Journal of Computers Vol. 32 No. 2, 2021, pp. 164-175
doi:10.3966/199115992021043202014

Multi-level Data Security Program Based on Quantum Key

De-Xin Zhu[1,3], Xin-Jian Li[1], Ya-Ting An[1], Jun-Wei Zhou[1], Qi-Yuan Huang[1], Xiao-Hui Li[1,3], Jia-Nan Wu[1,3], Li-Jun Song[2,3*]

[1] College of Computer Science and Technology, Changchun University, Changchun 130022, China
{zhudx, lixh, wujn}@ccu.edu.cn

[2] Institute for Interdisciplinary Quantum Information Technology, Jilin Engineering Normal University, Changchun 130022, China
songlj@jlenu.edu.cn

[3] Jilin Engineering Laboratory for Quantum Information Technology, Jilin Engineering Normal University, Changchun 130022, China
songlj@jlenu.edu.cn

Received 1 May 2020; Revised 15 May 2020; Accepted 30 May 2020

Abstract. A multi-level data security program based on quantum key is proposed in this paper aiming to improve the security of documents in computers. Since the generation of quantum keys is secure theoretically, incorporating time phase coded quantum key distribution networks into classical networks in this program provides a practical way to achieve dual-network integration. Moreover, a quantum key utilization strategy of three quantum keys, including one-time-pad, 16-byte key AES-128 algorithm and SM4 algorithm, are employed according to the importance level of the documents based on low quantum key bit rates of commercial optical fibers. Experimental results demonstrate that dual networks can operate steadily and the encryption/decryption for a 10 MB document of the proposed multi-level security device costs less than 10 s. Hence, a high level of protection for data security is realized through the proposed multi-level data security program.

Keywords: quantum key, multi-level data security, one-time-pad

1 Introduction

Numerous applications of computers contribute to the convenience of our life and work, which also carry out potential threats to people's privacy and information security. Viruses and hacker attacks, which lead to computer breakdown, will not only result in the information leakage but also reduce the economic benefits. Data encryption techniques have been developed and used to improve the information security as well as protect the information confidentiality of the users, enterprises and countries by applying complicated encryption and intricate programming, which increases the difficulty of cracking data information. Previous studies have been investigated to meet the increasing requirements of data encryption, leading to the improvement of data encryption in different application areas. Ref. [1] presents methods and tools for GDPR compliance through privacy and data protection engineering; Ref. [2] proposes a new, distributed blockchain-based protection framework to enhance the self-defensive capability of modern power systems against cyber-attacks; In view of the problem of protecting on end users' data stored in Cloud server, Ref. [3] presents a novel data protection method combining Selective Encryption (SE) concept with fragmentation and dispersion on storage; Due to poor ability of resisting attack and poor encryption performance, Ref. [4] puts forward a method of multistage encryption for user

* Corresponding Author

privacy data based on big data; Ref. [5] proposes an attribute-based encryption scheme with the hidden access structure for data security sharing of internet of things, this scheme can achieve fine-grained access control of ciphertext and guarantee data privacy. Ref. [6] proposes a ring-based privacy-preserving aggregation scheme. Nevertheless, the key is generated according to the classical key agreement protocol in the present encryption techniques, which is pseudo-random generated by computer, and thus is potential to be compromised because of the certain rules it follows.

Quantum secure communication realizes the security key distribution between the two remote parties based on the indivisibility of single photon and the no-cloning theorem of quantum state [7], which enables the unconditional secure encrypted communication by combining with one-time pad cryptosystem. Unlike the classical encryption techniques, the security of quantum communication is guaranteed by the fundamental principles of quantum physics, which have been proved to be unconditional secure in theory. In recent years, research studies on quantum key distribution [8-9] have contributed to the construction of practical quantum networks such as quantum satellite networks, quantum metropolitan networks and quantum link networks. Alibaba Cloud, electric power, finance and other industries have practically applied quantum key encryption to various fields [10-14]. The integration of quantum key distribution technology in the present data security program takes full advantages of the physical properties of quantum key, which effectively enhances the system security by combining with the present program.

In this work, a multi-level data security program based on quantum key is presented. In the program, quantum key distribution is developed by time phase coding, which incorporates quantum key distributor into classical networks. Furthermore, a quantum key utilization strategy is proposed, which applies a multi-level encryption/decryption algorithm according to the data level, and therefore realizes multi-level security protection of data.

2 Theories

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) and quantum teleportation. QKD technology is based on BB84 protocol, which uses photon polarization state to transmit information. Uncertainty principle and no-cloning theorem ensure the unconditional security of BB84 protocol. QKD enables both sides of communication to generate random and secure keys to encrypt and decrypt messages.

Current QKD program is composed of five parts, including quantum light source, quantum state preparation, channel, detection and post-processing procedure of quantum state, as shown in Fig. 1.

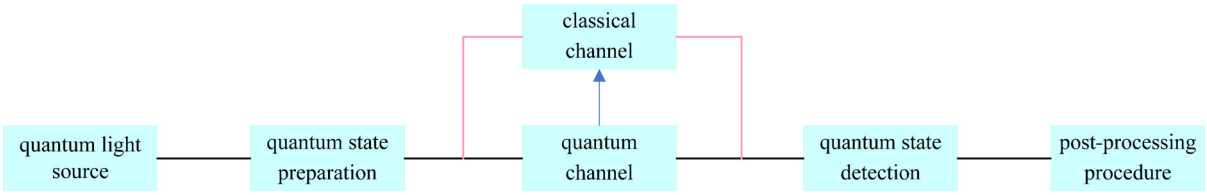

Fig. 1. Quantum key distribution model

2.1 Quantum Light Source

In original BB84 protocols, the modulation and demodulation of a single photon is required. In QKD system, the most widely used is the attenuated laser, which is usually deployed by the combination of a semiconductor laser and an optical attenuator. The coherent light field can be expressed as:

$$\left|\sqrt{\mu}e^{i\theta}\alpha\right\rangle=\left|\alpha\right\rangle \tag{1}$$

$$\left|\alpha\right\rangle=e^{-\mu/2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}\left|n\right\rangle \tag{2}$$

where $\mu = |\alpha^2|$ is the average number of photons. $|n\rangle$ is the photon number state, which represents there are n photon states.

Hence, the probability of n photons in a coherent state with an average photon number of μ per pulse is given by:

$$P(n|\mu) = \frac{\mu^n}{n!} e^{-\mu} \tag{3}$$

2.2 State Preparation

In BB84 protocol, the following set of four states are prepared: $S_{BB84} = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, the probabilities of which are p_1, p_2, p_3 and p_4, respectively. The total probability $\sum_{j=1}^{4} p_j = 1$ and the original BB84 protocol requires that $p_j = 1/4, j = 1,2,3,4$.

2.3 Channel

QKD consists of two channels. One is quantum channel for the transmission of encoded quantum state and the other one is classical channel for classical signal information exchange to achieve post-processing. In both situations, it is not possible to make assumptions about the quantum channel and it is supposed that the eavesdropper Eve can obtain all the information of the channel. Generally, quantum channel is divided into two types according to different transmission medias: optical fiber channel and free space channel.

2.4 State Detection

At the receiving end, the state detection module receives the quantum of light, decodes the quantum state and detects the photon according to the quantum key distribution protocol.

2.5 Post-processing

After the QKD system based on BB84 protocol, the two communication parties hold the virtually same sequences of random numbers, called the sifted key. The difference between them is defined as quantum bit error rate. Moreover, Shannon's information theory gives the theoretical minimum amount of common information exchange required to correct a given message, which can be described by a binary entropy function:

$$f_{er} = -q\log_2(q) - (1-q)\log_2(1-q) \tag{4}$$

where q is the measured quantum bit error rate of the sifted key.

In previous studies, various correction protocols have been proposed to correct the sifted key efficiently. Some protocols are of recursive structures, where multiple iterations are implemented to correct all the errors [15-16], and others are of non-recursive structures, which requires one-step iteration to correct all the errors [17-18].

Due to the information leakage caused by key exchange and correction procedure, the amount of information probably obtained by Eve is desired to be further compressed, which is called privacy amplification.

3 Systematic Design of the Program

3.1 Program Structure

The multi-level data security program based on quantum key includes quantum channel, classical channel, quantum communication device, quantum key server, multi-level security device and computer, which are performed as follows:

quantum channel: for the transmission of quantum state. The quantum signals propagated through quantum channel are limited by several impairments (i.e., scattering and loss). The function between fiber loss and distance is as follows: $\eta = 10^{-\alpha l/10}$. Herein, l is the fiber length and α is the attenuation coefficient of fiber, which is correlated to wavelength and fiber material.

classical channel: for the transmission of classical data.

quantum communication device: quantum communication device performs quantum key distribution through quantum channel, which generates quantum key and then saves it to quantum key server.

quantum key server: quantum key server includes quantum key storage module and quantum key management module. Quantum key storage module is employed to store the generated key from quantum communication device to database while quantum key management module exports the key into multi-level security device, and then deletes the key from database.

multi-level security device: multi-level security device composes of quantum key loading module, quantum key management module and document encryption/decryption module. Quantum key loading module obtains the key from quantum key management server and stores it to database. Quantum key management module moves or deletes the obtained key according to the usage of the key. The document encryption/decryption module consists of the encryption and decryption function of one-time-pad, AES-128 (Advanced Encryption Standard) algorithm or SM4 algorithm.

Computer: computer includes data sending module and data receiving module. Data sending module sends the pending data to multi-level security device; data receiving module obtains the encrypted or decrypted data from multi-level security device.

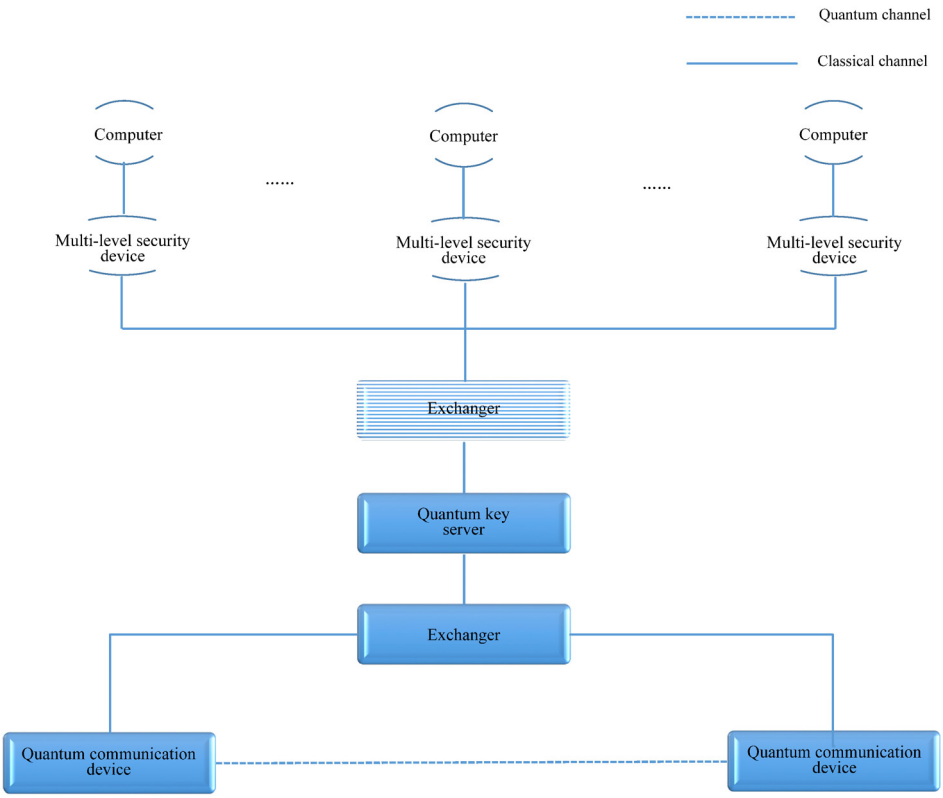

Fig. 2. Structure of multi-level data security program

3.2 Multi-level Security Device Key Utilization Strategy

Multi-level security device database has six datasheets, explained as follows:

(1) quantum key datasheet encrypted by one-time-pad, the key of which is denoted as OPT_{en_qk} ;

(2) quantum key datasheet decrypted by one-time-pad, the key of which is denoted as OPT_{de_qk} ;

(3) quantum key datasheet encrypted by SM4 algorithm, the key of which is denoted as SM_{en_qk} ;

(4) quantum key datasheet decrypted by SM4 algorithm, the key of which is denoted as SM_{de_qk} .

(5) quantum key datasheet encrypted by AES-128 algorithm, the key of which is denoted as AES_{en_qk} ;

(6) quantum key datasheet decrypted by AES-128 algorithm, the key of which is denoted as AES_{de_qk} .

Multi-level security device obtains key from quantum key server, and the key utilization strategy is shown as the following:

(1) load the quantum key into three encrypted quantum key datasheets respectively;

(2) the equipment receives the unencrypted plaintext documents from the computer, which is denoted as $Data_{pt}$;

(3) select encryption algorithm for the document according to the importance level of the document, and the encrypted document is denoted as $Data_{ct}$;

When using one-time-pad encryption algorithm, execute $Data_{ct} = OPT_{de\_qk} \oplus Data_{pt}$, $OPT_{de\_qk} = OPT_{en\_qk}$, and delete OPT_{en_qk} from datasheet; when adopting SM4 encryption algorithm, execute $Data_{ct} = SM4(SM_{en\_qk}, Data_{pt})$, $SM_{de\_qk} = SM_{en\_qk}$, and delete SM_{en_qk} from datasheet; when applying AES-128encryption algorithm, execute $Data_{ct} = AES(AES_{en\_qk}, Data_{pt})$, $AES_{de\_qk} = AES_{en\_qk}$, and delete AES_{en_qk} from datasheet;

(4) the device receives the cryptograph document from the computer, estimates the decoding algorithm, takes the key from the quantum key datasheet, performs decryption and deletes the decryption key simultaneously.

3.3 Data Processing Program in Multi-level Security Device

According to the importance level of the document, the proposed program designs three different data encryption functions: one-time-pad, AES-128 algorithm and SM4 algorithm. One-time-pad adopts the exclusive-or operation of ciphertext and plaintext. The length of key in AES-128 algorithm and SM4 algorithm is 16 bytes. The procedures of data processing in multi-level data security program is shown in Fig. 3.

The steps of the proposed program are as follows:

(1) start the quantum communication device and generate quantum key. Multi-level security device obtains the quantum key from the quantum key server;

(2) load the quantum key to three encrypted quanta key datasheets;

(3) wait for the data and processing instructions from the computer. If it is an encryption operation, execute (4), otherwise execute (5);

(4) select encryption algorithm according to the processing instruction, extract quantum key from encrypted quantum key datasheets, perform encryption and store the key to the decryption quantum key datasheet;

(5) select decryption algorithm according to the processing instruction, extracts quantum key from decryption quantum key datasheets, performs decryption and deletes the key from the decryption quantum key datasheet;

(6) multi-level security device sends the processed data to computer.

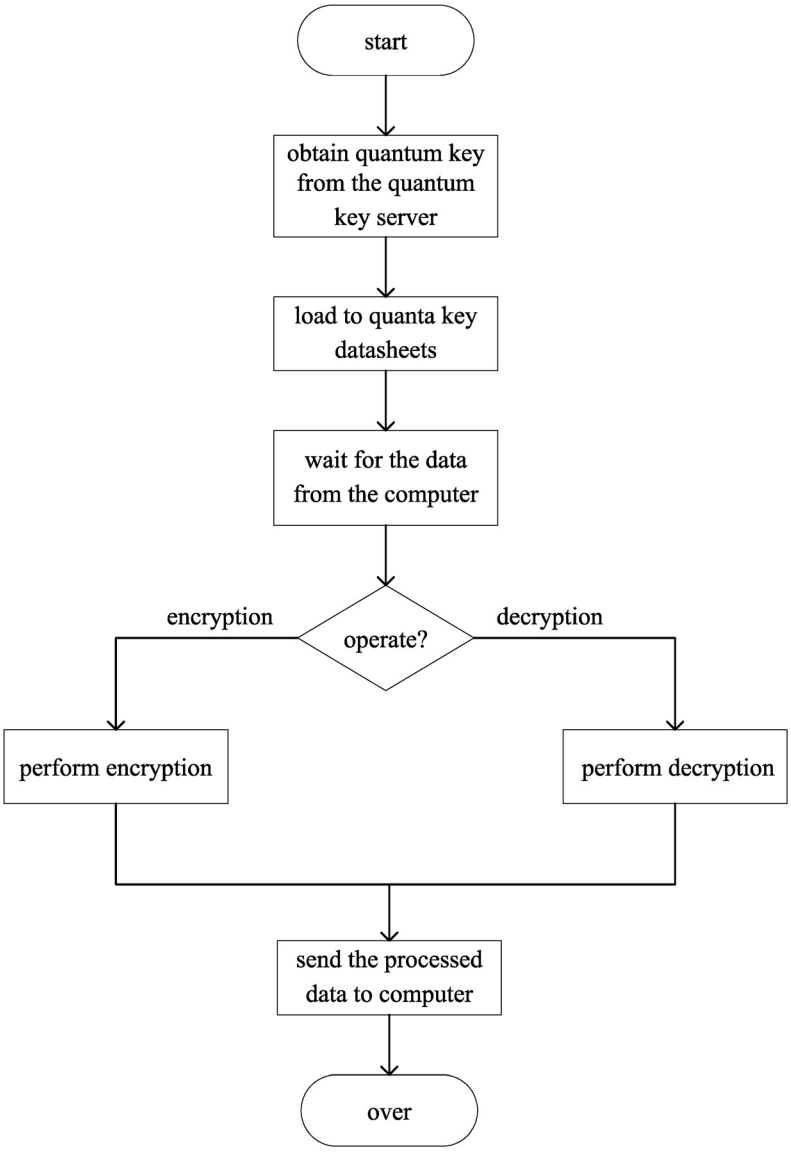

Fig. 3. Procedures of data processing in multi-level data security program

4 Experiments and Data Analysis

4.1 Topology of Program Network

The proposed program combines the time phase quantum key distributor with the classical networks. The designed multi-level data security program network topology based on quantum key consists of two parts: the multi-level security device network topology for getting quantum key and the multi-level security device network topology for using quantum key, as shown in Fig. 4 and Fig. 5, respectively. The architectures are summarized as follows:

(1) Unit A and Unit B are connected by switches with optical modules, and the channels are double core optical fibers, which are respectively used for quantum channels and classical channels. The dotted line represents the quantum channel, which is established for quantum key distribution. The solid line represents the classic channel, which is used for equipment connection, reading quantum key and data transmission. The actual fiber length of Unit A and Unit B is about 33.6 km and the attenuation value of optical fiber links is less than or equal to 18 dB. All the optical fiber links are naked and optical amplifier or other equipment is not included.

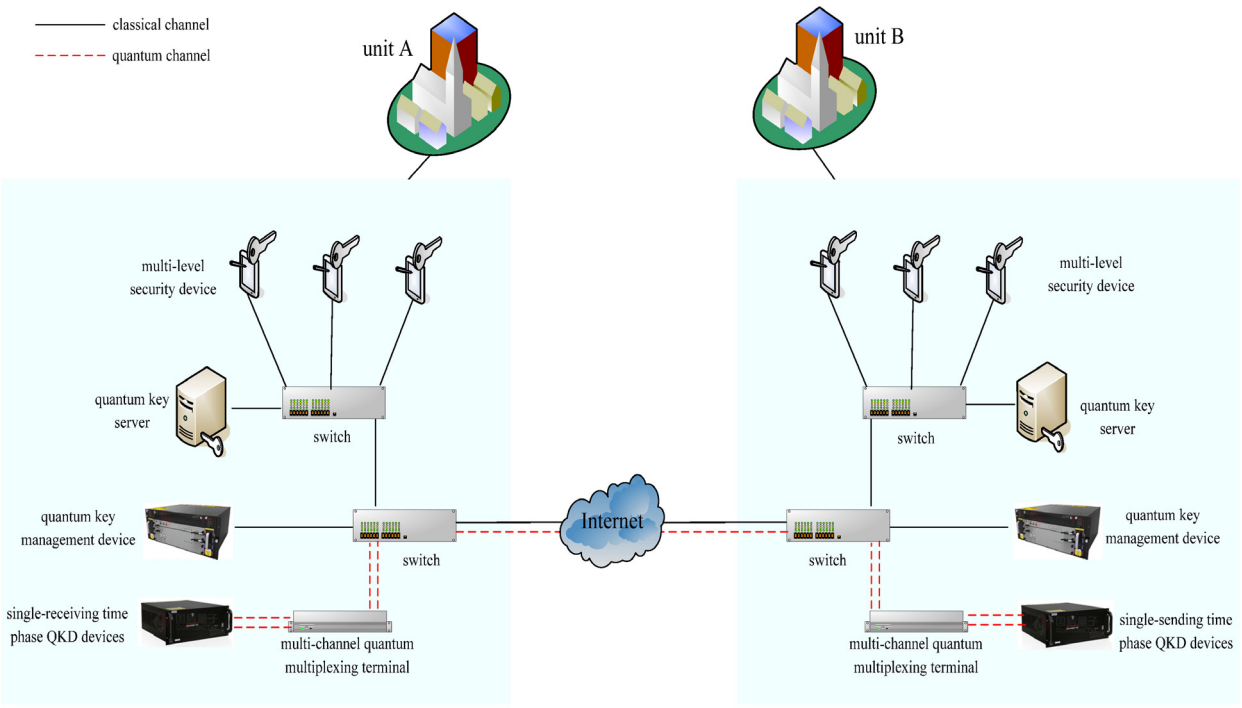

Fig. 4. Multi-level security device for acquiring quantum key topology

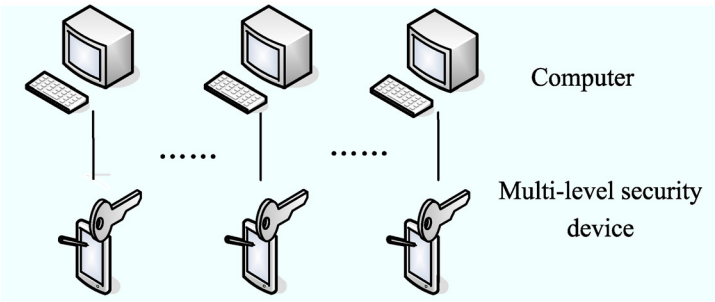

Fig. 5. Multi-level security device for using quantum key topology

(2) Quantum communication devices include single-receiving time phase QKD devices and single-sending time phase QKD devices. The two QKD devices generate key through quantum channel, and store to quantum key management equipment. The quantum key server loads the key from the quantum key management device and stores it to database. Based on the decoy-state BB84 protocol, the QKD device integrates the quantum signal transceivers with operating frequency up to the order of GHz, wavelength of 1550 nm and bandwidth of 200.

(3) The multiple expansion of quantum key distribution rate is realized by multi-channel quantum multiplexing terminal, which converges several QKD devices into the same fiber for transmission through WDM (wavelength-division multiplexing) networks.

(4) Multi-level security device adopts raspberry pi 4B, 64 bit, 1.5 GHz quad-core CPU, 4 GB DDR4 memory, Gigabit Ethernet network card and Linux operating system.

(5) Each computer is directly connected to the multi-level security device, and thus it is impossible for cross encryption and decryption.

4.2 Analysis of Generation of Quantum Key Data

The physical distance between the two ends of the fiber is approximately 33.6 km and the outdoor temperature is-21℃. The quantum key is generated by quantum key distribution on both sides and the

data is loaded with an interval of an hour. The quantum key bit rate and bit error rate are shown in Fig. 6 and Fig. 7, respectively.

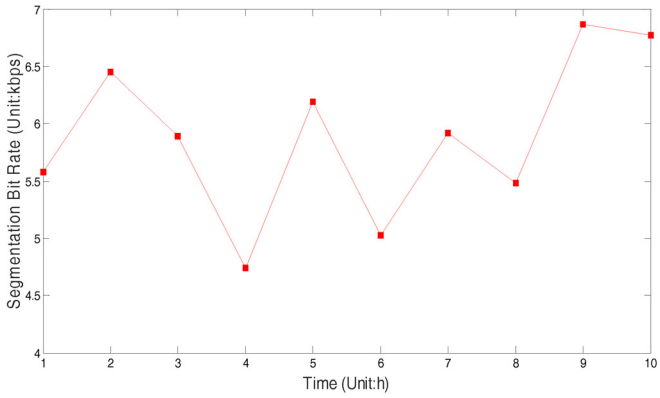

Fig. 6. The quantum key bit rate

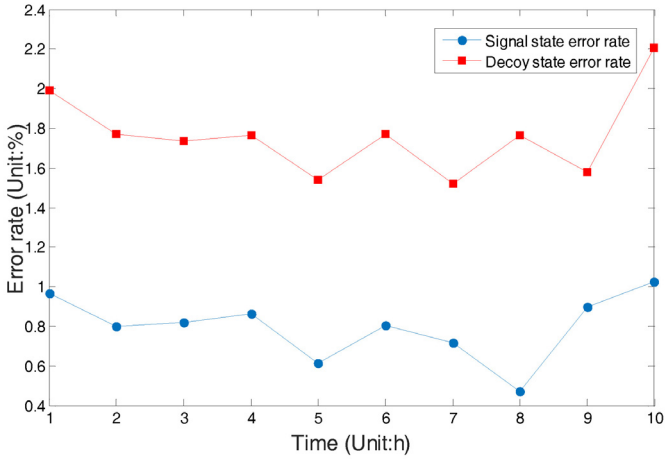

Fig. 7. The quantum key error rate

When the quantum communication device operates stably for 10 hours, the average sifted key per hour is 37.4 kbps. The sifted key is not the final quantum key. It needs to be processed by error reconciliation and privacy authentication. Sifted key can't guarantee the data of Alice and Bob are completely consistent, so it is necessary to correct the data of both sides. Error reconciliation corrects the inconsistent keys of Alice and Bob, reduces the bit error rate and the information obtained by the Eve. Privacy amplification is used to reduce the eavesdropping information of Eve in the process of error reconciliation. After the correction of quantum key distribution post-processing and the privacy amplification, the key length is reduced, and the average final bit rate per hour is 5.9kbps. Due to the low quantum key bit rate, multiple encryption/decryption program is adopted.

4.3 Analysis of Operation Data of Multi-level Security Device

When quantum communication device is operating, quantum key management device gains the key at an average transmission rate of 5.9 KBPS. In addition, the quantum key server loads the key from quantum key management device at a rate of 2kb/s, and saves to database. Multi-level security device requires to prepare key, and connects with computer directly, waiting for the process instructions of computer. The proposed program adopts one-time-pad, AES-128 algorithm and SM4 algorithm respectively, implementing encryption and decryption to text documents and word documents. The experimental results are shown in Table 1 to Table 4. Only ten groups of data are included in the result table. Fig. 8, Fig. 9, Fig. 10, Fig. 11 show the time trend of the three algorithms for text documents and word documents.

Table 1. Encryption table of text documents

Document size (KB)		50	100	200	500	800	1024	3072	5120	8192	11264
Time (ms)	one-time-pad	26	46	84	231	637	475	1644	2384	4905	5650
	AES-128	26	53	68	149	306	336	1149	1605	3472	3780
	SM4	20	64	91	145	418	411	1750	1897	3832	4206

Table 2. Decryption table of text documents

Document size (KB)		50	100	200	500	800	1024	3072	5120	8192	11264
Time (ms)	one-time-pad	32	53	95	241	481	684	1916	2802	4780	6801
	AES-128	20	54	70	158	332	342	1131	1838	3086	6380
	SM4	32	104	181	230	661	844	2291	3836	5611	7935

Table 3. Encryption table of word documents

Document size (KB)		50	100	200	500	800	1024	3072	5120	8192	12288
Time (ms)	one-time-pad	35	58	83	193	325	498	1284	2382	3945	5087
	AES-128	18	73	135	296	305	367	1195	1997	3138	5330
	SM4	29	45	227	176	445	554	1754	2474	3919	5893

Table 4. Decryption table of word documents

Document size (KB)		50	100	200	500	800	1024	3072	5120	8192	12288
Time (ms)	one-time-pad	64	95	105	234	394	616	1645	3301	4929	5913
	AES-128	19	89	134	214	316	384	1257	1881	3099	5307
	SM4	71	50	626	662	1022	1191	3095	4055	5354	6811

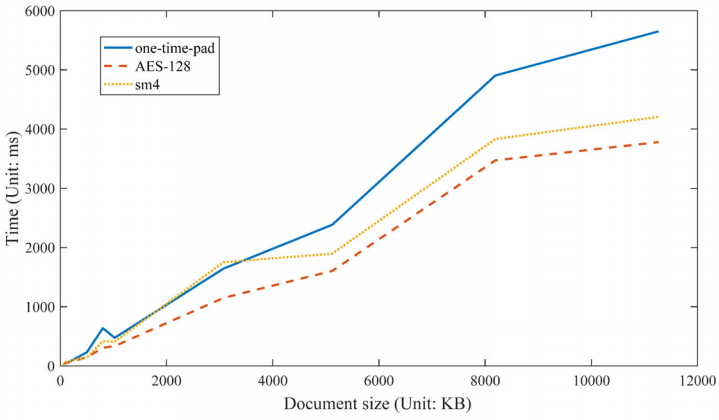

Fig. 8. Time trend of encrypting text documents

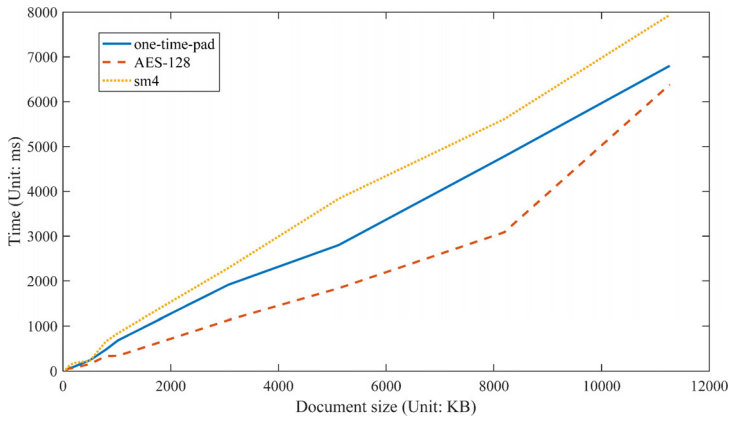

Fig. 9. Time trend of decrypting text documents

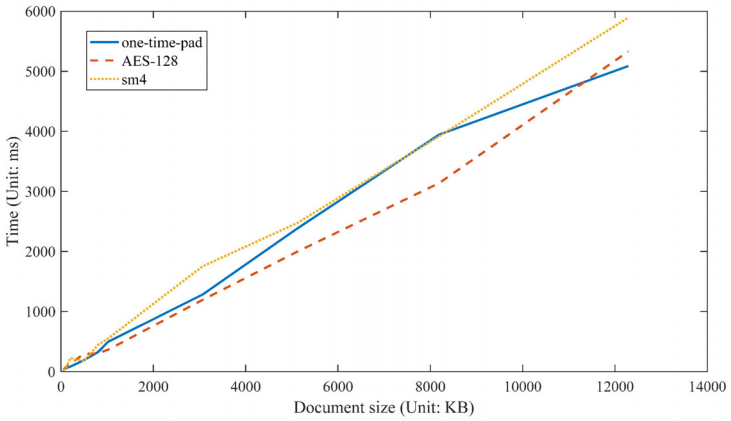

Fig. 10. Time trend of encrypting word documents

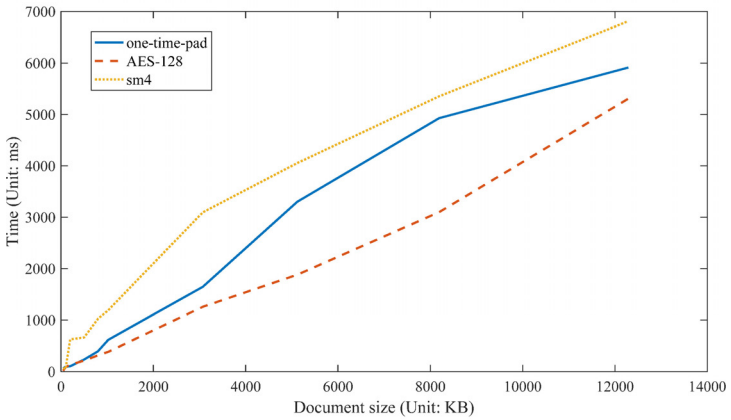

Fig. 11. Time trend of decrypting word documents

The encryption/decryption algorithm is selected according to the importance level of the documents. Assuming that the document security is of a high level, one-time-pad is then adopted, where one plaintext corresponds to one ciphertext. Otherwise, AES-128 algorithm or SM4 algorithm is applied and the key length of both is 16 bytes. It can be illustrated form the tables that the approach of AES-128 algorithm shows speed advantage while conducting encryption/decryption on documents of different size.

5 Conclusions

In this paper, a multi-level data security solution program based on quantum key is proposed. The characteristics and benefits of quantum key are explored adequately by combining the time phase quantum key distribution networks and classical networks. Based on the low quantum key bit rate, a quantum key utilization strategy of three quantum keys are employed. The ratio of ciphertext and plaintext in one-time-pad is 1:1, while the length of key in both AES-128 algorithm and SM4 algorithm is 16 bytes. Through experiments, the quantum key bit rate and quantum key bit error rate of the quantum key distribution network are illustrated. Moreover, the time required for encryption/decryption of text documents and word documents according to different algorithm is also performed. As a result, it can be concluded that the proposed system operates steadily and guarantees the data security.

Acknowledgments

This work is supported by the Science and technology of Jilin province development plan projects with grants No. 20170204023GX, Jilin development and reform commission construction fund (2020C020-2),

the Education Department of Jilin Province with grants No. JJKH20191202KJ, No. JJKH20170496KJ, JJKH20191201KJ, JJKH20200577KJ.

References

[1] Y. Martin, A. Kung, Methods and Tools for GDPR compliance through privacy and data protection engineering, In 2018 IEEE European Symposium on Security and Privacy Workshops (2018) 108-111.

[2] G. Liang, S.-R. Weller, F. Luo, J. Zhao, Z.-Y. Dong, Distributed Blockchain-Based Data Protection Framework for Modern Power Systems Against Cyber Attacks, IEEE Transactions on Smart Grid 10(3)(2018) 3162-3173.

[3] H. Qiu, H. Noura, M. Qiu, Z. Ming, G. Memmi, A user-centric data protection method for cloud storage based on invertible DWT, IEEE Transactions on Cloud Computing 1-1(2019).

[4] C. Li, Z. Wang, Multi-level Encryption Simulation of User Privacy Data in Big Data Environment, Computer Simulation 36(11) (2019)159-162.

[5] Z.-Y. Zhao, J.-H. Wang, Z.-Q. Zhu, L. Sun, Attribute-Based Encryption for Data Security Sharing of Internet of Things, Journal of Computer Research and Development 56(6) (2019) 1290-1301.

[6] K.-J Zhang, Q.-L. Han, Z.-P. Cai, G.-S. Yin, RiPPAS: A Ring-Based Privacy-Preserving Aggregation Scheme in Wireless Sensor Networks, Sensors (17)2 (2017)

[7] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, Using Quantum Key Distribution for Cryptographic Purposes: A Survey, Theoretical Computer Science 560(1)(2014) 62-81.

[8] A. Boaron, G. Boso, D. Rusca, V. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussieres, M. Li, D. A Nolan, A. Martin, H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, Physical review letters 121(19)(2018) 190502.

[9] Z.-Y. Li, Y.-C. Zhang, F.-H. Xu, X. Peng, H. Guo, Continuous-variable measurement-device-independent quantum key distribution, Physical Review A 89(5)(2014) 052301.

[10] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P.-Y. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, J.-W Pan, Satellite-relayed intercontinental quantum network, Physical review letters 120(3)(2018) 030501.

[11] G. Sharma, S. Kalra, Identity based secure authentication scheme based on quantum key distribution for cloud computing, Peer-to-Peer Networking and applications 11(2) (2018) 220-234.

[12] M. Kaur, S. Kalra, Security in IoT-based smart grid through quantum key distribution, In Advances in Computer and Computational Sciences (2018) 523-530.

[13] Y.-L. Zhao, Y. Cao, W. Wang, H. Wang, X.-S. Yu, J. Zhang, M. Tornatore, Y. Wu, B. Mukherjee, Resource Allocation in Optical Networks Secured by Quantum Key Distribution, IEEE Communications Magazine, 56(8)(2018) 30-137.

[14] C.-Y. Wang, J. Gao, Z.-Q. Jiao, L.-F. Qiao, R.-J. Ren, Z. Feng, Y. Chen, Z.-Q. Yan, Y. Wang, H. Tang, X.-M. Jin, Integrated measurement server for measurement-device-independent quantum key distribution network, Optics express 27(5)(2019) 982-5989.

[15] G. Brassard, L. Salvail, Secret-key reconciliation by public discussion, Workshop on the Theory and Application of Cryptographic Techniques (1993) 410-423.

[16] W.-T. Buttler, S.-K. Lamoreaux, J.-R. Torgerson, G.-H. Nickel, C.-H. Donahue, C.-G. Peterson, Fast, efficient error reconciliation for quantum cryptography, Physical Review A 67(5)(2003) 052303.

[17] R. Gallager, Low-density parity-check codes, IRE Transactions on information theory 8(1)(1962) 21-28.

[18] D.-J. Mackay, Good error-correcting codes based on very sparse matrices, IEEE trans-actions on Information Theory 45(2)(1999) 399-431.