Quantum Authentication Scheme Based on Fingerprint-Encoded Graph States

Fei Li[1], Ying Guo[1(✉)], and Jiankun Hu[2]

[1] School of Information Science and Engineering, Central South University, Changsha 410083, China
yingguo@csu.edu.cn
[2] School of Engineering and Information Technology, University of New South Wales at Australian Defence Force Academy, Canberra, ACT 2610, Australia

Abstract. We demonstrate an improved quantum authentication scheme which involves fingerprint recognition and quantum authentication. This scheme is designed to solve the practical problem in knowledge-based quantum authentication systems. It can satisfy the requirement of secure remote communication by using fingerprint-encoded graph states. The encoded graph states, which determine the preferred legitimate participants in the deterministic network, enable the facility of the implementable fingerprint-based authentication. The fingerprint template used for authentication in this scheme is of revocability and diversity. Security analysis shows that the proposed scheme can effectively defend various attacks including forgery attack, intercept-resend attack and man-in-the-middle attack. What's more, this novel scheme takes advantages of the merits in terms of both fingerprint recognition and quantum authentication, rendering it more secure, convenient and practical for users than its original counterpart, knowledge-based quantum authentication.

Keywords: Fingerprint · Graph state · Authentication · Security
Quantum cryptography

1 Introduction

Most of the classical authentication algorithms depend on computational complexity and intractable mathematical problems [1,2]. However, with the rapid development of quantum technology, and especially the realization of a quantum computer, the classical algorithms may be broken, and thus the conventional authentication systems, including fingerprint recognition, will be in potential danger. Thus, a new authentication approach, namely the quantum authentication, comes into being. The main argument in favor of quantum authentication

Project supported by National Natural Science Foundation of China (Grant No. 61379153, 61572529).

J. Hu et al. (Eds.): MONAMI 2017, LNICST 235, pp. 164–177, 2018.
https://doi.org/10.1007/978-3-319-90775-8_14

originates from its tantalizing promise of providing unconditional security and detection against eavesdropping, due to the fundamental properties of quantum mechanics [3,4].

Recently, several quantum authentication protocols have been proposed in both theoretics and implementations. Dušek et al. [5] put forward an authentication protocol which combines quantum key distribution and classical identification procedure. Ljunggren et al. [6] proposed an authority-based user authentication system in quantum key distribution. Zhang et al. [7] presented an one-way quantum identity authentication protocol based on ping-pong technique and property of quantum controlled-NOT gate. Also, based on ping-pong technique, Yuan et al. [8] proposed an authentication protocol by using single-particle states. Chang et al. [9] presented an authentication protocol based on three-particle W state and quantum one-time pad. Naseri proposed a revisiting quantum authentication scheme based on entanglement swapping [10].

Nevertheless, the quantum authentication protocols which have been proposed are basically based on what you know. With the extensive application of quantum authentication and the deep development of informationization, authentication mechanisms based on what you know won't suffice to verify a person's identity [11]. Because, inevitably, these quantum authentication protocols will suffer the same trouble as those conventional and knowledge-based authentication protocols. For instance, with the development of the network, more and more people will need to remember a large of number of passwords, such as for online-banking, e-mail, social networks and so on, which is evidently inconvenient and makes users prone to errors. Thus, in order to memorize better, the authentication information tends to be short, which readily leads to security issues. However, if the authentication information is long for safety concerns, it will be easily forgotten. With practical application of quantum authentication, this problem has to be solve. Fortunately, combining fingerprint recognition and quantum authentication can ingeniously solve this problem, because only with the scanning of users finger over the sensor, the identity authentication process will be completed. However, the detailed realization of fingerprint-based quantum authentication protocols has not been discussed yet.

In the past decades, various types of fingerprint recognition methods have been proposed [12–15]. Comparing to other biometric traits, fingerprint has its own unique characteristics. There are no two identical fingerprints in the world so that other people can't pretend to be legitimate users. Moreover, fingerprint identifiers cannot be easily misplaced, forged or shared, which guarantees the security of fingerprint recognition. Thus, fingerprint-based quantum authentication not only possesses the advantage of unconditional security and detection against eavesdropping during the remote transmission, but also it is more convenient and practical than the knowledge-based authentication. The proposed fingerprint-based authentication methods can be divided into two categories, namely alignment-based [16] and alignment-free [17] approaches. For the alignment-based approach, a registration point(core) is required to align the

fingerprint image before further processing. In contrast to the alignment-based approach, no registration point is needed in the alignment-free approach.

In this paper, we propose a practical quantum authentication protocol using the fingerprint-encoded graph states. Graph state, as a special entangled quantum state, can be expressed by a mathematical graph whose vertices and edges are superb resources for establishing an elegant quantum network [19]. Compared to other quantum states, using the fingerprint-encoded graph states to transmit messages has several peculiar advantages. On one hand, graph states are the most easily available multipartite quantum states [20,21]. On the other hand, each graph state can be represented with a mathematical graph so that it is conducive for us to understand how information spreads.

The rest of the paper is structured as follows. Section 2 details the framework of our authentication protocol. Section 3 shows the security of the proposed protocol. Finally, the conclusion is drawn in Sect. 4.

2 The Authentication Scheme with the Fingerprint-Encoded Graph States

2.1 Binary Representation Generation of Authentication

Fingerprint is an important feature of human beings. The word *fingerprint* is popularly perceived as synonymous with individuality. The most significant structural characteristic of a fingerprint is the pattern of interleaved ridges and valleys. Usually, ridges run smoothly in parallel but exhibit one or more regions where they assume distinctive shapes (characterized by high curvature, frequent ridge terminations, etc.). These regions, called singularities or singular regions. According to the characteristic of singular regions, fingerprint can be classified into five categories: left loop, right loop, whorl, arch and tented arch. The core point corresponds to the center of the north most loop or whorl type singularity. For arch fingerprints and tented-arch fingerprints, the core point is difficult to be defined. Even, for loop fingerprints and whorl fingerprints, sometimes it is also difficult to correctly locate the core point due to the high variability of fingerprint patterns during capture. Thus, the type of the selected fingerprint has a great influence on the security of alignment-based authentication, because the accuracy of alignment-based authentication depends highly on the core point, while the security of alignment-free authentication is independent of the type of the selected fingerprint.

In what follows, we describe an alignment-free revocable fingerprint template generation. The fingerprint can be represented by a set of minutiae points extracted from the fingerprint image, which is denoted by $m_i = \{x_i, \mathrm{y}_i, \theta_i\}$, where x_i, y_i and θ_i are the x, y coordinates and the orientation of the i^{th} minutiae, respectively. Due to various factors during fingerprint capture, single minutiae point is readily subjected to elastic deformation, while a minutiae pair which is formed by two minutiae points tends to be immune to nonlinear distortion. The procedure of extracting binary information from minutiae pairs is listed below.

Step 1. **Features extracted from minutiae pairs**. We connect a pair of minutiae by a straight line. The invariant features used in our work are the length L between the two minutiae points and two angles, denoted by α and β, between the orientation of each minutiae and the straight line. Let F_{ij} represent the invariant feature extracted from a minutiae pair which is made up of the minutiae m_i and m_j. As shown in Fig. 1, $F_{ij} = \{L_{ij}, \alpha_i, \beta_j\}$.

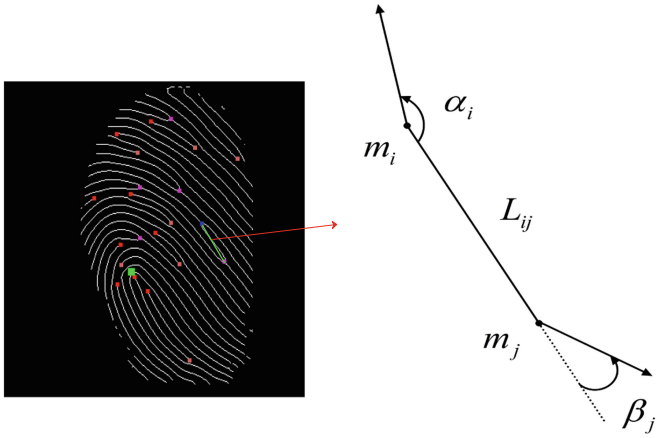

Fig. 1. The invariant feature extracted from the minutiae pair (m_i, m_j). L_{ij} is the length between the two minutiae pair. α_i and β_i are the angles between the straight line and the orientations of the minutiae m_i and m_j, respectively.

In order to obtain the value of F_{ij}, the values X_{ij} and Y_{ij} need to be calculated as follows:

$$\begin{bmatrix} X_{ij} \\ Y_{ij} \end{bmatrix} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i \\ \sin\theta_i & \cos\theta_i \end{bmatrix} \begin{bmatrix} x_j - x_i \\ -(y_j - y_i) \end{bmatrix}. \tag{1}$$

Therefore, we have

$$L_{ij} = \sqrt{X_{ij}^2 + Y_{ij}^2}, \quad \alpha_i = \arctan(\frac{Y_{ij}}{X_{ij}}), \quad \beta_j = \alpha_i + \theta_j - \theta_i. \tag{2}$$

Step 2. **Quantization of the invariant features.** In order to resist the nonlinear distortion brought during the image acquisition, the features need to be quantized. An appropriate quantization step, that is the number of bits to quantize each feature, should be judiciously determined by experiments. Because, the accuracy of the system is closely dependent on quantization. Let len, a_1 and a_2 represent the length of binary representation of L_{ij}, α_i and β_j. So each pair of minutiae can be represented by a bit string whose length is $N = len + a_1 + a_2$.

Step 3. **Generation of the bit-string fingerprint representation.** After quantizing all the minutiae pairs, we convert the binary representation into the

decimal form to be the index of the histogram and then calculate the histogram of minutiae pairs. At the beginning, the histogram is made up of 2^N zeros. Then, we inspect each index and the value in the histogram corresponding to the index is added by one. Finally, we binarize the histogram with a simple rule that the value 1 in the histogram is retained whereas the rest of values is set to 0. So we get the bit-string representation for the fingerprint.

Step 4. **Permutation of the binary string.** The binary string generated in Step 3 is vulnerable and may be employed to access another fingerprint-based system. Thus, to protect the privacy of users, the string needs to be permuted. The permutation is based on the unique key, which is assigned to each user. In other words, different users employ different manners during permutation. The key for permutation is random so that the permutated template cant reveal any information about the original template without the user-specific key.

2.2 Information Transmission Using Graph States

The graph state is an entangled state, which can be described with a simple undirected graph mathematically [22]. An undirected graph $G = \{V, E\}$ is made up of a set of n vertices and a set of edges $E = \{e_{ij} = (v_i, v_j)\}$, where v_i and v_j are neighbors when there is a edge connecting them. In a graph state, each vertex represents a qubit. All of graph states generate from an initial state [23]

$$|+\rangle^{\otimes n} = H^{\otimes n}|0\rangle^{\otimes n}, \quad H = |+\rangle\langle 0| + |-\rangle\langle 1|, \tag{3}$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and H is the Hadamard operator. After applying the two-qubit controlled-phase gate (denoted by CZ) on all pairs of qubits whose corresponding vertices are adjoining, we can get an initial graph state

$$|G\rangle = \prod_{(v_i,v_j)\in E} CZ_{(v_i,v_j)}|+\rangle^{\otimes n}, \tag{4}$$

where

$$CZ|kk'\rangle = (-1)^{kk'}|kk'\rangle, \quad k, k' \in \{0, 1\}, \quad |kk'\rangle \in H_2^{\otimes 2}. \tag{5}$$

The order of applying CZ gates is unimportant, because the operation possesses the exchange property that establishes the deterministic quantum network.

Usually, each vertex of a graph state is labeled by an index. For instance, the index of the vertex v_i is i. In order to make better use of graph states, we label each vertex with two more bits. So, the vertex v_i is labeled as (i, l_{i1}, l_{i2}). The two extra label bits are employed to transmit classical information. For ease of understanding, we define the quantities $l_{i*} = (l_{i1}, l_{i2})$ for the i^{th} vertex, $l_{*j} = (l_{1j}, l_{2j}, \ldots, l_{nj})$ for the j^{th} bit of all vertices, and $l = (l_{11}, l_{12}, l_{21}, l_{22}, \ldots, l_{n1}, l_{n2})$ for the graph state. By the way, when the vertex has no label, l_{i*} is set to $(0, 0)$. With these additional labels, we can obtain the labeled graph state by

$$|G_l\rangle = \bigotimes_i (X_i^{l_{i1}} Z_i^{l_{i2}})|\tilde{G}\rangle, \quad |\tilde{G}\rangle = \bigotimes_{j|v_j\in V} S_j|G\rangle, \tag{6}$$

where $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ and $S = |0\rangle\langle 0| - i|1\rangle\langle 1|$. The partial phase shift gate [19] is employed to prevent the system from eavesdropping. For the sake of encoding and simplifying the manipulation ,we only retain local Z gates and introduce another kind of graph state, called the encoded graph state

$$|G_{l_{*2}}\rangle = \bigotimes_i Z_i^{l_{i2}} |\tilde{G}\rangle. \tag{7}$$

When l_{i1} is equal to 0 for $\forall i \in V$ in a labeled graph state, the labeled graph state becomes a encoded graph state, which can be expressed in the stabilizer formalism [22]:

$$K_i |G_{l_{*2}}\rangle = (-1)^{l_{i2}} |G_{l_{*2}}\rangle, \quad K_i = X_i \bigotimes_{(v_i, v_j) \in E} Z_j. \tag{8}$$

In the proposed protocol, the three-qubit labeled graph state, as depicted in Fig. 2, is used for the authentication information processing, which can be given by

$$|G_{l_{*2}}\rangle = \bigotimes_{i=1}^{3} Z_i^{l_{i2}} |\tilde{G}\rangle, \quad |\tilde{G}\rangle = \frac{1}{\sqrt{2}}(|0++\rangle + |1--\rangle). \tag{9}$$

Consequently, the encoded graph state can be described by stabilizers

$$K_1 = X_1 \bigotimes Z_2 \bigotimes Z_3, \quad K_2 = Z_1 \bigotimes X_2 \bigotimes I_3, \quad K_3 = Z_1 \bigotimes I_2 \bigotimes X_3, \tag{10}$$

with eigenvalues (l_{12}, l_{22}, l_{32}).

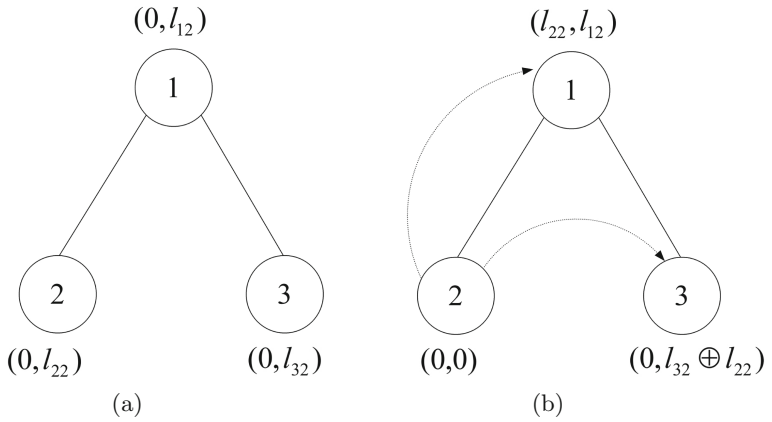

Fig. 2. A labeled graph state for three players and information transmission using the stabilizer. (a) The initial labeled graph state with eigenvalues (l_{12}, l_{22}, l_{32}). (b) By performing the stabilizer K_1 on the encoded graph state, the bit l_{22} is transmitted to other parties, i.e., $l_{1*} = (l_{22}, l_{12})$, $l_{2*} = (0, 0)$, $l_{3*} = (0, l_{32} \bigoplus l_{22})$.

By performing above-derived stabilizers on the graph state, we can accomplish the encoded process. For example, acting upon the encoded graph state by the first stabilizer K_1 results in

$$\begin{aligned} K_1^{l_{22}}|G_{l_{*2}}\rangle &= (X_1^{l_{22}} \bigotimes Z_2^{l_{22}} \bigotimes Z_3^{l_{22}})(\bigotimes_{i=1}^{3} Z_i^{l_{i2}}|\tilde{G}\rangle) \\ &= X_1^{l_{22}} Z_1^{l_{12}} \bigotimes I_2 \bigotimes Z_3^{l_{22}} Z_3^{l_{32}}|\tilde{G}\rangle \\ &= |G_{l=(l_{22},l_{12},0,0,0,l_{32} \bigoplus l_{22})}\rangle \\ &= (-1)^{l_{12}l_{22}}|G_{l_{*2}}\rangle. \end{aligned} \tag{11}$$

It implies that the bit l_{22} is transmitted from the vertex v_2 to v_1 and v_3. After that, we take local Pauli measurements in bases $\{X_i, Y_i, Z_i\}$ to get one-bit outcomes s_i^X, s_i^Y and s_i^Z [19,24], respectively. When the measurement outcome is the value 1, s_i^α is set to the value 0. Otherwise, s_i^α is assigned the value 1. Finally, we access the labeled bits by using the relations

$$l_{22} = s_1^Z \bigoplus s_2^X, \quad l_{32} = s_1^Z \bigoplus s_3^X. \tag{12}$$

2.3 Implementation of Authentication Processing

Suppose that Alice is the user, Bob is the server of a certain application which possesses the users' fingerprint templates, and Trent acts as the reliable third party. Then we detail the practical implementation of the fingerprint-based quantum authentication in the deterministic network.

Enrollment Phase. In this phase, the system needs to generate a fingerprint template for Alice. Firstly, Alice's fingerprint characteristic is sensed and captured by a fingerprint scanner to produce a fingerprint sample. Usually, a quality checking operation is first implemented to guarantee that the acquired sample is reliable enough for successive processing. Then, we extract the minutiae from the fingerprint and generate the binary representation (denoted by $E^n(x)$). Taking $E^n(x)$ as the control parameter, Alice's fingerprint template can be constructed as

$$|f_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{E_i(x)}|i\rangle, \tag{13}$$

which is kept by Bob. After that, Alice and Bob obtain their keys K_a and K_b through quantum key distribution in quantum networks, where K_a is the key shared between Alice and Trent, and K_b is the key between Bob and Trent.

Authentication Phase. In this phase, Alice submits a request to Trent and claims that she is Alice and wants to communicate with Bob.The authentication procedure among Alice, Bob and Trent, as shown in Fig. 3, is listed below.

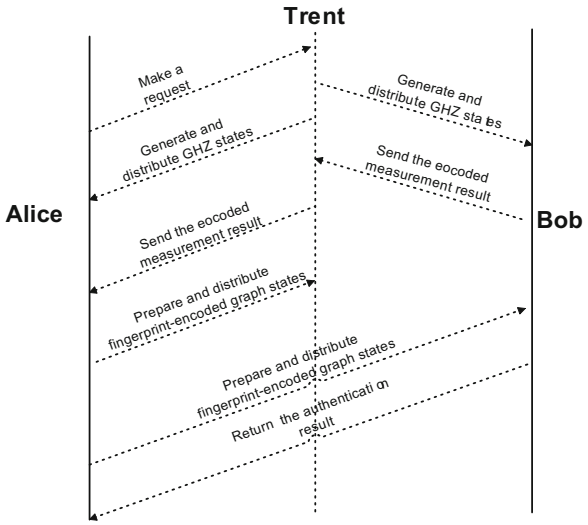

Fig. 3. The procedure of authentication. After receiving Alice's request, Trent prepares GHZ states and distributes them to Alice and Bob, respectively. Then, there is a qualification examination among Alice, Bob and Trent. After that, Alice inputs her fingerprint and the system generates the authentication information, which is encoded into graph states and sent to Bob and Trent by performing stabilizers on graph states. Finally, Bob compares the authentication information with the enrollment template and returns the authentication result.

Step 1. Trent generates k GHZ tripartite states after receiving Alice's request. Two particles of each GHZ tripartite state are transmitted to Alice and Bob respectively and the remaining one is kept by himself. Bob and Trent randomly measure their own particles, leading to Bob's measurement result R_b and Trent's measurement result R_t.

Step 2. Bob encrypts R_b with the key K_b

$$y_b = K_b(R_b), \tag{14}$$

and then sends y_b and R_b to Trent through a classical channel.

Step 3. Trent decrypts y_b with the key k_b

$$R'_b = K_b(y_b). \tag{15}$$

If R'_b is equal to R_b, it implies that Bob is honest. Otherwise, the protocol is aborted. After examining the qualification of Bob, Trent encrypts R_b and R_t with the key K_a

$$y_t = K_a(R_b, R_t), \tag{16}$$

and then sends y_t to Alice through a classical channel.

Step 4. Alice decrypts y_t and selects corresponding measurement bases to measure her particles according to R_b and R_t. After that, she compares her measurement result R_a with R_b and R_t. If the yielded results satisfy the correlation of the GHZ tripartite states, Alice executes the following authentication procedures. Otherwise, Alice supposes that Trent is dishonest or the channel is insecure and then the protocol will be aborted.

Step 5. Alice inputs her fingerprint and the system generates a binary representation(denoted by $E^n(y)$) for the fingerprint with the afore-described method in enrollment phase.

Step 6. Alice prepares n three-qubit encoded graph states. The label of the i^{th} encoded graph state is $l^i = (0, 0, 0, E_i(y), 0, 0)$. Alice retains the second particle of each graph state and distributes the first particle of each graph state to Trent. And the other particles are sent to Bob.

As shown in Fig. 4, applying the first stabilizer K_1^i on the i^{th} encoded graph state for all i yields

$$(K_1^i)^{E_i(y)}|G_{l^i=(0,0,0,E_i(y),0,0)}\rangle = |G_{l^i=(E_i(y),0,0,0,0,E_i(y))}\rangle, \tag{17}$$

where $1 \leq i \leq n$. It indicates that the bit $E_i(y)$ is transferred from Alice to Bob and Trent.

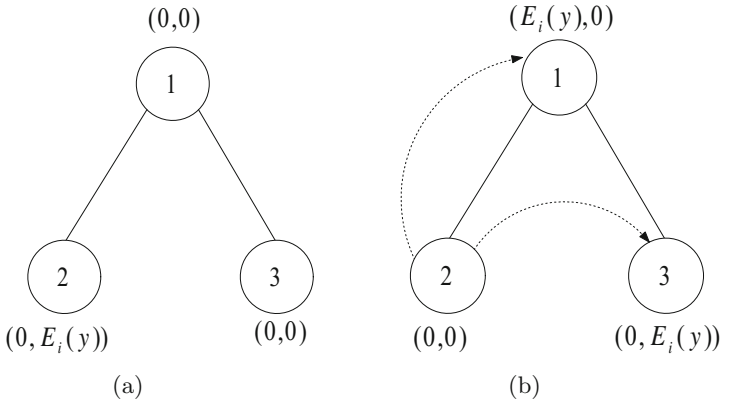

Fig. 4. Transmission of the representation information. (a) The initial encoded graph state with the label $l = (0, 0, 0, E_i(y), 0, 0)$. (b) Equivalent state with the representation bit $E_i(y)$ transmitted from Alice to Bob and Trent.

Step 7. Bob applies measurement operations on the yielded encoded graph state $|G_{l^i=(E_i(y),0,0,0,0,E_i(y))}\rangle$, and obtains the binary representation $E^n(y)$ of Alice's fingerprint. According to $E^n(y)$, the authentication qubit (denoted by $|f_y\rangle$) is generated by

$$|f_y\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{E_i(y)}|i\rangle. \tag{18}$$

Step 8. Bob compares the authentication qubit with the enrollment qubit. The similarity score will be obtained by calculating their inner product

$$Score = (|f_x\rangle, |f_y\rangle). \tag{19}$$

If the score is above the threshold, Bob regards Alice as a legitimate user. Otherwise, Bob rejects Alice's request.

In the above-mentioned authentication scheme, the encoding operations of the stabilizers is simple and readily implemented, and thus the transmission and measurement of the authentication information can be achieved handily by performing local unitary operations rather than the complicated joint operations in the traditional schemes.

3 Security Analysis

3.1 Forgery Attack

The forgery attack is focused on the strategy of non-message attack, lost-key attack and cross-matching attack. The fingerprint database FVC2002 DB1 is used to test our proposed scheme. In order to evaluate the accuracy of a fingerprint-encoded authentication system, the false acceptance rate (FAR) and the false rejection rate (FRR) should be introducted. FAR is the probability of mistaking two fingerprints from two different fingers to be from the same finger, whereas FRR is the probability of mistaking two fingerprints from the same finger to be from two different fingers.

Non-message attack: The attacker, Eve, pretends to be a legitimate user and attempts to pass through the authentication without any valid information. In such a situation, the probability of a successful attack is $P = (\frac{1}{2})^N$. Obviously, when N is big enough, the probability is $P = (\frac{1}{2})^N \approx 0$. To demonstrate the performance of the proposed protocol under non-message forgery attack, every user is assigned with a unique user-specific key in our experiment. As shown in Fig. 5(a), if we select an appropriate threshold, the ideal result, where FAR and FRR are both equal to 0, can be obtained. It indicates that the probability of a successful attack is 0 in practical application.

Lost key attack: It is the worst case where the user's key is known by Eve. In conventional knowledge-based quantum authentication, Eve can successfully pretend herself to be Alice to communicate with Bob when the user's key is compromised. In other words, the probability of a successful lost key attack is 100% in this case. However, in our proposed scheme, even if the user's key has lost, because the key kept by the user is random and independent of the user'fingerprint, Eve still requires a large number of attempts to uncover the binary fingerprint representation. To demonstrate the performance under lost key attack, we performed this experiment by assigning the same key to all users. As shown in Fig. 5(b), it demonstrates that even if the user's key is stolen by Eve, the probability of mistaking the adversary as a legitimate

user is still quite low in our proposed scheme. However, once the user's key has lost in conventional knowledge-based authentication, the system will be completely exposed to the adversary.

Cross-matching attack: Eve attempts to employ the template generated in one application to have access to other applications where the template owner has registered. Because the key for permutation is random, two templates generated from the same user won't match. This case was simulated by using different keys to permute the binary string generated from the same fingerprint impression and then we calculated their similarities. Figure 5(c) shows that the FAR curve in this experiment is similar to the FAR curve for non-message attack and there is a clear separation between the FAR curve and

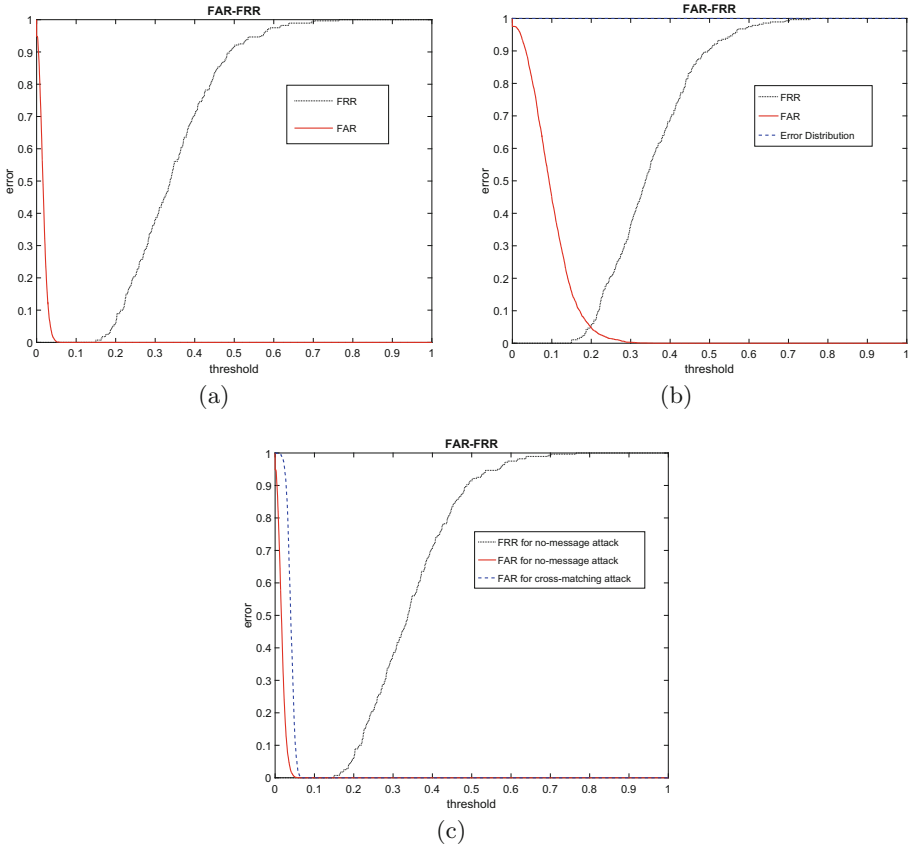

Fig. 5. The probability of a successful forgery attack. Experimental parameters is set as: $len = 6$, $a_1 = 5$, and $a_2 = 5$. (a) The FAR-FRR distribution for non-message attack. (b) The FAR-FRR distribution for lost key attack. The dash blue curve gives the error distribution for the conventional knowledge-based quantum authentication, namely the false acceptance rate under lost key attack. (c) The FAR-FRR distribution for cross-matching attack. (Color figure online)

the FRR curve, as if the templates originating from the same user in different applications are generated from different users. Thus, the cross-matching attack cannot be achieved. Meanwhile, it means revocability and diversity that when an enrolled template is compromised, a new fingerprint template can be regenerated, and it cannot match with the compromised template even though both are generated from the same fingerprint. Due to the revocability and the diversity of the template, the drawback in fingerprint recognition, that the number of each people's fingerprints which are used for authentication is small and limited, can be solved quite well. Furthermore, the original biological authentication information can be well protected from eavesdropping during remote transmission. What's more, compared to the conventional knowledge-based authentication, the users can get rid of remembering a large number of passwords, which can't compromise security.

The user can regularly update the key which is used for permutation to generate a new template. As mentioned above, the new template won't match the old template so that the security of the fingerprint template can be enhanced and guaranteed.

3.2 Intercept-Resend Attack

In order to pass through the authentication, Eve may intercept the particles which Alice sends to Bob or Trent and then resend a forged sequence to Bob or Trent according to her measurement result. However, the label of each particle sent to Bob and Trent is $(0, 0)$, namely having no information about the binary fingerprint representation encoded into these particles. Thus, even if Eve measures the particles intercepted, she obtains nothing, namely

$$I(E, T) = 0, I(E, B) = 0. \tag{20}$$

where $I(E, T)$ is the mutual information between Eve and Trent, and $I(E, B)$ is the mutual information between Eve and Bob. What's more, the correlation between the particles intercepted and the particles kept by Alice is released, which affects transferring the label bits. Thus, even if Eve intercepts the particles, she cannot get any valid information and the disturbed actions can be detected by in the authentication phase.

3.3 Man-in-the-Middle Attack

To obtain the information which Alice sends to Bob, Eve disguises herself as Bob to communicate with Alice, and also plays the role of Alice to communicate with Bob. As we know, in quantum cryptography, there is a fundamental assumption that Eve cannot simultaneously obtain information on quantum channels and classical channels. Therefore, when Eve receives the particles which Trent sends to Alice or Bob and disguises herself to communicate with the other one, according to the assumption, she cannot obtain the information on the classical channels.

Furthermore we consider a situation that Eve plays the role of Trent. Because Eve don't know the correct key corresponding to Alice, the measurement results R_a, R_b and R_t will not satisfy the correlation of the GHZ tripartite states. Therefore, Alice can find that Trent is dishonest and then the protocol will be aborted.

4 Conclusion

We have demonstrated an improved quantum authentication scheme based on fingerprint-encoded graph states. It has the advantages of both fingerprint recognition and quantum authentication in the remote deterministic quantum networks, which is more convenient, practical and secure than knowledge-based quantum authentication. There are two phases, namely enrollment phase and authentication phase, involved in our proposed scheme. In enrollment phase, the system generates the user's fingerprint template which is revocable and diverse, whereas in authentication phase the system generates the binary fingerprint representation for the user and then the binary information is transmitted using the fingerprint-encoded graph states. Security analysis shows that the proposed scheme can effectively defend various attacks including forgery attack, intercept-resend attack and man-in-the-middle attack.

References

1. Niu, P., Chen, Y., Li, C.: Quantum authentication scheme based on entanglement swapping. Int. J. Theor. Phys. **55**, 1–11 (2016)
2. Jin, Z., Teoh, A.B.J., Ong, T., Tee, C.: A revocable fingerprint template for security and privacy preserving. KISS Trans. Internet Inf. Syst. **4**, 1327–1342 (2010)
3. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: QKD-based quantum private query without a failure probability. Sci. China Phys. Mech. Astron. **58**, 100301 (2015)
4. Gaudiano, M., Osenda, O.: Entanglement in a spin ring with anisotropic interactions. Int. J. Quant. Inf. **13**, 1550057 (2015)
5. Dušek, M., Haderka, O., Hendrych, M., Myška, R.: Quantum identification system. Phys. Rev. A **60**, 149–156 (1998)
6. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication and quantum key distribution. Phys. Rev. A **62**, 299–302 (2000)
7. Zhang, Z.S., Zeng, G.H., Zhou, N.R., Xiong, J.: Quantum identity authentication based on Ping-pong technique for photons. Phys. Lett. A **356**, 199–205 (2006)
8. Yuan, H., Liu, Y., Pan, G., Zhang, G., Zhou, J., Zhang, Z.: Quantum identity authentication based on Ping-pong technique without entanglements. Quant. Inf. Process. **13**, 2535–2549 (2014)
9. Chang, Y., Zhang, S., Yan, L., Li, J.: Deterministic secure quantum communication and authentication protocol based on three-particle W state and quantum one-time pad. Sci. Bull. **59**, 2835–2840 (2014)
10. Naseri, M.: Revisiting quantum authentication scheme based on entanglement swapping. Int. J. Theoret. Phys. **55**, 2428–2435 (2016)
11. Maltoni, D., Maio, D., Jain, A., Prabhakar, K.S.: Handbook of Fingerprint Recognition. Springer, London (2009). https://doi.org/10.1007/978-1-84882-254-2

12. Wang, Y., Hu, J.: Global ridge orientation modeling for partial fingerprint identification. IEEE Trans. Pattern Anal. Mach. Intell. **33**, 72 (2011)
13. Jin, Z., Teoh, A.B.J., Ong, T.S., Tee, C.: Generating revocable fingerprint template using minutiae pair representation. In: 2nd International Conference on Education Technology and Computer, pp. 22–24. IEEE Press, New York (2010)
14. Yang, W., Hu, J., Wang, S.: A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement. IEEE Trans. Inf. Forensics Secur. **9**, 1179–1192 (2014)
15. Wong, W.J., Teoh, A.B., Kho, Y.H., Wong, M.L.D.: Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template. Pattern Recogn. **51**, 197–208 (2016)
16. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating cancelable fingerprint templates. IEEE Trans. Pattern Anal. Mach. Intell. **29**, 561–572 (2007)
17. Lee, C.H., Choi, C.Y., Toh, K.A.: Alignment-free cancelable fingerprint templates based on local minutiae information. IEEE Trans. Syst. Man Cybern. **37**, 980–992 (2007)
18. Thomas, A.O., Ratha, N.K., Connell, J.H., Bolle, R.M.: Comparative analysis of registration based and registration free methods for cancelable fingerprint biometrics. In: 19th International Conference on Pattern Recognition, pp. 8–11. IEEE Press, New York (2008)
19. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A **78**, 042309 (2011)
20. Lu, C.Y., Zhou, X.Q., Gühne, O., Gao, W.B., Zhang, J., Yuan, Z.S., Goebe, A., Yang, T., Pan, J.: Experimental entanglement of six photons in graph states. Nat. Phys. **3**, 91–95 (2007)
21. Walther, P., Resch, K.J., Rudolph, T., Schenck, E., Weinfurter, H., Vedral, V., Aspelmeyer, M., Zeilinger, A.: Experimental one-way quantum computing. Nature **434**, 169 (2005)
22. Nest, M.V.D., Dehaene, J., Moor, B.D.: An efficient algorithm to recognize local Clifford equivalence of graph states. Phys. Rev. A **70**, 423–433 (2004)
23. Hein, M., Eisert, J., Briegel, H.J.: Multi-party entanglement in graph states. Phys. Rev. A **69**, 666–670 (2003)
24. Keet, A., Fortescue, B., Markham, D., Sanders, B.C.: Quantum secret sharing with qudit graph states. Phys. Rev. A **82**, 4229–4231 (2010)