Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Commercial password modification for face recognition systems using quantum key distribution networks

Hai Huang[1,] ✉

[1] *School of Economics and Business Administration, Chongqing University, Chongqing, 400044, China*

ABSTRACT

Information security is the most concerned issue in modern communication, with the continuous development of new computing technologies, classical cryptography has been difficult to effectively guarantee information security, quantum key distribution technology through the theory of quantum mechanics to ensure the absolute security of key distribution. Therefore face recognition system oriented optimization using quantum key distribution, this paper is based on the advantages of OQKD technology such as easy to implement, low overhead, high security, optimization for commercial privacy queries in the system. On the basis of the quantum key distribution regional network of trust relay, a new type of quantum key distribution experimental network structure based on switching nodes which is more flexible, energy-saving and efficient is proposed. Finally, the method of this paper is comprehensively verified through modeling simulation, and the simulation results show that the average call loss is 3.67% when the quantum key generation rate is increased to 20Kbps, which is significantly reduced. Moreover, the network call loss can be reduced to less than 11% when the method of this paper is adopted in the same situation, and the network call loss is even smaller. It shows that the call loss of the network will be greatly reduced when the key generation rate is increased with a fixed amount of voice traffic.

Keywords: quantum key distribution network, switching node, OQKD, trust disruption, cryptographic security

1. Introduction

Face recognition is an emerging biometric technology. This technology studies how to find out the part that describes the face in the image data such as video or photo, and analyze the information contained in the face, such as the identity, age, and emotion of the face owner and so on. Compared with mature biometric technologies such as fingerprint recognition and iris recognition, face recognition technology has the advantages of unique non-contact and non-compulsory, which can be better

✉ Corresponding author.
E-mail address: cquhuanghai888@163.com (H. Huang).
Received 03 March 2024; Revised 20 April 2024; Accepted 10 November 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-517

accepted by people [1-4]. The technology has a vast development prospect. In recent decades, with the deepening of face recognition related research, various face recognition algorithms have been bred, such as template-based methods, feature-invariant based methods, skin color and gray scale histogram based methods, etc. The recent emergence of neural networks and deep learning models, which achieve accuracy performance on open source databases that can challenge humans, has pushed the research on face recognition to new heights [5-7]. Researchers have adapted the original models, trained a large number of models with better performance, and put the models on the Internet for others to download and study. The whole field of face recognition is in the process of high-speed iteration, and the development momentum is very strong. This momentum has led to a proliferation of commercial attempts and applications related to face recognition. Commercial companies have been exploring the applicable scenarios of face recognition, and the demand for face recognition systems has gradually increased [8-10].

With the rapid development of computer technology and communication technology, the Internet plays an increasingly irreplaceable role in the normal life of human beings. People rely on the network to obtain information from all over the world, and at the same time, they also share their information with others through the network. In this process a large amount of data is transmitted over the network, how to guarantee the security of these data is a crucial issue, in the past decades, the key system based on the decomposition of large numbers has been used as an important means to ensure data security [11-14]. The complexity of algorithms based on the decomposition of large numbers ensures that they are difficult to crack in polynomial time, guaranteeing the security of this type of key system. However, as the theory of quantum computer becomes more and more mature, its ultra-high parallel computing capability will question whether the key system based on the decomposition of large numbers can still guarantee the security. For this reason, finding a new type of key system to ensure the secure transmission of information has become an urgent problem [15-17]. In this case, quantum secure communication has become an important research direction for the new generation of key system because of its absolute physical security. Quantum secure communication prepares quanta with multiple states as the carrier of information, and transfers the key between the two parties of communication through the sequence of quanta with different states Physically, a quantum is in the superposition of multiple states, but the state of the quantum is uniquely determined when a definite means of observation is used [18-19]. This physical property ensures that the quantum encryption is not eavesdroppable and that the quantum is capable of efficient key transfer. With the maturity of quantum secure communication, quantum key distribution networks have been tested for practical applications [20-21].

In summary, face recognition has become an indispensable identity authentication method in commercial scenarios, but the development of this technology brings convenience and is accompanied by a number of security problems, therefore, it is of great practical significance to study how to utilize quantum key distribution networks for commercial password modification of the face recognition system to take into account the data security and identity recognition performance [22-24].

This paper proposes the optimization based on quantum key distribution network for face recognition system for commercial password modification. In this paper, firstly, an in-depth research on quantum key distribution technology is carried out, then for the protection of commercial password privacy, this paper adopts OQKD technology for optimization based on the advantages of high security of OQKD technology, so that it can query relevant data information under the premise of protecting the privacy of both parties. On this basis, the quantum key distribution of trust relay is introduced to construct a quantum key distribution network based on exchange nodes to realize the quantum key distribution network. Finally, the simulation test of this paper's method is carried out by building a quantum key distribution network platform, which verifies the effect of this paper's method and provides a design reference for the quantum key distribution network in system cryptographic security optimization.

2. Quantum key distribution network for identification systems

2.1. Quantum Key Distribution

Quantum key assignment was first proposed in 1984 and marked the creation of quantum cryptography as a branch of research. Quantum key distribution is only a key step in achieving unconditional secure encryption, and the entire encryption process must be completed in conjunction with "one password at a time" encryption, but it is customary to use the term "quantum cryptography" to refer to "quantum key distribution".

All QKD protocols can be divided into two parts: quantum communication and classical data processing. In the quantum communication part, a quantum state is prepared and sent through a quantum channel, which is measured and the corresponding data are obtained. For the consideration of increasing the channel capacity as well as reducing the decoherence effect, optical fiber is usually used as the quantum communication channel in practical applications. In the classical data processing part, and through a securely authenticated (can be eavesdropped, but not tampered with) classical data channel exchanges information such as pair base, checksum, error correction and secrecy amplification, and from the measurement result extracts the common security key of both parties. The protocol is by far the most intensively studied and widely used protocol, containing almost all the base elements of the protocol idea.

In the BB84 protocol, Alice first generates two strings of random bits using a true random number generator, denoted as:

$$x = \{x_1, \ldots x_i, \ldots\} \tag{1}$$

$$a = \{a_1, \ldots a_i, \ldots\} \tag{2}$$

where x_i is the bit information to be sent to Bob, and a_i is used to decide which set of bases to use to prepare the signal state representing x_i: e.g., $a_i = 0$, modulated by the right-angled base $\{|0\rangle, |1\rangle\}$, $a_i = 1$, modulated by the diagonal base $\{|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}\}$. $\{|0\rangle, |+\rangle\}$ for code $x_i = 0$ and $\{|1\rangle, |-\rangle\}$ for code $x_i = 1$. The non-clonability principle ensures that no one can perfectly distinguish between non-orthogonal states (e.g., $|0\rangle$ and $|+\rangle$), and thus it is not possible to perform an intercept-retransmit attack without introducing additional errors. A more rigorous analysis proves that not only the intercept-retransmit attack, but also any operation that attempts to extract information from the signaling state introduces an additional error to Bob's result, and by the magnitude of the error (BER) Alice and Bob can estimate the maximum amount of information that the eavesdropper has gained to determine whether the security key can be extracted. This idea is the common principle of all QKD protocols.

The quantum states used for encoding do not necessarily have to be limited to two-dimensional Hilbert space selection, and can be of higher or even infinite dimensions. Extending the BB84 protocol to the general case, the process of quantum state preparation can be formulated as follows: Alice generates a string of N-coded random numbers $x = \{x_1, \ldots x_i, \ldots\}$ as well as a string of M-coded random numbers $a = \{a_1, \ldots a_i, \ldots\}$, randomly picks one out of the set of M quantum states according to the value of a_i, and then, according to the value of x_i, prepares the quantum state $|\phi_{a_i}, x_i\rangle\phi_{a_i,x_i}\langle$ in the set as a signaling state to be sent to Bob. Each set of state collections should have the same average state density operator, i.e., $\sum_{n=0}^{N-1} = p_{m,n} |\phi_{m,n}\rangle\langle\phi_{m,n}| = \sigma, \forall m \in \{0, \ldots, M-1\}$, where $p_{m,n}$ is the probability of picking state $|\phi_m, n\rangle$. In BB84, M = N = 2, all $p_{m,n}$ are taken as 1/2, and σ is the unit matrix $|0\rangle\langle 0| + |1\rangle\langle 1| = |+\rangle\langle +| + |-\rangle\langle -| = I\rangle$.

After receiving the signal state, Bob similarly generates a string of M-constant random numbers $b=\{b_1,...b_i,...\}$ for selecting the measurement base, and then performs a POVM measurement on the signal state to obtain the measurement result $y=\{y_1,...y_i,...\}$.

At the end of the quantum communication process, and perform the following data processing operations:

1) Publish the base selection information a and b of both parties through the classical channel with security authentication, and discard the results that will be inconsistent and invalid (not conforming to the response specified in the protocol) for both parties' base selections.

2) From the remaining data, a portion of the results are published for parametric estimation to estimate parameters such as BER, channel efficiency, etc.

3) According to the results of parametric estimation to estimate the eavesdropper may obtain the upper bound of the amount of information, the two sides can decide to declare the communication is invalid (the eavesdropper may have access to all the key information), or continue to carry out the error correction and confidentiality of the amplification process to ultimately obtain a common string of security pins.

2.2. OQKD mechanism based on commercial password privacy protection

In face recognition system privacy protection, data mining, data distribution and data analysis are the key concerns in cryptographic security, password modification and privacy applications.NPD quantum protocol is based on the unintentional quantum key distribution establishes the unintentional key between the user and the data service center. By entering a secret integer in the identification system the user can query the related data service and protect the information in the privacy dataset. In this paper, an OQKD-based quantum key distribution is proposed for commercial cryptography in identification systems, which can query the relevant data information and perform the corresponding password modification while protecting the privacy of both parties. The protocol has higher security and better feasibility and can be better applied in commercial cryptography.

NPQ queries the user Alice to have a private integer x and the database Bob to have a private integer set $B=\{x_1,x_2,...,x_i,...,x_n\}$ where $x,x_i\in\{0,1,...,N-1\}(1\le i\le m)$ and assumes $N=2^n$. Alice wants to query the element x in the private dataset that is closest to her x without revealing x her private information. Moreover, NPQ satisfies the following privacy requirements:

Alice's privacy, Bob cannot learn private information about Alice's integer x.

Bob's privacy, Alice cannot query the database for private information other than the nearest element x_i.

The database Bob and the user Alice perform n inadvertent quantum key distribution (OQKD) processes to establish n key strings respectively, where the key at Bob is denoted as $K_1,K_2,...,K_n$ and she knows all the bits of each K. The key at Alice is noted as $K_1^*,K_2^*,...,K_n^*$, and she only knows one bit $K_i^*(x)$ for each K_i^*. Here $K_i^{'}(x)$ denotes the xth bit of the key string $K_i^{'}$, and it is worth noting that here x is exactly the secret integer of the user Alice. The exact steps of the OQKD process are as follows:

Step1 Bob randomly prepares a series of photons, each of which is in one of the four states $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$, and sends them one by one to Alice, where it is agreed that $|0\rangle$ and $|1\rangle$ are coded as 0, and $|+\rangle$ and $|-\rangle$ as 1.

Step2 Alice randomly selects one of the measurement bases $\{|0\rangle,|1\rangle\}$ and $\{|+\rangle,|-\rangle\}$ for each photon received, and discloses the photons that have been successfully measured, ignoring the information carried by the missing photons.

Step3 For each photon that Alice has successfully measured, Bob discloses one of the four pairs of non-orthogonal quantum states $A_{\alpha,\beta}$.

Step4 Alice uses her own measurements and Bob's public results to reverse-engineer the original state of the outgoing photon, and thus get the key bit values. Here Alice has 1/4 probability to record

each key bit value correctly. For example, Bob sends a photon $|+\rangle$ and discloses $A_{0,+}$, Alice receives the photon and selects the $\{|0\rangle,|1\rangle\}$ base measurement to get the result $|1\rangle$, at this time Alice can correctly deduce that the original state is $|+\rangle$, and record the bit value "1". Another example is that Bob still sends a photon $|+\rangle$ and discloses $A_{0,+}$, but Alice receives the photon and selects the $\{|0\rangle,|1\rangle\}$ -base measurement to get a result of $|0\rangle$. At this time, Alice is unable to correctly deduce the original state and records the bit value as "?". By this method an inadvertently generated key string ROK of length $N+a-1$ is established between Alice and Bob (parameter a will be described in Step5), in which Bob is fully aware of all the bit values noted as ROK_B; but Alice theoretically knows only 1/4 of them, noted as ROK_A.

Step5 Classical post-processing of the unintended raw key string ROK: the ROK of length $N+a-1$ is denoted as $R_0R_1...R_{N+a-2}$; accordingly, the unintended final key FOK is denoted as $F_0F_1...F_{N+a-2}$.

In order to control the number of known bits in Alice's unintended final key FOK_A as a, Bob calculates the security parameter k in advance according to the following formula:

$$k=\lceil \log_4[(N+a-1)/a]\rceil \tag{3}$$

Alice and Bob generate their respective FOKs by the following method:

$$F_\alpha = \bigoplus_{j=\alpha}^{\alpha+k-1 \bmod N+\alpha-1} R_j, 0\le\alpha\le N+a-2 \tag{4}$$

Step6 Honesty test, for the a bit she knows, Alice randomly chooses $a-1$ bits to test Bob's honesty. That is, she asks Bob to disclose the bit values corresponding to these bits. If the values Bob discloses are not exactly the same as the values recorded by Alice, then we consider Bob to be dishonest. Once Bob is found to be deceptive, Alice will terminate this round of key establishment and return directly to Stepl; otherwise Alice and Bob each discard these $a-1$ detected bits in FOK and leave the remaining key bits unchanged (including no change in relative position), noted as FCOK, and then continue to the next step.

Step7 Secret shift operation, Alice computes the value of shift factor s based on her secret integer x and the known bit subscript y of the key FCOKA, non-sent to Bob:

$$s=y-x \tag{5}$$

Step8 Based on the computed s values, Alice and 1Bob each II s shift their key FCOK. Where $x<0$ represents right shift and $s>0$ represents left shift. After shifting, the key at Bob is noted as K_i and at Alice as K_i^*. In this way, Bob knows all the bits of key K_i, while Alice knows only one bit of K_i^*, i.e., $K_i^*(x)$.

2.3. Quantum key distribution network based on switching nodes

2.3.1. Quantum Key Distribution Networks Based on Trusted Relaying. The quantum key distribution network based on trust relay is currently the most feasible quantum key distribution network, which utilizes the principle of one secret at a time to realize the key transfer between multiple trustworthy relay nodes at a distance, based on the trustworthy relay quantum key distribution network as shown in Figure 1. The distribution of quantum keys K1, K2 and K3 can be performed between Alice and node 1, node 1 and node 2, and node 2 and Bob. Between Alice and Bob, the interval is large so that direct quantum key distribution is not possible or the rate of quantum key distribution is low. To realize the distribution of key between Alice and Bob take the following approach:

1) Alice generates a set of random sequences, which is the key K to be distributed between Alice and Bob, called the global key;

2) Alice encrypts the global key K using the quantum key K1 in a one-at-a-time fashion, i.e., $S_1=K1\oplus K$;

3) Alice sends S_1, over the classical channel, to node 1

4) Node 1 decrypts S_1 using the quantum key K1 shared with Alice and obtains K, i.e., $K = K1 \oplus (K1 \oplus K)$

5) Node 1 and node 2 repeat Alice's operation;

6) Bob receives the encrypted message S_3 from the classical channel and decrypts it using K3 to obtain the global key K, i.e., $K = K3 \oplus (K3 \oplus K)$, and a key distribution process based on the trusted relay node is completed.

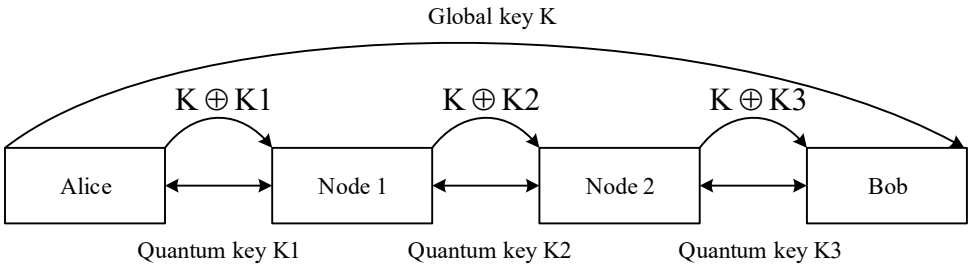

Fig. 1. Based on trusted relay quantum key distribution network

The quantum key distribution networking scheme based on trust relaying is very easy to implement, while key distribution between two or more points separated by any distance can be accomplished theoretically. However, in this type of network, all the nodes on the path that the global key distribution passes through are informed of the global key K. Therefore, in order to ensure the security of the key, it is necessary to require that all the intermediate nodes are trustworthy. If the intermediate nodes are insecure, then the unconditional security of key distribution established by quantum mechanics will be gone. In order to solve this problem, a compromise route, namely multipath secret sharing, has been proposed. The multipath structure is shown in Fig. 2, where the key distribution between Alice and Bob is done through two paths: through Alice, node 1, node 2, and Bob share the key Kl: through Alice, node 3, node 4, and Bob share the key K4, and the final key shared between Alice and Bob is $K1 \oplus K4$. Under this mechanism, any key between the key K4 and the K1 set of keys are not in danger of being intercepted by the eavesdropper, and only when both sets of keys are stolen at the same time the eavesdropper gets the complete key $K1 \oplus K4$. Thus by this way the security of key distribution is increased probabilistically.

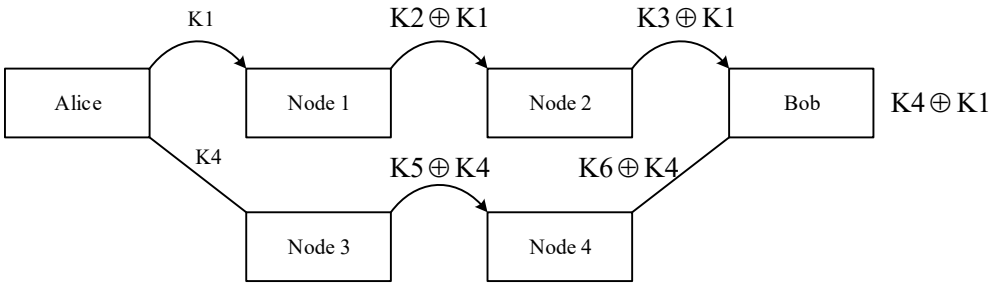

Fig. 2. Multipath structure

2.3.2. Quantum Key Distribution Network Construction Based on Switching Nodes. At present, the key devices and point-to-point communication technology of quantum confidential communication are gradually maturing, and the future quantum communication will inevitably develop in the direction of networking and globalization, therefore, the networking technology is the key to realize the wide-area coverage of the quantum communication network to be solved, and to this end, we design the hardware prototype of reconfigurable and scalable quantum switching node based on the

"space-division-wave-division" switching and complete the functional verification for the conversion of the path of quantum key distribution. To this end, we design a reconfigurable and scalable quantum switching node hardware prototype for quantum key distribution path conversion based on "space-division-wave-division" switching and supporting four-port dual-wavelength, and complete its functional verification. At the same time, we also design a low-cost multi-functional quantum node structure supporting single-fiber bi-directional transmission, which saves a lot of fiber and wavelength resources.

Aiming at the shortcomings of simple structure and lack of flexibility of the current switching node for quantum switching network, a four-port dual-wavelength switching node prototype based on "space division + wavelength division" switching has been designed by utilizing six optical switches, and its basic structure includes a transmission function module, a control function module and a network element management module. Its basic functions include: switching function, split-insertion function, control function, and management function.

Alice end adopts narrow pulse weak coherent laser source to generate carrier signal, Bob adopts single photon detector to receive single photon signal, and the quantum switching node is used to dynamically connect the transceiver and transmitter which need to communicate. The receiver and sender use phase modulation, and the phase modulation demodulation function is realized by the double unequal arm interference loop structure, which can realize the quantum key distribution between the sender and receiver together with the BB84 protocol. This system consists of three parts: the optical circuit part, the circuit control part and the upper computer part. At the same time, synchronous light, classical light and quantum signal are multiplexed into one optical fiber for transmission through CWDM, and reach the demultiplexing after path selection through the quantum switching node, and the synchronous signal light source and the quantum signal light source use the same trigger.Alice and Bob complete the quantum key negotiation, and complete the encrypted transmission and decryption of the system data. The structure of the quantum key distribution network based on the switching node is shown in Fig. 3. This network is vertically divided into three layers, with the quantum transmission layer at the bottom, the control layer in the middle, and the application layer at the top. The quantum transmission layer, i.e., the quantum key distribution network based on the exchange node is built with three users Alice, Bob, and Carot using only one pulsed laser between each two users. Because there is no need to generate keys all the time in the process of key distribution, Alice-Bob, Alice-Carot, and Bob -Carot can utilize the system idle time to time-share the key distribution between them, and the formed keys exist in their respective key pools. The whole process also includes transmission of quantum, synchronized and classical signals, and routing control of exchange nodes.

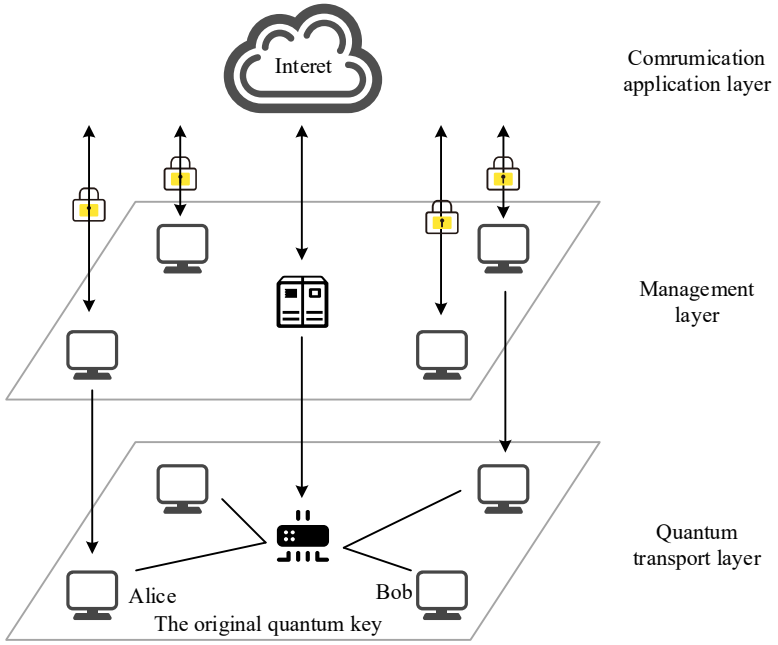

Fig. 3. The quantum key distribution network structure based on the exchange node

3. Quantum key distribution network simulation experiment

3.1. Simulation analysis based on trust relay network

In order to study and verify the feasibility of the key distribution network in this paper, a quantum key distribution network simulation platform is built in this paper. The subsection will simulate and analyze two different algorithms as a comparison. The simulation content is mainly divided into two parts, firstly, the impact on call loss in the case of multipath transmission is simulated, and secondly, the impact on network call loss in the case of single-path transmission is simulated, so as to verify the feasibility of the algorithmic scheme of this paper.

3.1.1. Network call loss analysis. In the simulation process, the parameters that need to be set are the call volume, key generation rate, speech coding rate, and the initial key volume of the key pool, and in order to analyze the call loss of the network it is also necessary to count the number of calls and the number of rejections in the network. The call loss of the trust relay QKD network is obtained by setting the call volume to 0.12erl and the quantum key generation rate to 5Kbps, and the simulation results are shown in Fig. 4. From this simulation result, it can be seen that the algorithm used in this paper makes the network call loss basically remain between 12 and 18% after 20 minutes, and the average network call loss is 15.2%.

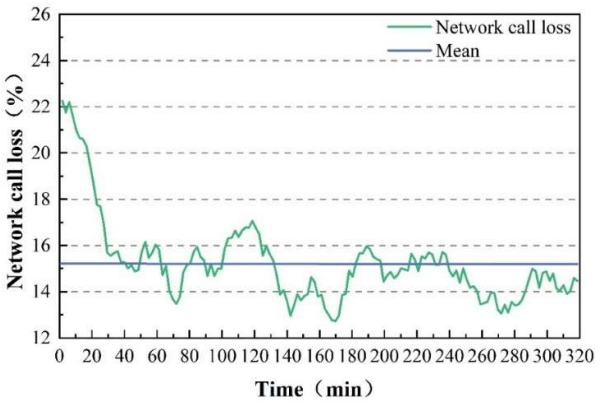

Fig. 4. Network call loss simulation results(5Kbps)

For further verification, the quantum key generation rate is increased to 20Kbps, and the resulting call loss of the trusted relay QKD network is shown in Fig. 5. From this simulation result, it can be seen that the call loss of the network is controlled between 0 and 6%, and the average call loss is 3.67%, which is below 4%. It shows that in the case of fixed call volume, increasing the key generation rate will greatly reduce the call loss of the network, which can well meet the system requirements, i.e., the feasibility of this scheme is verified.

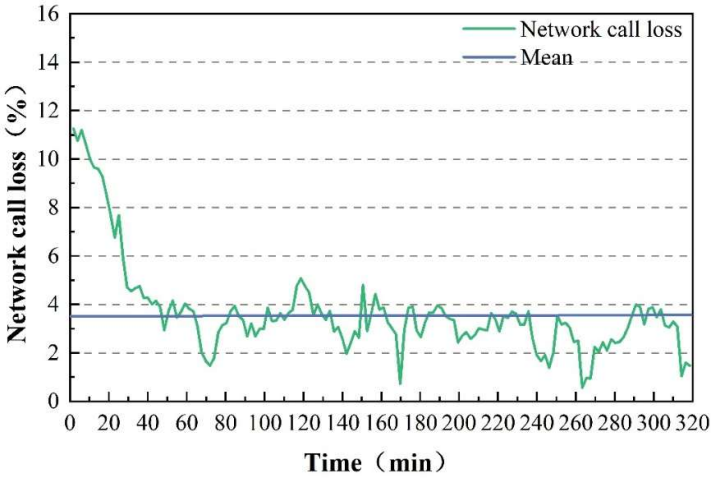

Fig. 5. Network call loss simulation results(20Kbps)

3.1.2. Comparative analysis of network call loss. In this paper, simulations are conducted from a single path to verify the impact of this paper's method on the network call loss. Multipath is considered from the enhancement of the overall security of the network, however, from the theoretical analysis, the design of multipath will inevitably increase the call loss of the network, and the requirement for the key generation rate will certainly be higher. Therefore, in this paper, the call volume is set to 0.12erl, the quantum key generation rate is set to 5Kbps, and the single-path routing algorithm based on bandwidth utilization is used to compare with the method in this paper. The comparison of network call loss of different methods is shown in Fig. 6, from the simulation results, it can be seen that the network call loss can be reduced to less than 11% in the same situation when using the method of this paper, the network call loss is smaller, which shows that the method proposed in this paper has high requirements on the key generation rate, but it can effectively improve the security of the network.

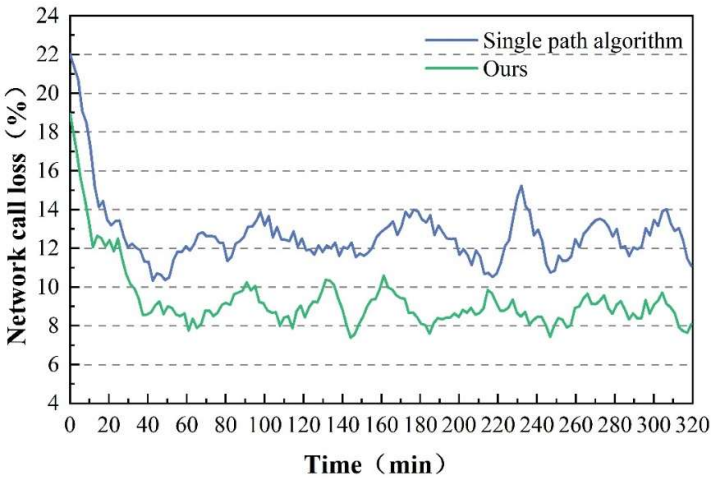

Fig. 6. The network call loss comparison of different methods

3.2. Quantum Key Distribution Network Performance Testing

Verify the effectiveness of the method of this paper, the pre-improved quantum key distribution node stability test is compared with the method of this paper. The phase difference between the transmitter and receiver are kept in phase, and the results of the pre-improved quantum key distribution node stability test are shown in Figure 7. From the figure, it can be seen that the phase change period is about 3 minutes, and the visibility of interference fringes can be calculated based on the maximum and minimum values of the measured single photon counts, and the visibility of interference fringes of this node is about 98%. After a long period of testing and observation, it is found that the visibility of interference fringes of the fiber optic quantum key distribution node deteriorates significantly after a period of normal operation. After careful study and comparison, it is found that due to the use of flange connection for the optical devices in the quantum key distribution node, the long period of operation may cause the node arm length difference to shift, and the visibility of interference fringes decreases, which ultimately results in the increase of the quantum key bit error rate.

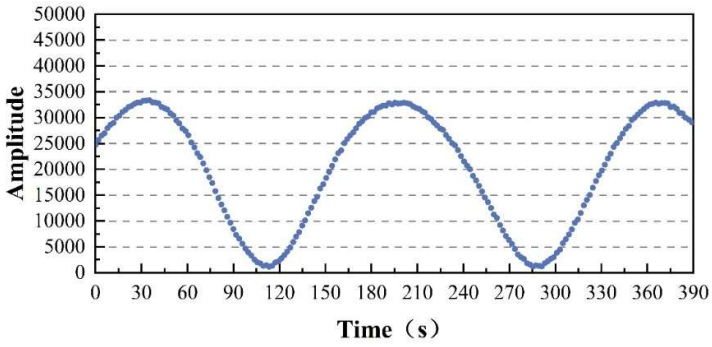

Fig. 7. The results of the test results of the former quantum key distribution node stability

The stability test results of the improved quantum key distribution node in this paper are shown in Fig. 8. After the stability measurement of the improved quantum key distribution node using the independently designed and developed single-photon detector monitoring program, it can be seen that the stability period of the improved node is greatly improved, and the period of the phase change is increased to about 10 minutes. Thus, the time interval of phase tracking compensation can be appropriately increased in the process of quantum key distribution to improve the system quantum key generation rate and reduce the quantum key BER at the same time. It shows that the improved quantum key distribution node in this paper has better effects and can be practically applied to the face recognition system.

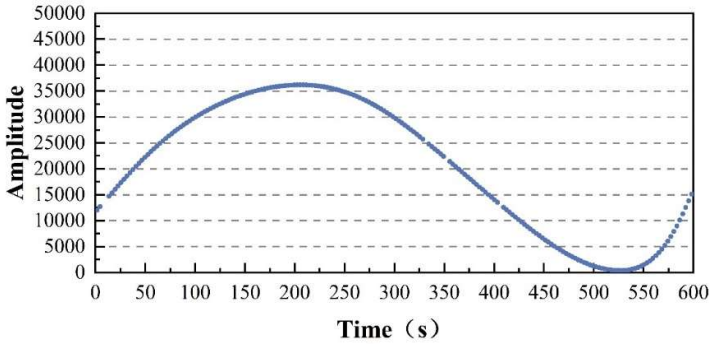

Fig. 8. Improved post-node stability test results

4. Conclusion

This paper optimizes the password protection based on quantum key distribution for face recognition system, and constructs a quantum key distribution network based on trust interruption and exchange nodes.

In the simulation experiment, in the call volume set to 0.12erl, quantum key generation rate of 5Kbps, the algorithm adopted by this paper makes the network after 20 minutes of call loss basically maintains between 12~18%, the average network call loss is 15.20%. While increasing the quantum key generation rate to 20Kbps, the average call loss is 3.67%, and the network loss is reduced by 11.53%, which indicates that in the case of a fixed amount of traffic, increasing the key generation rate will greatly reduce the call loss of the network, which can well meet the system requirements, and verifies the feasibility of this scheme. In addition, the single-path routing algorithm based on bandwidth utilization is compared with the method of this paper, and the network call loss can be reduced to less than 11% when the method of this paper is used in the same situation, and the network call loss is smaller, which further verifies the performance of the method of this paper.

The phase change period after the present optimization is about 3 minutes, and the visibility of the interference fringes of the node is about 98%. At the same time, the fiber optic quantum key distribution node after a period of normal operation, the visibility of interference fringes deteriorates significantly, causing the node arm length difference to appear offset, and the quantum key BER increases. The node stabilization period is greatly improved after the improvement in this paper, and the phase change period is increased to about 10 minutes. The quantum key generation rate of the system is improved while the quantum key BER is reduced. It shows that the quantum key distribution node improved in this paper gets good results.

References

[1] Li, L., Mu, X., Li, S., & Peng, H. (2020). A review of face recognition technology. IEEE access, 8, 139110-139120.

[2] Adjabi, I., Ouahabi, A., Benzaoui, A., & Taleb-Ahmed, A. (2020). Past, present, and future of face recognition: A review. Electronics, 9(8), 1188.

[3] Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face recognition: Past, present and future (a review). Digital Signal Processing, 106, 102809.

[4] Singh, S., & Prasad, S. V. A. V. (2018). Techniques and challenges of face recognition: A critical review. Procedia computer science, 143, 536-543.

[5] Orrù, G., Marcialis, G. L., & Roli, F. (2020). A novel classification-selection approach for the self updating of template-based face recognition systems. Pattern Recognition, 100, 107121.

[6] Wang, M., & Deng, W. (2021). Deep face recognition: A survey. Neurocomputing, 429, 215-244.

[7] Almabdy, S., & Elrefaei, L. (2019). Deep convolutional neural network-based approaches for face recognition. Applied Sciences, 9(20), 4397.

[8] Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face recognition systems: A survey. Sensors, 20(2), 342.

[9] Nawaz, N. (2020). Artificial intelligence applications for face recognition in recruitment process. Journal of Management Information and Decision Sciences, 23, 499-509.

[10] Zeng, M., & Chiu, C. L. (2021, November). The use of facial recognition for online business with the perspective of customer adoption. In 2021 14th CMI International Conference-Critical ICT Infrastructures and Platforms (CMI) (pp. 1-7). IEEE.

[11] Sun, W., Wang, W., & Bai, C. (2024). A new method of large integer prime decomposition for network public

key cryptosystem. International Journal of Security and Networks, 19(3), 159-167.

[12] Yu, Q. (2024). Network data privacy security aggregation method based on big data pattern decomposition. International Journal of Computer Applications in Technology, 74(1-2), 26-33.

[13] Manasrah, A. M., AL-Rabadi, A. R., & Kofahi, N. A. (2020). Key pre-distribution approach using block LU decomposition in wireless sensor network. International Journal of Information Security, 19(5), 579-596.

[14] Li, D., Xiong, S., & Yuan, G. (2023). Large Integer Decomposition Encryption Algorithm for Computer Network Data Communication Combined with Double BP Neural Network Combination Model. Procedia Computer Science, 228, 609-618.

[15] Yuan, C., Chen, W., & Li, D. (2018). A Hierarchical Matrix Decomposition-Based Signcryption without Key-Recovery in Large-Scale WSN. Wireless Communications and Mobile Computing, 2018(1), 5929828.

[16] Feng, J., Yang, L. T., Zhu, Q., & Choo, K. K. R. (2018). Privacy-preserving tensor decomposition over encrypted data in a federated cloud environment. IEEE Transactions on Dependable and Secure Computing, 17(4), 857-868.

[17] Bi, H. (2022). Aggregation encryption method of social network privacy data based on matrix decomposition algorithm. Wireless Personal Communications, 127(1), 369-383.

[18] Senthoor, K., & Sarvepalli, P. K. (2022). Theory of communication efficient quantum secret sharing. IEEE Transactions on Information Theory, 68(5), 3164-3186.

[19] Khorrampanah, M., & Houshmand, M. (2022). Effectively combined multi-party quantum secret sharing and secure direct communication. Optical and Quantum Electronics, 54(4), 213.

[20] Cao, Y., Zhao, Y., Wang, Q., Zhang, J., Ng, S. X., & Hanzo, L. (2022). The evolution of quantum key distribution networks: On the road to the qinternet. IEEE Communications Surveys & Tutorials, 24(2), 839-894.

[21] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., ... & Voznak, M. (2020). Quantum key distribution: a networking perspective. ACM Computing Surveys (CSUR), 53(5), 1-41.

[22] Zhu, D., Li, X., Li, X., Wei, R., Wu, J., & Song, L. (2018). A Quantum Identity Authentication Protocol Based on Optical Transmission & Face Recognition. International Journal of Online Engineering, 14(4).

[23] Román, R., Arjona, R., López-González, P., & Baturone, I. (2022, September). A quantum-resistant face template protection scheme using kyber and saber public key encryption algorithms. In 2022 International Conference of the Biometrics Special Interest Group (BIOSIG) (pp. 1-5). IEEE.

[24] Abdelfatah, R. I. (2024). Robust biometric identity authentication scheme using quantum voice encryption and quantum secure direct communications for cybersecurity. Journal of King Saud University-Computer and Information Sciences, 36(5), 102062.