercial supermarket server	0.60	0.91	1.21	1.50	1.81	2.10	1.49

Table 2. 24-byte key plaintext information

Number of visits to the quantum key gateway	10	15	20	25	30	35	40
Average responding time of the commercial supermarket server	0.61	0.91	1.20	1.51	1.81	2.11	2.24

Table 3. 40-byte key plaintext information

Number of visits to the quantum key gateway	10	15	20	25	30	35	40
Average responding time of the commercial supermarket server	0.61	0.90	1.23	1.49	1.80	2.09	2.39

5. Conclusions

A quantum key-based mobile security payment scheme was proposed in this paper. The proposed scheme fully utilized the characteristics and advantages of the quantum key to design the quantum key gateway for key extraction. First, the QKD devices of both payment sides generate the quantum key through the quantum link. Then, the quantum key gateway is preset using the 16-byte key. The quantum key gateway obtains the quantum key through the AES-128 algorithm, and the QR code is generated. Finally, the mobile device scans the QR code and adopts the one-time pad encryption scheme to transmit the payment information to the payment platform. The proposed scheme not only guaranteed the security of the symmetric quantum key generation in WAN, but also prevented malicious users from eavesdropping on the transmitted plaintext quantum key in LAN. It solved the problem of secure transmission of the payment information in the network.

Acknowledgements

This work is supported by the Science and Technology of Jilin Province Development Plan Projects (No. 20170204023GX) and the Education Department of Jilin Province (No. JJKH20191202KJ, JJKH20170496KJ, and JJKH20191201KJ).

References

1. S. Li and X. Y. Li, “Mobile Secure Payment Solution based on Encrypted SMS Verification Code,” *Journal of Computer Applications*, Vol. 37, No. 8, pp. 2270-2274, August 2017
2. Y. Liu and H. Y. Ge, “NFC Security Payments Protocol with Cloud of Secure Elements,” *Computer Engineering and Design*, Vol. 38, No. 9, pp. 2363-2368, September 2017
3. F. Xu and Y. J. Ye, “Design and Practice of a New Campus Card Payment System in Mobile Internet Scenarios,” *Journal of Zhejiang University*, Vol. 45, No. 1, pp. 60-64, January 2018
4. R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, et al., “Using Quantum Key Distribution for Cryptographic Purposes: A Survey,” *Theoretical Computer Science* , Vol. 560, No. 1, pp. 62-81, December 2014
5. D. X. Zhu, X. H. Li, R. K. Wei, J. N. Wu, and L. J. Song, “A Quantum Identity Authentication Protocol based on Optical Transmission and Face Recognition,” *International Journal of Online Engineering*, Vol. 14, No. 4, pp. 58-69, April 2018
6. J. W. Han, R. H. Liu, X. Sun, and L. J. Song, “Identity-based Encryption Scheme based on Cloud and Quantum Keys,” *Journal of Jilin University* (*Engineering and Technology Edition*), Vol. 48, No. 2, pp. 551-557, March 2018
7. J. Q. Wang, Z. C. Ma, X. Z. Li, L. Sun, and C. W. Hu, “Quantum Secure Communication Network Architecture and Mobile Application Solution,” *Telecommunications Science*, No. 9, pp. 10-19, 2018
8. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, et al., “Field Test of Quantum Key Distribution in the Tokyo QKD Network,” *Optics Express*, Vol. 19, No. 11, pp. 10387-10409, 2011
9. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, et al., “Provably Secure and Practical Quantum Key Distribution Over 307km of Optical Fibre,” *Nature Photonics*, Vol. 9, pp. 163-168, December 2015
10. A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, “Real-World Two-Photon Interference and Proof-of-

Principle Quantum Key Distribution Immune to Detector Attacks," *Physical Review Letters*, Vol. 111, No. 13, pp. 130501, October 2018

11. D. Liu, S. Wang, J. Zhou, M. L. Xu, W. Chen, and Z. P. Han, "Application of Quantum Keys in SSL VPN of Power Grid," *Power System Technology*, Vol. 38, No. 2, pp. 544-548, February 2014
12. Z. B. He, Z. P. Cai, Q. L. Han, W. T. Tong, L. M. Sun, and Y. S. Li, "An Energy Efficient Privacy-Preserving Content Sharing Scheme in Mobile Social Networks," *Personal and Ubiquitous Computing*, Vol. 20, No. 5, pp. 833-846, 2016
13. G. L. Sun, T. Chen, Y. Y. Su, and C. L. Li, "Internet Traffic Classification based on Incremental Support Vector Machines," *Mobile Networks and Applications*, Vol. 23, No. 4, pp. 1-8, 2018
14. G. C. Guo, H. Zhang, and Q. Wang, "Review on Development of Quantum Information Technology," *Journal of Nanjing University of Posts and Telecommunications*, Vol. 37, No. 3, pp. 1-14, March 2017
15. X. P. Yang, H. T. Chen, L. C. Mei, and P. Z. Wang, "Research on Quantum Key Distribution Technology in Intelligent Substation," *Telecommunications Science*, No. 10, pp. 163-169, October 2018
16. S. K. Liao, W. Q. Cai, W. Y. Liu, L. Zhang, Y. Li, J. G. Ren, et al., "Satellite-to-Ground Quantum Key Distribution," *Nature*, Vol. 549, pp. 43-47, September 2017
17. J. Huang, B. Xi, P. Li, F. Zhang, and X. J. Zhao, "Method for Detecting Wiretapping Attack in Satellite Network based on Quantum Cryptography," *Computer Science*, Vol. 43, No. 7, pp. 157-161, July 2016
18. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Dey Distribution and Coin Tossing," in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175-179, January 1984

Dexin Zhu is a lecturer in the School of College of Computer Science and Technology at Changchun University and studies computer applications and quantum communication. E-mail address: 38925023@qq.com.

Xiaohui Li is an associate professor in the School of College of Computer Science and Technology at Changchun University and studies computer applications and quantum communication.

Jianan Wu is an associate professor in the School of College of Computer Science and Technology at Changchun University and studies computer networking technology.

Lijun Song is a professor in the School of Institute for Interdisciplinary Quantum Information Technology at Jilin Engineering Normal University and studies quantum information.