Quantum Key Mobile Distribution Method, System, Terminals, and Storage Medium for Communication System Encryption in Power System

Cheng Zhang, Yunpeng Zhang, Lin Ma, Yunxiao Wang, Lina Zhao, and Gaozhou Wang

***Abstract*—In this paper, mobile distribution method, system, terminal, and storage medium based on quantum key (QK) are introduced for communication system encryption in electric power system, which mainly includes following steps. Firstly, the QK management platform (QKMP) can initialize the embedded QK mobile storage device (QKMSD). Secondly, if the QKMSD is initialized, the QKMP will finish the distribution of QKMSD to users, in the meantime, users finish the registration and activation by binding the user identity with the device. Thirdly, the QK charger (QKC), as well as the QKMP, accomplishes the verification to QKMSD, respectively. If the verification is succeeded, the QKC will obtain the QK from original QKMSD, and QK is written-in the QKMSD, finishing the QK charging. Final experimental results demonstrate that, by QKMSD with QK charging authority, secure distribution of QK in the non-fiber communication environment can be implemented.**

***Index Terms*—Quantum communication, quantum key mobile distribution, information security, communication encryption, power system.**

I. Introduction

With the improvement of the system computation ability, especially the emerge of the quantum computation technology, current widespread asymmetric encryption system face the risk of being cracked. Currently, quantum communication technique can be the only communication method with the ability of unconditional security, which has the widespread application prospect.

Quantum communication is the innovation communication method by applying quantum states and entanglement on information and key transmission. Based on the principles of quantum mechanics, the quantum communication can provide the absolute security in the aspects of theory and protocol, which cannot be eavesdropped by illegal user. Generalized quantum communication includes quantum key distribution (QKD), quantum teleportation, quantum dense coding, and quantum secure direct communication. The quantum teleportation, quantum secure direct communications, and quantum secret sharing of quantum communication are hotspots in the frontier basic theory research field and the scientific experiment exploration aspects all the time. However, owing to the restriction in development of application, industrial application of quantum communication still has a long way to go.

In the current, quantum communication referred in the field is the narrow quantum communication technology, which is referred as QKD or quantum secret communication. On the basis of quantum states carriers as well as Heisenberg uncertainty principle [1] and quantum non-cloning theorem [2], senders and receivers in the communication share the key by quantum channel, which is the combination of the quantum mechanics and cryptography. In the communication, cipher cannot be transmitted by QKD, and the quantum channel is utilized to transmit the key between the senders and receivers. With the help of single photon quantum state's preparation, transmission, measurement, and typical communication protocol post-processing, the quantum key (QK) sharing can be achieved between senders and receivers. Moreover, combined with one-time pad symmetric encryption mechanics, which is that two sides of communication utilize the cipher with the same length of information to execute the bit-by-bit encryption and decryption, the absolute secure quantum communication can realize. In 1984, Bennett and Brassard [3] presented the first QKD protocol, Bennett-Brassard 1984 (BB84) protocol, beginning the research in the field of QKD. After decades of development, quantum communication technology develops rapidly from theory to experiment as well as application. Quantum secret communication technology has been researched for application in the aspects of military, finance, government, affairs, energy, etc. Chun *et al*. [4] proposed a handheld free space QKD scheme based on dynamic motion compensation. With the assistance of dynamic beam-steering, reference frame independent coding and fast indistinguishable pulse generation, the secret key rate which is above the 30kbps over 50 centimeters can be obtained. Mark *et al*. [5] utilized entangled photons, and introduced a free space QKD system over very large distance, where a new type of QKD link is demonstrated by modulating retro-reflectors, and its power requirement is tested to be low. Tajima *et al*. [6] presented applications of QKD network, which contains three aspects: quantum layer, key management layer, and key supply layer. The functions and

Manuscript received November 27, 2019; revised February 12, 2020. This work was supported by the Research on New Generation Key Technology of Security Defense: Quantum Identification and Quantum Encryption Based Terminal Secure Accessing Key Technology and Application Research, State Grid Shandong Electric Power Company Science and technology project funding (No. 5206271800CZ), and National Self-Dependent Innovation Demonstration Area Development and Construction Funds of Shandong Peninsula, China (No. 2017SDBD-GJJS004).

Cheng Zhang, Lin Ma, Yunxiao Wang, Lina Zhao, and Gaozhou Wang are with the Information and Telecommunication Company, State Grid Shandong Electric Power Company, Jinan 250001, Shandong, China (e-mail: 56839200@qq.com, ma_lin1991@126.com, 996207306@qq.com, zhaolina_upc@163.com, 434897705@qq.com).

Yunpeng Zhang is with the Shandong Luneng Software Technology Co.,Ltd., State Grid Shandong Electric Power Company, Jinan 250001, Shandong, China (e-mail: zhyp_1993@hotmail.com).

DOI: 10.7763/IJET.2020.V12.1175

architecture of each layer were introduced to give a specific definition. Besides, validity and usefulness of QKD's system application were also demonstrated in this paper. To tolerate the excess noise in plug-and-play dual phase modulated continuous variable QKD, Bai *et al.* [7] proposed to apply noiseless linear amplifier to increase the transmission distance and accomplish the noise suppression. In [8], Wang et al. applied software defined networks (SDN) on QKD to elaborate the overall architecture, related interfaces, and protocols, whose experimental results show that SDN's application improves the efficiency of the QKD network. Zhao *et al*. [9] presented a resource allocation scheme, which includes the joint assignment of routing, wavelength, and time-slot to build channels in software-defined optical network (SDON) with QKD. In [10], Cao *et al*. proposed an innovative architecture of QKD over- wavelength division multiplexing (WDM) networks, where the successful probability of quantum key pool construction can be improved with reducing secret key consumption's flexibility.

However, due to the restriction of specification, problems still remain in quantum safe communication technology, which are demonstrated as follow:

1) QKD has problems in low coding rate, short transmission distance, poor resistance to interference on commercial optical fiber, which cannot apply for single optical fiber long distance transmission. Besides, QK transmission needs to increase the trusted relay station every 50km to 80km for QK relaying, which increase the application cost.
2) Owing to the restriction of current specification, QK should be distributed by the independent optical transmission channel, which means more rigor requirements for optical fiber resources. This is another problem for popularization and application of QKD.
3) The existing QKD system has low QK coding rate, which cannot meet the key requirements of one-time pad communication for high speed business data. This means the current QKD cannot achieve the genuine unconditional security referred to Shannon's theorem [11].

Points presented above result in that the quantum secret communication can be merely applied on the enough optical fiber resource, and the application cost is higher. Thus, the trial applications only carry out in the industries with high security demand such as military, finance, etc. As a conclusion, it is urgent to introduce QK mobile distribution method, system, terminal, and storage based on dependable computing, solving the problem in QK distribution, limited application scene, and high application cost, which are common in quantum secret optical fiber communication.

The rest of this paper is organized as follows. In Section II, the theoretical basis of quantum theory is presented. Section III addresses the concrete proposed method, system, terminals, and storage medium. Section IV gives operational experimental results of the proposed scheme, and demonstrates its functions in detail. Conclusions and future works are finally given in Section V.

II. Quantum Theory

Since quantum theory is introduced, it has abundant and widespread applications in many fields. Among those fields, quantum information science is one of the most import applied subjects. In quantum information science, information is expressed by quantum states. Information transmission is to send the quantum states by quantum channel, information processing is the controlled evolution of the quantum states, and information extraction is to execute the quantum measurement on quantum system. Generally, quantum information theory contains quantum communication and quantum computation.

A. Quantum Communication

Quantum communication is the communication technology, which is the application of quantum mechanics basic theory bases on the material quantum character. The greatest advantage of quantum communication is that it has the unconditional security in theory and efficiency. Unconditional security in theory means that the Hypothesis 1 can be theoretically proved. Efficiency is to apply the superposition and entanglement of quantum states, transmitting and processing the information beyond limits of classical communication [12]. Thus, quantum communication is extremely meaningful to finance and telecommunication.

Hypothesis 1. Even if attackers have infinite computation resources and any means of channel interception permitted by physics, quantum communication can still guarantee the secure information exchange between both sides of communication.

The development overview of quantum communication field is shown in Fig. 1.

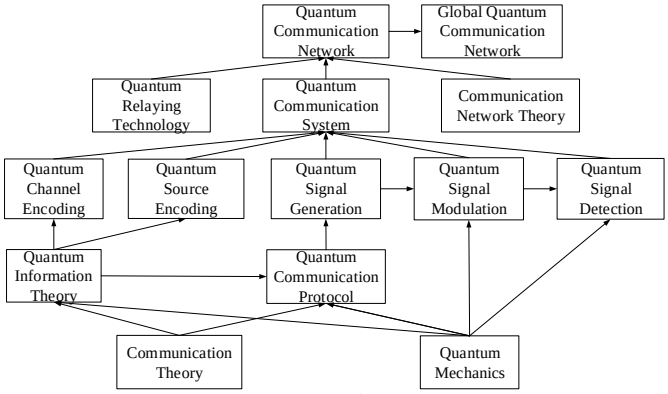

Fig. 1. Development overview of quantum communication.

Communication theory and quantum mechanics are two basis of the quantum communication field, forming the multiple quantum communication protocols, as known as quantum communication schemes [13]. To build an entire quantum communication system, the basis is quantum encoding theory, the core is specific quantum communication protocol, and quantum information or typical information is transmitted by achieving the quantum signal generation, modulation, and detection. With the development of communication network theory and the breakthrough of quantum relaying technology, quantum communication network can evolve from local area network (LAN) to wide area network (WAN) with a large scale, even to global quantum communication network.

B. QKs' Generation, Communication and Distribution: BB84 Protocol

In this paper, BB84 protocol is the most basic and important theory in QKD, which guarantee the method's smooth execution and system's running in working order.

BB84 protocol was proposed by Bennett and Brassard in 1984, which is the earliest as well as the most applicable protocol. What more important is that BB84 is the basic of other quantum protocols, such as B92 protocol [14], six-state protocol [15], and decoy-state protocol [16]. This protocol can make two authenticated sides of communication establish the key continuously in two faraway places, and then accomplish the secure communication by one-time pad codebook encryption protocol. BB84 protocol is based on Heisenberg uncertainty principle and character that quantum state cannot be precisely cloned , which is totally different from the basic computation complexity-based principle in typical cryptography, introducing the methods that can firstly provide the unconditional security in physical theory. This opens up the new fields of QKD and secure communication. Owe to its simplicity and strong operability, BB84 is proved, demonstrated, and applied in sequence, and it becomes the first widespread-used practical quantum communication protocol.

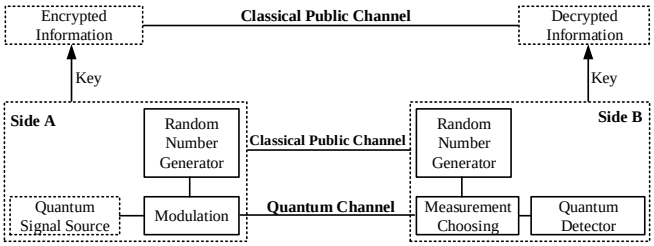

Fig.2. Schematic diagram of BB84 protocol.

As is shown in Fig. 2, firstly, the basic condition of BB84 is to possess a quantum signal resource, randomly generating four signals of quantum state. Next, modulated quantum signal can accomplish transmission by a quantum channel such as optical fiber or free space. Then, the received quantum signal can be measured efficiently, and the basis vector used for measurement is selected randomly. Meanwhile, an auxiliary classical public channel is utilized to transmit the typical basis vector comparison and other information. Moreover, the typical public channel should be verified, and any eavesdropper can obtain the classical information by eavesdropping but cannot alter the information. On the above condition, secure key can be built between two sides of communication, and two sides can apply one-time pad encryption transmit the encrypted information for secure communication. In the practical system, classical public channel is the same one, Fig. 2 illustrates separately according to the logical functions for clearer narration.

Fig. 3 gives the flowchart of the BB84 protocol. Side A firstly select the basis vector to make the quantum state, and send it to side B by quantum channel. After side B receive the quantum state, it will select the horizontal polarization (H), vertical polarization (V) or +45° polarization (+), -45° polarization (-) basis vector to finish the measurement. Owing to the total independence and randomness of basis vector selection in side A and B. Two sides of communication will have 50% probability of applying the same basis vector, and acquiring the completely correlated results. But there will be 25% error rate in the measured data of side B.

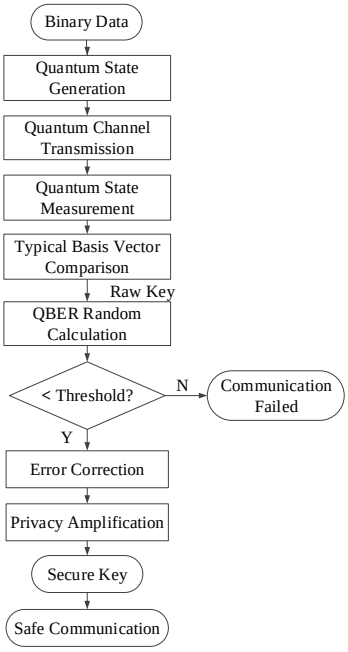

Fig. 3. Flowchart of BB84 protocol.

To decrease the error rate, side A and side B should compare the basis vector to pick out the correlated results. Side B discloses its own measurement basis vector, and side A compares side A's basis vector with its own-made basis vector, and discloses the same parts of side B's public basis vector. Finally both sides merely retain the same parts of basis vector. The above process is known as screening process, and the reserved key is the raw key. Then, both sides disclose a part of raw keys to estimate the bit error rate (BER) and the possible eavesdropper. If the BER is in certain threshold, error correction technology is used to correct the error, and privacy amplification [17] is further applied on the corrected key, which can eliminate the information leakage in communication and error correction. Finally, the unconditional safe key can be extracted. In fact, owing to the non-ideal devices and channels, there must be error in raw key. What's more, the eavesdropping can result in these errors, which forms the quantum BER (QBER).

III. Main Theory of Proposed Method, System, Terminal and Storage

In order to solve the shortcomings of current technologies, QK mobile distribution method, system, terminals, and storage are proposed in this paper, realizing and solving the secure QK distribution and the last mile in QK application.

A. QK Mobile Distribution Method

As can be shown in Fig. 4, the flowchart of the QK mobile distribution method in this paper is given. To be more concrete, the bold terms on the top of each block are the initiator, and the ones under the block are the acceptor. The QK-based mobile distribution method can be described as follow:

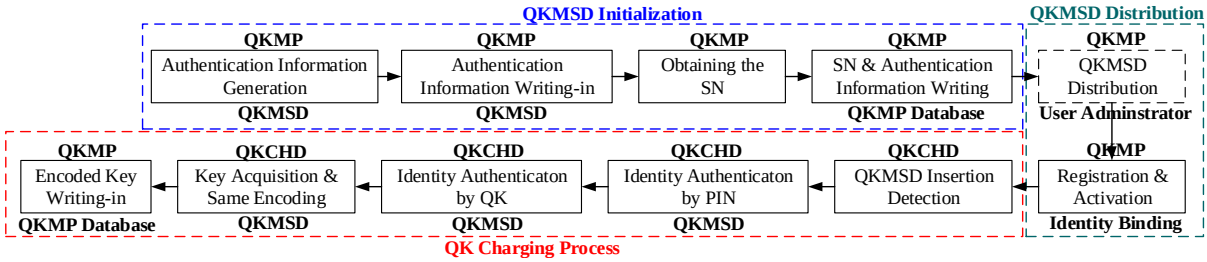

Fig. 4. The flowchart of the QK mobile distribution method.

Step 1. The QK management platform (QKMP) execute initialization process on the QK mobile storage device (QKMSD).

Step 2. If the initialization of QKMSD finishes, the QKMP will distribute the QKMSD to users, and the QKMSD carries on the identity binding with users for completing the registration and activation.

Step 3. QK charger (QKC) and QKMP will carry on identity authentication to the inserted QKMSD, separately. If the identity authentication passes, the QK in the original QK device can be obtained by the QKC, and QK will write to the QKMSD, finishing the QK charging.

To be more concrete, the details of every steps will be demonstrated as follows, which can be seen in Fig. 5.

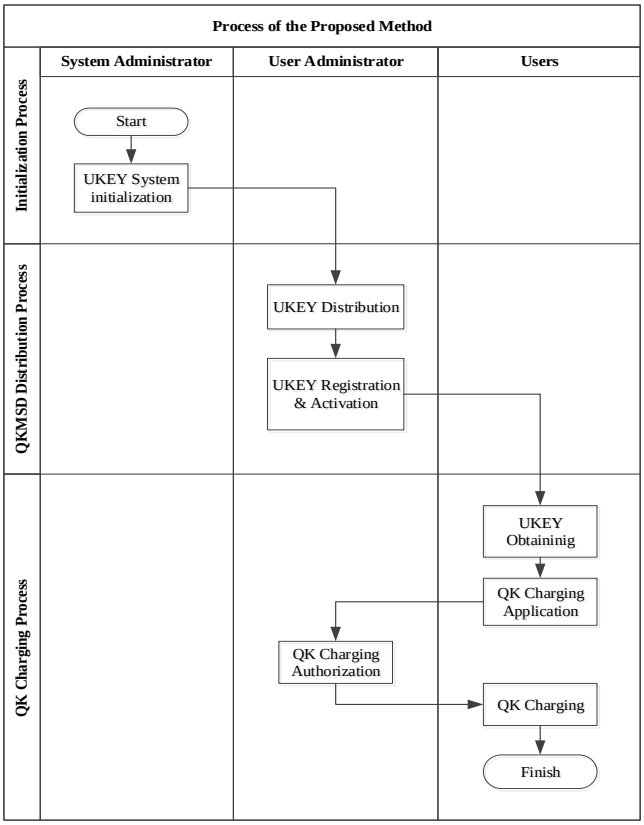

Fig. 5. Flowchart of the QK-based mobile distribution method.

In Step 1 (**Initialization Process**), the initialization processing of QKMP contains:

1) Insert the QKMSD into the hardware device distribution management module of QKMP;
2) User administrator executes the initialization process by operation interface of the hardware device distribution management module in QKMP;
3) QKMP generates the unique digital certificate or QK string for each QKMSD, and embeds the digital certificate or QK string information into the encrypted storage area of secure chips on QKMSD. It's worth noting that digital certificates and QK strings, which are stored in the encrypted storage area of secure chips on QKMSD, can guarantee that QKMSD cannot be counterfeited;
4) QKMP obtains the device serial number (SN) of the QKMSD, and embeds with the digital certificates or QK string information together into the QKMP database.

In Step 2 (**QKMSD Distribution Process**), if the initialization processing of QK mobile storage device finishes, the distribution, registration, and activation processing contains:

1) Insert the QKMSD into the hardware device distribution management module of QKMP;
2) User administrator executes the registration and activation process by operation interface of the hardware device distribution management module in QKMP;
3) If the QKMSD finishes initialization, the QKMP will distribute it to the user administrator;
4) According to the user application status, the user administrator will finish the process of QK mobile binding with the user identity in the QKMP, which means that the registration and activation are finished.

In Step 3 (**QK Charging Process**), the details mainly contains:

1) Insert the QKMSD into QKC;
2) QKC will automatically detect the insertion of the QKMSD, and the identity authentication will be executed on QKMSD with the help of the user's input personal identification number (PIN) code of the QKC;
3) If the identity authentication passes, the QKMP obtain the QK from the QKMSD, and execute the identity authentication on the QKMSD;
4) If the identity authentication passes, the QKC obtain the QK in original QK device, and the QKC as well as the QKMP will obtain the consistent key to achieve the same coding;
5) QKC will insert the coded QK into the QKMSD, and the QKMP will write the QK into database of the QKMP.

B. QKs' Generation, Communication and Distribution: BB84 Protocol

QK mobile distribution system introduced in this paper mainly includes QKMP, QKMSD with certain quantity, QKCHP, and all components in this system achieve the communication by the quantum private network, which can be seen in Fig. 6. The QK-based mobile distribution system can be demonstrated as follows, which contains:

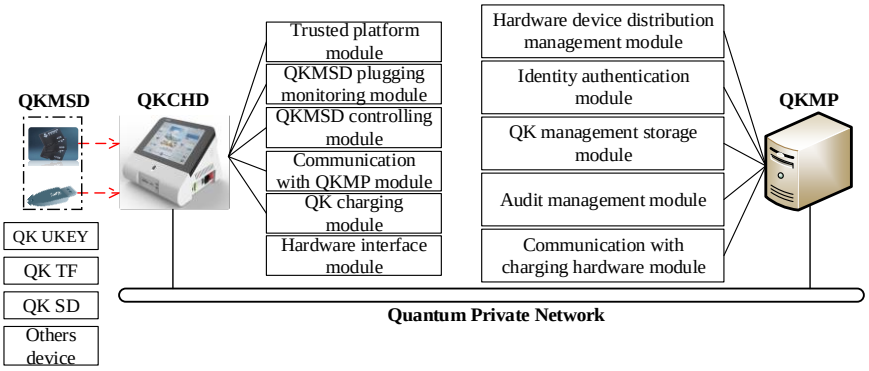

Fig. 6. The basic network of QK mobile distribution system.

1) **QKMP**: it is applied for the initialization, user distribution, registration and activation of the QKMSD. Besides, it can also be used for identity authentication of QK-embedded mobile storage device in the QK charging process.as well as the re-coding and encrypted storage for the QK. To be more detailed, the QKMP contains:

Hardware device distribution management module: its configuration is used to for initialization, user's distribution, as well as registration and activation of the QKMSD. Besides, it can report the loss, freeze, and cancel the loss of the QKMSD.

Identity authentication module: its configuration is used for accomplishing the identity authentication of QKMSD during the QK charging process. In detail, the identity authentication methods mainly include QK-based identity authentication and digital certificate authentication.

QK management storage module: its configuration is used for obtaining the QK manager or QKs in the QK generator device, QK re-coding, encrypted storage, whole process management, and providing the QK service to outsiders. Concretely, on the basis of privatization interface protocol, s storage module obtain the QK manager or QK in QK generator, as well as re-code and securely store the QK, providing the whole process management such as QK's extraction, coding, distribution, utilization, freezing, restoration, and destroying, as well as services for outsiders.

Audit management module: its configuration is used for accomplishing the secure audit of the time logs, such as identity authentication, QK charging, QK freezing, QK restoration, QK destroying, etc., as well as the search and statistics of the audit results.

Communication with charging hardware module: its configuration is used for communications with the QKC, and accomplishing the transmission of the identity authentication information and parity information which is checked for QK charging coding consistence during the process of QK charging.

2) Quantitative QKMSDs: it is applied for the mobile storage for QK. The demonstrated QKMSD contains: QK UKEY, QK trans-flash (TF) card, QK secure digital memory (SD) card, and other mobile devices embedded with secure chips.

3) QKC: it is applied for identity authentication of QK-embedded mobile storage device in the QK charging process, obtaining the QK in the original QK device, and writing the QK in the QKMSD. Moreover, the QKC contains:

Trusted platform module: its configuration is used for accomplishing the identity authentication of the QKMSD. Concretely, trusted platform module is utilized for accomplishing the trusted guide of the QKC's launching. For instance, if let trusted cryptography module (TCM) [18] be the trusted root, when the machine starts up, TCM is applied for measuring and verifying the integrity of startup module, then startup module will measure and verify the integrity of the embedded operating system (EOS), and finally EOS will measure and verify the integrity of applications and the secure storage as well as authentication of the QK and digital certificate.

QKMSD plugging monitoring module: its configuration is used for automatically monitoring the plugging status of the QKMSD. In detail, once QKMSD plugging monitoring module detect the QKMSD's plugging, QKMSD controlling module will be invoked automatically.

QKMSD controlling module: its configuration is used for prohibiting the QKMSD which is not safely initialized applying on the QKC. Specifically, QKMSD controlling module applies the hardware SN or certificate authentication methods, prohibiting the QKMSD without secure initialization applying on the QKC.

Communication with QKMP module: its configuration is used for communication with QKMP, accomplishing the transmission of the identity authentication information and parity information which is checked for QK charging coding consistence during the process of QK charging.

QK charging module: its configuration is used for obtaining the QK in original QK device, and writing into the QKMSD after identity authentication. In detail, QK charging module is based on the privation interface protocol of the QK device to obtain QKs in the QK manager or QK generator, which are accordance with QK in QKMP. Moreover, the same coding scheme is applied and QK will be written into the QKMSD after authentication.

Hardware interface module: it is equipped with the Ethernet interface, universal serial bus (USB) interface, SD card interface, TF card interface, etc.

C. Terminals

Terminal demonstrated in this paper contains processor and memory, while communication unit is for better demonstration of the terminals in the network, and it is used for establish the communication channels, achieving the communication with other terminals, which is shown in Fig. 7. As can be seen in Fig. 7, all components can communicate through one or more buses.

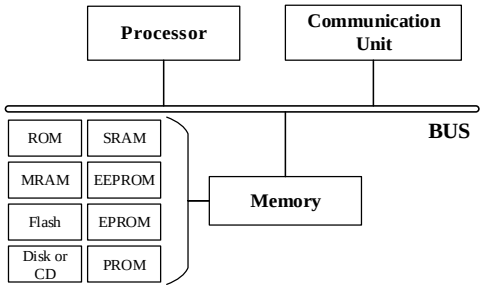

Fig. 7. The diagram of terminals in this paper.

Processor used for invoking the computer program from memory to run, which means that above methods can be executed. Processor is the controlling core of the storage terminals, utilizing different types of interfaces and lines to link the each parts of entire electronic terminals. By running or executing the program or module in the memory, as well as invoking the data stored in memory, various functions and data processing can be executed in the electronic terminals. Processor illustrated in this paper consists of integrated circuit (IC), and it can be single package or multiple package with same or different functions.

Memory used for computer program's instructions storage. It can be realized by any types of volatile and non-volatile memory terminals or their combinations, such as static random access memory (SRAM), electrically erasable programmable read-only memory (EEPROM), electrically programmable read-only memory (EPROM), programmable read-only memory (PROM), read-only memory (ROM), magnetic random access memory (MRAM), flash memory, and disk or CD.

D. Computer Storage Medium

Computer instructions are stored in the demonstrated computer readable storage medium. When instructions run, the above methods can be executed as expressed in chapter A. The computer storage medium mainly includes disk, CD, ROM, RAM, etc.

E. Computer Program Product with Instructions

The computer programs should be executed for above methods' correct execution illustrated in chapter A.

IV. Main Theory of Proposed Method, System, Terminal and Storage

In this section, operational experimental results of the proposed method and system are given and analyzed. In Table 1, in order to accomplish the integrate functions, the method and system's application environments as well as their configuration are shown. In this experiment, 1 application servers (AS), 1 data server (DS), 1 QKC (industrial customized machine), and 1 personal computer (PC) are required. The mobile terminal tested in this experiment is run with Android 5.1, whose parameters are Qualcomm snapdragon 615 (MSM8939) 1.2GHz, 3GB RAM, 16GB ROM.

TABLE I: Configuration of the Application Environment

Devices	Application Server	Data Server	QKC	PC
Type	Inspur NF5270M4	Inspur NF5270M4	Qkchr-100	Dell Inspiron 5557
CPU	Intel Xeon E5 2620, 2.4GHz	Intel Xeon E5 2620, 2.4GHz	Intel i3-6100, 2.4GHz	Intel i7-6500U, 2.5GHz
Memory Capacity	16 GB	16 GB	8 GB	8 GB
Disk Capacity	500 GB	500 GB	80 GB SSD	1 TB
Network Adapter (NA)	Intel I350 Gigabit Network Connection	Intel I350 Gigabit Network Connection	Intel I210 Gigabit Network Connection	Realtek PCIe FE Family Controller
OS	CentOS 6.6	CentOS 6.6	Ubuntu 16.04 TLS	Windows 10 Family Version
Tested Software	QK Update Management Software; Quantum Authentication Secure Service Software; QKMP Software; Quantum Service's Service Software	MySql 5.1.9	QK Charging Software	QSS_QMC Software

Fig. 8 and Fig. 9 shows the visual interface of QK charging process. After QKC starting up, system automatically enters the QK charging interface, notes will be shown for inserting the administrator UKEY, and PIN code should be input for administrator UKEY. Then, user UKEY (quantum secure UKEY or secure TF card) should be inserted, and PIN code will be inserted again for entering the QK charging system interface.

Fig. 8. Interface of QK charging.

In Fig. 8, QK charging interface consists of four functions: device information, QK charging, device management, and logout. In device information, the device ID, user's name, and remaining QK volume can be checked.

Fig. 9. Interface of QK charging volume selection.

After clicking the QK charging button, the selecting interface of QK charging volume will pop up, and the volume

can be 1 MB to 9 MB, which is shown in Fig. 9. Users will select the needed QK charging volume according to its requirement. Once the charging volume is confirmed, the progress bar of QK charging will pop up. When the progress bar reaches 100%, QK charging finishes.

Fig. 10~Fig. 13 illustrate the quantum secure encryption for mobile terminals. As is shown in Fig. 10, network parameter configuration should be done before first-time using. In basic parameter configuration of Fig. 10(a), connection name, gateway, port, authentication types, and user certificate information are shown. Specific certificate selection is shown in Fig. 10(b).

(a) Basic parameter configuration (b) Certificate selection

Fig. 10. Network parameter configuration of mobile terminals.

As can be seen in Fig. 11, after network configuration, the service configuration should be finished. By clicking the QK UKEY button, interface in Fig. 11(a) can be shown, and the selection 'Using QK encryption' should be turned on. Next, quantum safe service center (QSSC) address and its port should be input, and remaining volume of QK UKEY can be checked out. Then, in configuration of the App, 'national secret algorithm' selection under the algorithm standard title should be turned on, which is shown in the fifth line of Fig. 11(b).

(a) Applying the quantum encryption (b) Basic configuration and algorithm

Fig. 11. Service configuration of mobile terminals.

When configuration is accomplished, terminals can achieve the quantum security access and login. Before quantum security access, the QK charging process should be finished, which can be seen in Fig. 8 and Fig. 9. Users link the quantum secure UKEY with the mobile terminals by OTG, and the system will automatically detect the QK secure UKEY. Furthermore, the quantum security access configuration will operate. Fig. 12 shows the login process of quantum security access. In Fig. 12(a), system notes that SD Key is detected and user's password should be input. After verification success of SD Key, in Fig. 12(b), system notes that quantum UKEY is detected and user's password should be input.

(a) SD key input (b) KEY input

Fig. 12. Login process of quantum security access.

Finally, the quantum security access state will be updated to 'already logged in', and the quantum secure encrypted channel is built up for the further data secure access of business application, which is shown in Fig. 13.

(a) 'already logged in' reminder (b) setting up logs for quantum secure channel

Fig. 13. Login success of quantum security access.

V. Conclusion

In this paper, QK-based mobile distribution method, system, terminal, and storage medium are introduced to improve the information security. With the assistance of the QKMSD and the authority of QK charging, the QK can be distributed to the users, which can accomplish the QK secure distribution under the non-fiber environment, solving the difficult 'last mile' problem in QK application. Moreover, the system structure is simple, solving the authentication problem of mutual secure quantum communication between quantities of mobile users, which makes the basis for the widespread low-cost application of the quantum

communication technology. Furthermore, the optimization of QKD mobile method and system will be researched in the future.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Cheng Zhang, Lin Ma and Chuanqi Wu conceived the scheme and designed the experiments; Cheng Zhang, Yunpeng Zhang, Lin Ma, Yunxiao Wang, Lina Zhao, and Gaozhou Wang performed the experiments; Cheng Zhang, Lin Ma, Yunxiao Wang, Lina Zhao, and Gaozhou Wang analyzed the results; Yunpeng Zhang drafted the manuscript; and Hao Deng and Yunpeng Zhang revised the manuscript. All authors have read and approved the final manuscript.

Acknowledgment

All of our author thanks Chuanqi Wu and Hao Deng for their great help in finishing this paper's work and revising this paper.

References

[1] B. Paul, H. Teiko, and L. Pekka, "Heisenberg's uncertainty principle," *Physics Reports*, vol. 452, pp. 155-176, Nov. 2007.
[2] L. L. Gui, "Duality quantum computing and duality quantum information processing," *International Journal of Theoretical Physics*, vol. 50, pp. 1305-1318, Apr. 2011.
[3] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," in *Proc. IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, India, 1984.
[4] H. Chun, C. Iris, F. Grahame, C. Larry, B. Bryan, G. Glenn, C. Colin, N. Antti, W. Joachim, O. Dominic, and David, B, "Handheld free space quantum key distribution with dynamic motion compensation," *Optics Express*, vol. 25, pp. 6784-6795, Mar. 2017.
[5] B. Mark, R. S. William, M. Rita, F. S. Mike, G. G. Peter, and J. Reintjes, "Mitigating pointing requirements and turbulence effects in free-space quantum key distribution," *SPIE 10660, Quantum Information Science, Sensing, and Computation X*, pp. 1-7, United States, 2018.
[6] A. Tajima, T. Kondoh, T. Ochi, M. Fujiwara, K. Yoshino, H. Lizuka, T. Sakamoto, A. Tomita, E. Shimamura, S. Asami, and M. Sasaki, "Quantum key distribution network for multiple applications," *Quantum Science and Technology*, vol. 2, pp. 1-9, July 2017.
[7] D. Y. Bai, P. Huang, H. X. Ma, T. Wang, and G. H. Zeng, "Performance improvement of plug-and-play dual-phase-modulated quantum key distribution by using a noiseless amplifier," *Entropy*, vol. 19, pp. 1-15, Oct. 2017.
[8] H. Wang, Y. L. Zhao, and A. Nag, "Quantum-key-distribution (QKD) networks enabled by software-defined networks (SDN)," *Applied Sciences*, vol. 9, pp. 1-12, May 2019.
[9] Y. L. Zhao, Y. Cao, W. Wang, H. Wang, X. S. Yu, J. Zhang, T. Massimo, and Y. Wu, "Resource allocation in optical networks secured by quantum key distribution," in *Proc. 2017 Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC)*, pp. 1-8, Sinapore, 2017.
[10] Y. Cao, Y. L. Zhao, Y. Wu, X. S. Yu, and J. Zhang, "Time-scheduled quantum key distribution (QKD) over WDM networks," *Journal of Lightwave Technology*, vol. 36, pp. 3382-3395, Aug. 2018.
[11] A. Reynal, H. Manabu, and S. Jonas, "Formalization of Shannon's theorems," *Journal of Automated Reasoning*, vol. 53, pp. 63-103, Jun. 2013.
[12] L. Kogias, Y. Xiang, Q. Y. He, and G. Adesso, "Unconditional security of entanglement-based continuous-variable quantum secret sharing," *Physical Review A*, vol. 85, pp. 1-6, Jan. 2017.
[13] H. Yin and Y. Han, *Quantum Communication Principle and Technology*, Beijing: Publishing House of Electronics Industry, 2013, pp. 10-20.
[14] Y. G. Yang, S. J. Sun, P. Xu, and J. Tian, "Flexible protocol for quantum private query based on B92 protocol," *Quantum Information Processing*, vol. 13, pp. 805-813, Mar. 2014.
[15] B. Dagmar, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, pp. 1-5, May 1998.
[16] L. O. Mailloux, R. D. Engle, M. R. Grimaila, D. D. Hodson, J. M. Colombi, and C. V. McLaughlin, "Modeling decoy state quantum key distribution systems," *Journal of Defense Modeling and Simulation*, vol. 12, pp. 498-506, June 2015.
[17] Y. G. Yang, P. Xu, R. Yang, Y. H. Zhou, and W. M. Shi, "Quantum Hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Scientific Reports*, vol. 6, pp. 1-14, Jan. 2016.
[18] C. L. Huang, C. W. Hou, H. D. Dai, Y. Ding, S. L. Fu, and M. L. Ji, "Research on Linux trusted boot method based on reverse integrity verification," *Scientific Programming*, vol. 2016, pp. 1-12, 2016.

Cheng Zhang was born in 1987. His current research interests include are information security and electric power industrialization.