Experimental Research on Application of Quantum Key in Video Conference System

https://doi.org/10.3991/ijoe.v14i04.8376

Dexin Zhu, Jianan Wu
Changchun University, Changchun, Jilin Province, China

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

Rongkai Wei, Xiaohui Li, Wei Wang
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—Data transmission in the traditional video conferencing system faces certain security risks currently. Therefore, this study proposed an experimental scheme for the application of quantum key in the traditional video conferencing system. According to this scheme, the quantum gateway was seamlessly embedded into the traditional video conferencing system, based on which the data transmitted through the video conferencing system could be encrypted by the quantum key generated by such quantum gateway. A new quantum key expansion algorithm was put forward because of the relatively low code generation rate of the quantum key of quantum gateway, and the feasibility of the algorithm was verified using the National Institute of Standards and Technology frequency test standard. Quantum keys with different error rates were used to conduct encryption and decryption of three 720p single-screen video images. Moreover, the peak signal-to-noise ratio of the original and decrypted images was calculated. A comparison between these values and theoretical values proved that the quantum key could ensure a normal image quality of the video. This study is of great significance for applying quantum key in the real video conferencing systems and ensuring the security of video data transmission.

Keywords—PSNR, quantum gateway, quantum key, video conference system

1 Introduction

At present, the world has entered into the information era, for which enterprises need video conferences based on more efficient, convenient, and advanced multimedia communication technology to realize increasingly frequent cross-region communications and quick decision-making. During video conferences, many contents require internal confidential information of enterprises, governments, and armies. Hence, security of such video data is of crucial importance. If such data are maliciously attacked or stolen, markets, societies, and countries are seriously impacted, which is an obstacle in the development of video technology at present. Hamidouche [1] proposed a real-time selective video encryption solution in the scalable extension of High-Efficiency Video Coding standard to meet the security requirements of video communications. Rohara [2] proposed data hiding with codeword substitution in encrypted MPEG-4(Moving Picture Experts Group 4) videos. However, with the rapid development of computer technology, the central processing unit has been characterized by increasingly rapid arithmetic speed and powerful decryption capability. Especially, quantum computers will come up in the future, for which encrypting video data will be increasingly difficult due to the complexity of mathematical algorithm to meet the high degree of confidentiality requirements in video conferencing.

Quantum communication is a newly developed subject combining quantum physics and cryptology, which serves as a new cryptosystem realizing cryptographic thought using methods in quantum physics. Quantum communication technology can realize encrypted communication based on the physical properties of quantum state and theories of quantum physics and is generally recognized as a provable secure secret communication technology [3]. The basic thought of quantum communications was put forward mainly by Bennett et al. successively during the 1980s and 1990s, which mainly included quantum key distribution (QKD) [4] and quantum teleportation [5]. The current QKD technology can realize 400-km-magnitude wired QKD [6] and free-space QKD [7]. The QKD technology based on the fundamental principles of quantum mechanics can establish unconditional security key between two parties involved in communication. Therefore, its practicability in the quantum network has gained increasing attention. Liu [8] put forward a plan for integrating the existing classic wireless communication network and quantum network. Kelley [9] proposed a quantum network security framework for the cloud. Petrila [10] analyzed the effect of disabled neurons in classical and quantum networks information processing. Although various studies provided some plans for contents related to quantum network, they included no specific analysis based on a certain application.

Therefore, an experimental strategy on the application of quantum key in video conferencing system was designed in this study. This study not only established a networking scheme for seamlessly connecting the quantum gateway to the video conferencing system but also put forward a quantum key expansion algorithm based on the fact that quantum key generation rate is lower than encryption consumption rate of quantum key and thus realizes absolutely secure communication of video data characterized by the one-time pad. This study is of great significance for the application of quantum key in the actual video conferencing systems and guarantees the safety of video data transmission.

2 Networking Scheme for the Experiment

Figure 1 represents a quantum key video conferencing system that cannot be wiretapped. In this system, the key distribution technology is used to realize the sharing of quantum key between the receiver and the sender. Video terminals can obtain a quantum key from the quantum key transmitting device, for which video data is encrypted based on the "one-time pad" key system. Encrypted data can be transmitted to other vide terminals through the classic network, and such video terminals can realize decryption by using the shared quantum key and display video data.

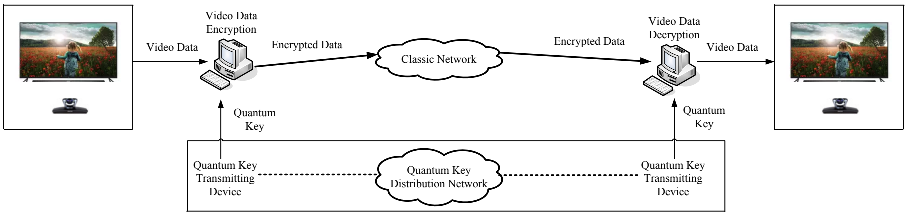

Fig. 1. Overview of video conferencing system based on the quantum key.

In the present study, the three-node quantum communication network and classic network were combined. The topology of the designed video conferencing system based on the quantum key is indicated in Figure 2.This system comprised the following:

1. The dotted line represents the quantum optical fiber line, which was used for the distribution of quantum key. Arrow represents the classic optical fiber line, which was used as the encryption communication line for the video conferencing system.
2. Each of the Bob end and the Alice end of the quantum optical fiber line needed its own quantum gateway and soft gateway. The soft gateway could read the quantum key through the quantum gateway. The quantum keys of all Alice end at the opposite end were stored at the soft gateway of Bob end, and the quantum keys of Bob end at the opposite end were stored at the Alice end.
3. The (4 × 8)-matrixed photon switcher in the quantum optical fiber line can realize interconnection of the internal and external optical ports.
4. KGCS in the classic optical fiber line represents the key generation control server, which could be used to control the QKD process of the entire quantum optical fiber link. SIP(Session Initiation Protocol) represents the SIP server, which was used to establish the SIP user. Log represents the log server, which was used to check the operating status of the entire quantum optical fiber line.
5. Each terminal node could be directly connected to office applications, such as voice telephone and fax, or to the office data subnetwork, and the quantum gateway could serve as a firewall outlet of the subnetwork. When secure communication between internal IP transaction data and external section was conducted, it was necessary to realize such communication through the quantum gateway.

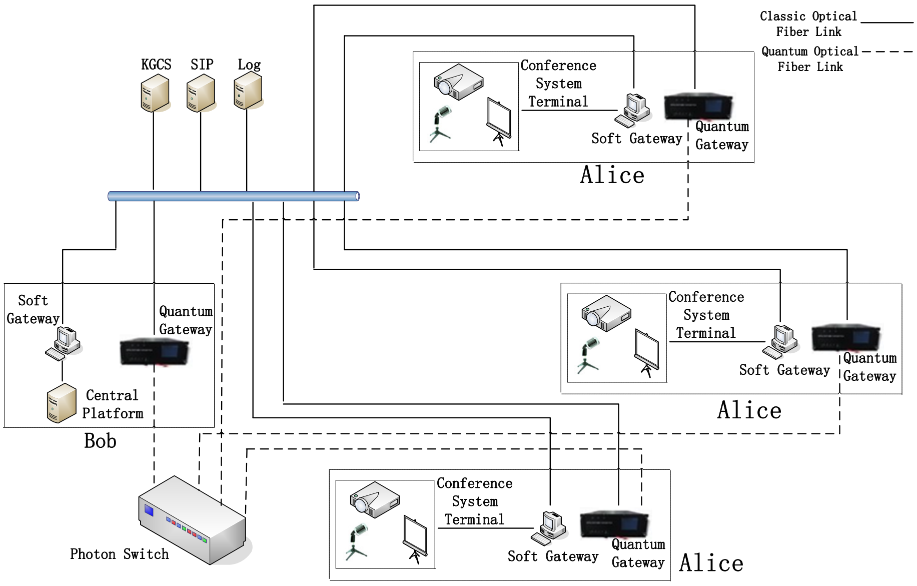

Fig. 2. Network topology of video conferencing system based on the quantum key.

The video conferencing system based on the quantum key was an IP data network, for which the H.323 system standard was adopted, including one central platform and three remote conference system terminals. The video conferencing system was constructed on a quantum secure communication network to ensure high-credibility information security of video conference. The central platform was composed of a specialized server, used for information transmission of conference information of various remote conference rooms. Various conference system terminals were connected to the central platform through the classic network. Various terminals were equipped with quantum gateway and high-definition video conference front end, which were responsible for receiving video images sent by the central platform and sending those images collected by local high-definition cameras to the central platform. Moreover, each terminal was equipped with a set of omnidirectional digital microphone, which could realize on-site sound collection at each video conference room and high-definition LCD TV(Liquid Crystal Display Television) that could realize image display on the LCD TV. Sound and video images of each conference room were seamlessly connected to quantum devices in the IP data transmission link, which could realize secure transmission of IP network data under the premise of no damage to the classic way of information data transmission.

3 Experiment and Analysis

3.1 Quantum Key Expansion Algorithm

For the application of quantum key in the video conferencing system, the mechanism of “one-time pad” was adopted to realize secure communication. For this, the plaintext data set was *P*(1), *P*(2), *P*(3), ... *P*(*i*), and the quantum key set was *K*(1), *K*(2), *K*(3), ... *K*(*i*). If the encryption algorithm of exclusive-or operation for each bit of plaintext and key was used to generate ciphertext *C*(*i*), then the encryption expression should be as follows:

$$C(i) = P(i) \oplus K(i) \tag{1}$$

Therefore, calculating the relation between the quantity of quantum key generation and quantity of quantum key consumption was necessary.

Quantity of Quantum Key Generation. The BB84 protocol was used for the QKD process of quantum communication network, and the formula for secure key rate of the BB84 protocol specific to commonly used weak coherent light in practice was provided through the GLLP （Gottesman Lo Lütkenhaus Preskill） formula [11]:

$$R \geq q\left\{-Q_u f(E_u)\right\}H_2(E_u) + Q_1\left[1 - H_2(e_1)\right] \tag{2}$$

where q indicates pair-base efficiency and BB84 should be 50%; Q_u represents the probability that optical pulse with an average photon number of u can be detected at the receiving end; E_u is the total quantum error rate; *f*(*E*$_u$) represents the efficiency of error correction; Q_1 represents the probability that a single-photon pulse can be sent and detected by the receiver end; and e_1 represents the error rate caused by the single-photon pulse.

For the QKD experiment of a three-node quantum communication network, an indoor single-mode optical fiber with an inner diameter of 9 µm, an outer diameter of 125 µm, and a wavelength of 1550 nm was adopted. After the generation of quantum key, the quantity of quantum key generation and code generation rate of quantum key were recorded every 0.5 m, as indicated in Table 1:

Table 1. Quantity of quantum key generation

Time (m)	***0.5***	***1***	***1.5***	***2***	***2.5***	***3***	***3.5***	***4***	***4.5***	***5***
Key quantity(*k*)	194.25	372.95	566.30	759.76	954.37	1147.87	1340.93	1536.24	1692.39	1887.31
Code generation rate (kbps)	45	47.6	51.4	55.2	48.2	55.3	51.4	48.5	45.2	52

Quantity of Quantum Key Consumption. The quantity of quantum key consumption depended on the volume of image data, for which the higher the resolution of images and the deeper the depth of images, the real the digitized images and the bigger the data volume would be. The volume of image data could be calculated using the following formula:

Data volume of image = Total number of pixels of image × image depth/8 (3)

Data volumes based on different resolutions and different depths are indicated in Table 2.

Table 2. Image data volumes

Image depth	**Image resolution**				
	320 × 240	***640 × 480***	***800 × 600***	***1280 × 720 (Standard high definition)***	***1920 × 1080***
3	28.13k	89.06k	175.78k	337.5k	759.38k
16	150k	475k	937.5k	1800k	4050k
24	225k	712.5k	1406.25k	2700k	6075k

To ensure clear images and no pause of video conferencing system, the definition and frame frequency of the single-screen video used in this study were set as 720p and 30fps, respectively, for which video coding standard was H.264 [12] and data compression ratio was 102:1. Therefore, the relationship between the quantity of quantum key consumption and that of quantum key generation is indicated in Figure 3.

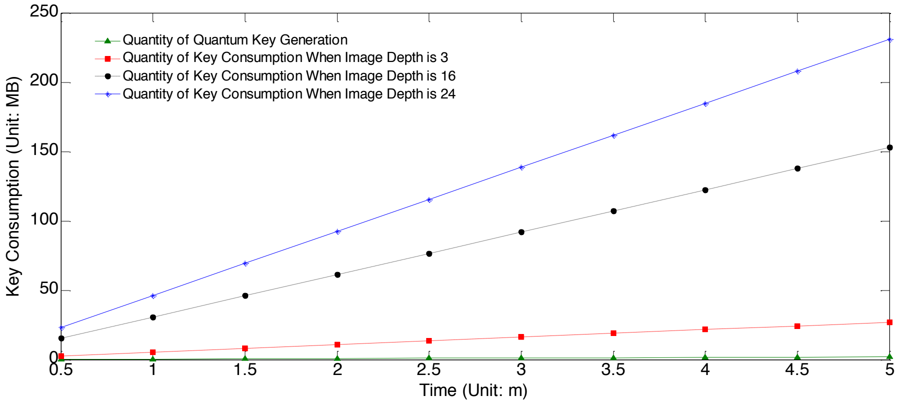

Fig. 3. Comparison between the quantity of quantum key generation and quantity of quantum key consumption.

As indicated in Figure 3, the quantity of quantum key generation of quantum gateway was smaller than the quantity of quantum key consumption for video encryption in the same period of time. The expansion of the quantum key was necessary to meet the requirement of "one-time pad" encryption scheme.

Quantum Key Expansion Algorithm. A new quantum key expansion algorithm was put forward in this study for the requirement of "one-time pad" encryption scheme for video conferencing system, and the feasibility of the algorithm was verified using the National Institute of Standards and Technology (NIST) frequency test standard, including the 16 test methods [13].

The binary sequence of quantum key obtained from various soft gateways was represented as follows: $T=\{t_1,t_2,\ldots,t_i,t_{i+1},\ldots,t_{1024}\},t_i\in\{0,1\},(i=1,2,\ldots,1024)$. The sequence of storage space of quantum key after the expansion was $K=\{k_1,k_2,\ldots,k_i,k_{i+1},\ldots,k_n\},k_i\in\{0,1\},(i=1,2,\ldots,n)$. On the basis of the sliding window principle, the procedures of quantum key expansion are indicated in Figure 4. The description of the algorithm used was as follows:

1. The quantum key sequence *T* with a length of 1024 was copied into sequence *K*.
2. The operation of $\{k_i\oplus k_{i+1}\},(i=1,2,\ldots,n)$ for adjacent quantum keys k_i and k_{i+1} was conducted in sequence *K*, and the result was stored in an unoccupied space of sequence *K*.

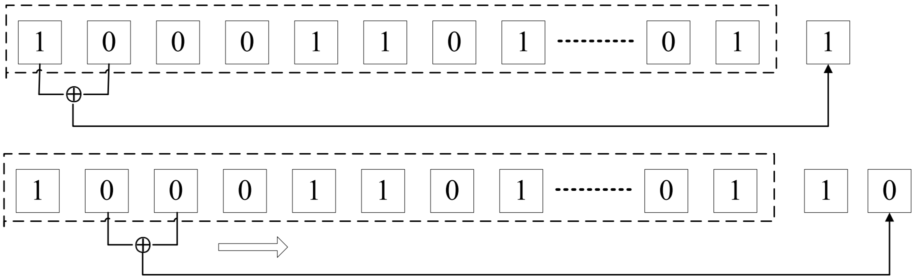

Fig. 4. Procedures for quantum key expansion.

3. The operation in Step 2 was repeated based on the quantity of keys to be consumed until the demand of consumption was met.

The frequency test provided by NIST could serve as the most fundamental proof for determining whether a sequence was nonrandom. The test for this was described as follows:

1. A quantum key sequence $T=\{t_1,t_2,\ldots,t_i,t_{i+1},\ldots,t_{1024}\},t_i\in\{0,1\},(i=1,2,\ldots,1024)$ with a length of 1024 was acquired. On the basis of the formula $k_i=\{2\times t_i-1\},(i=1,2,\ldots,1024)$, k_i was converted into ±1 and $S=\{k_1+k_2+\cdots+k_{1024}\},k_i\in\{-1,1\},(i=1,2,\ldots,1024)$ was acquired.

The statistical value of the test was calculated as follows: $S_{obs} = \dfrac{|S|}{\sqrt{2014}}$

2.

3. According to the definition of error function: $erf(x) = \dfrac{2}{\sqrt{\pi}}\int_0^x \exp(-z^2)dz$ and the definition of complementary error function: $erfc(x) = 1 - erf(x) = \dfrac{2}{\sqrt{\pi}}\int_x^0 \exp(-z^2)dz$, the $P\text{-value} = erfc\left(\dfrac{S_{obs}}{\sqrt{2}}\right)$ was calculated.
4. The $P\text{-value} \geq 0.01$ was calculated, indicating that the tested sequence was a random sequence.

A three-node quantum communication network was activated in this study to verify the feasibility of quantum key expansion algorithm, based on which multiple groups of quantum keys under different signal-state error rates and decoy-state error rates were collected. Of these, six groups of quantum keys were selected for expansion operation and then subjected to frequency test. The result of the frequency test is indicated in Table 3.

Table 3. Result of frequency test

Number of key groups	**Key length (bit)**						
	1024	***2048***	***3072***	***4096***	***5120***	***6144***	***7168***
1	0.7513	0.9062	0.4592	0.1988	0.1185	0.1804	0.1503
2	2.2980	1.8125	1.3778	1.3258	1.5416	1.1907	0.9688
3	2.0329	1.7500	1.7350	1.3921	1.3637	1.3892	1.8374
4	1.8561	1.6250	1.8626	1.1490	1.4625	1.0644	1.0690
5	2.9168	2.2187	2.3729	2.2318	2.5693	2.3094	1.9376
6	1.8119	0.875	0.6634	0.2651	0.1185	0.2706	0.1503

Table 3 indicates that after expansion operation on the original sequence using quantum key expansion algorithm, the new sequence could still maintain its randomness, thereby proving that this algorithm was feasible.

3.2 Impact of Error Rate of Quantum Key on Image Quality

The image quantity was seriously affected after encryption and decryption of video data using quantum key due to the error rate of quantum key in the process of generation. The objective assessment method for image quality was to solve the error between original images and those images received by a terminal. In the present study, the peak signal-to-noise ratio (PSNR) of original images and decrypted images was calculated to verify the quality of video images. PSNR referred to the logarithm of mean-square error between the original and processed images versus $(2^n - 1)^2$ (square of the maximum value of the signal, in which *n* refers to the bit number of each sampling value), for which the value range was PSNR □ [20,40]. The higher the

PSNR value, the higher the quality of video images. The mathematical formula used was as follows:

$$\mathrm{PSNR} = 10 \times \log_{10}\left[\frac{(2^n-1)^2}{\mathrm{MSE}}\right] \tag{4}$$

where MSE is the mean-square error between the original and processed images. The mathematical formula for MSE was as follows:

$$\mathrm{MSE} = \frac{\sum_{0 \le i \le M} \sum_{0 \le j \le N} \left(f_{ij} - f_{ij}^{'}\right)^2}{M \times N} \tag{5}$$

where f_{ij} and $f_{ij}^{'}$ refer to the corresponding frame of the original reference video and the corresponding frame of the distorted video and M and N refer to the height and width of the video frame, respectively.

In the present study, Foreman, Claire, and Calendar high-definition images of three single-screen videos with the definition of 720p were selected. The error rate of quantum key was first set as $er = \{0.5\%, 1.0\%, 1.5\%, 2.0\%, 2.5\%, 3.0\%, 3.5\%, 4.0\%, 4.5\%, 5.0\%\}$ to verify the impact of the error rate of quantum key on the image quality, and then these three images were encrypted and decrypted and the PSNR values of images with different error rates were finally calculated. Tables 4, 5, and 6 indicate that when the error rate of quantum key was $er \le 5.0\%$, the PSNR value of image belonged to the range of [20, 40].

Table 4. MSE and PSNR values of Foreman

Error rate (%)	**0.5**	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
MSE(dB)	0.0003	0.0006	0.0009	0.0011	0.0014	0.0017	0.0020	0.0022	0.0025	0.0028
PSNR(dB)	35.3513	32.0178	30.5208	29.4893	28.5472	27.7590	27.0566	26.4886	25.9497	25.4536

Table 5. MSE and PSNR values of Claire

Error rate (%)	**0.5**	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
MSE(dB)	0.0002	0.0003	0.0004	0.0007	0.0010	0.0012	0.0014	0.0015	0.0017	0.0018
PSNR(dB)	36.6536	35.1613	33.2441	31.5778	30.1673	29.2800	28.6949	28.1930	27.7459	27.3664

Table 6. MSE and PSNR values of Calendar

Error rate (%)	**0.5**	**1**	**1.5**	**2**	**2.5**	**3**	**3.5**	**4**	**4.5**	**5**
MSE(dB)	0.0002	0.0005	0.0008	0.001	0.0013	0.0015	0.0017	0.0020	0.0022	0.0025
PSNR(dB)	36.0339	32.8152	31.1390	29.9352	28.9670	28.3349	27.7054	27.0883	26.5441	26.0435

In the three-node quantum communication network, the error rate was recorded every 30 s for this study. Then, nine groups with relatively high error rates were selected. The aforementioned three images were encrypted and decrypted using these nine groups with different error rates, and the PSNR values of these images were then calculated. Figure 5 indicates the PSNR values under error rates in the quantum communication network. The PSNR values were larger than 30 dB, indicating that the quality of images before and after encryption and decryption could be guaranteed using quantum keys generated by the three-node quantum communication network.

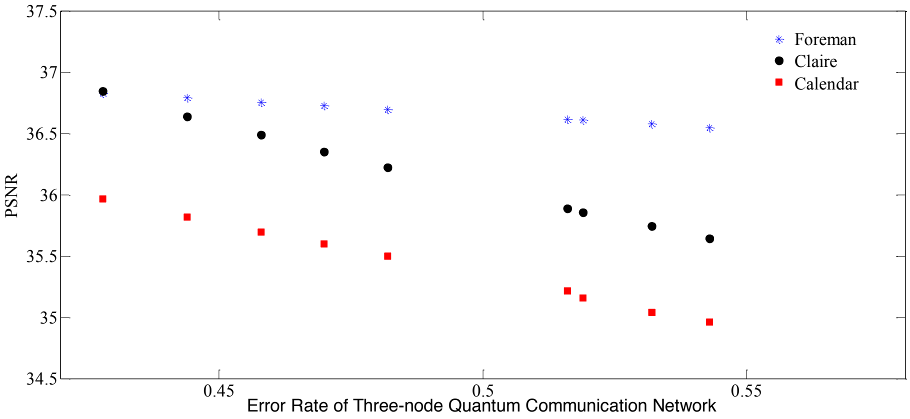

Fig. 5. PSNR values of the three-node quantum communication network under different error rates.

4 Conclusions

In the present study, an experimental scheme for the application of quantum key in video conferencing system was designed, in which a networking scheme combining classic network and quantum communication network was first put forward and a new quantum key expansion algorithm was proposed based on the reality of a relatively low code generation rate of quantum key. According to the sliding window principle, exclusive-or operation for the adjacent key pair was conducted and stored in the expanded storage space of quantum key after each sliding. It could be acquired through the application of NIST frequency test standard that quantum key frequency ≥0.01, namely that quantum key was random after expansion. Therefore, this algorithm was feasible. Finally, quantum keys with different error rates were used to conduct encryption and decryption of three 720p single-screen video images. Moreover, the PSNR of the original and decrypted images was calculated. It could be proved through comparison between such values and theoretical values that the normal image quality of video could be ensured. In this study, the theoretical feasibility of application of quantum key in video conferencing systems was verified, providing an important theoretical support for actual video conferencing systems based on quantum key encryption.

5 Acknowledgment

This study was supported by the Science and Technology of Jilin province development plan projects with grants No. 20170204023GX and the Education Department of Jilin Province with grants No.2016292, No.JJKH20170496KJ.

6 References

[1] Hamidouche, W., Farajallah, M., Sidaty, N., Assad, S. E., Deforges, O. (2017). Real-time selective video encryption based on the chaos system in scalable HEVC extension. Signal Processing Image Communication, 58(0):73–86. https://doi.org/10.1016/j.image.2017.06.007

[2] Rohara, J., Gaikwad, V. B. (2017). Using Codeword Substitution to Hide Data in Encrypted MPEG-4 Videos. IRJET., 04(04): 3276–3280.

[3] Wu, H., Zhao, Y., Zhao, Y., Zhao, M. (2017). Field application and security management of a telephone network and a high speed data transmission system with practical ber quantum cryptography. Scientia Sinica., 44(3): 312–321.

[4] 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.

[5] 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

[6] Yin, H. L., Chen, T. Y., Yu, Z. W., Liu, H., You, L. X. (2017) Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber. PHYS REV LETT., 3(1):74–79.

[7] Nguyen, H. V. ,Trinh, P. V., Pham, A. T., Babar, Z., Alanis, D. (2017). Network Coding Aided Cooperative Quantum Key Distribution Over Free-Space Optical Channels. IEEE Access,5(99): 12301-12317. https://doi.org/10.1109/ACCESS.2017.2712288

[8] Liu, X. H., Pei, C. X., Nie, M. (2014). Quantum wireless communication network model and performance analysis. Journal of Jilin University, 44(4):1177–1181.

[9] Kelley, B.,Prevost, J. J., Rad, P., Fatima, A. (2016). Securing Cloud Containers Using Quantum Networking Channels. IEEE International Conference on Smart Cloud, 103-111. https://doi.org/10.1109/SmartCloud.2016.58

[10] Petrila, I., Luca, B., Manta, V. (2016). Effects of disabled neurons in classical and quantum networks information processing. System Theory, Control and Computing (ICSTCC), 2016 20th International Conference on, 699-703. https://doi.org/10.1109/ICSTCC.2016.7790748

[11] Gottesman, D., Lo H. K., Preskill, J. (2004). Security of quantum key distribution with imperfect devices. Quantum Information & Computation,4(5):325-360. https://doi.org/10.1109/ISIT.2004.1365172

[12] Zach, O., Seufert, M., Hirth, M., Slanina, M., Tran-Gia, P. (2017). On use of crowdsourcing for H. 264/AVC and H. 265/HEVC video quality evaluation. Radioelektronika (RADIOELEKTRONIKA), 2017 27th International Conference, 1-6.

[13] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E. (2015). A statistical test suite for random and pseudorandom number generators for cryptographic applications. Applied Physics Letters, 22(7):1645-1798.

7 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. (38925023@qq.com)

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.

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.

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.

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.

Wei Wang 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.

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 13 March 2018 and 15 March 2018. Final acceptance 30 March 2018. Final version published as submitted by the authors.