Chen et al. *EPJ Quantum Technology* (2023) 10:11
https://doi.org/10.1140/epjqt/s40507-023-00170-5

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Quantum identity authentication based on the extension of quantum rotation

Geng Chen[1,2], Yuqi Wang[1,2*], Liya Jian[1,2†], Yi Zhou[1,2†] and Shiming Liu[1,2†]

*Correspondence:
paiter_w@126.com
[1]School of Computer, Minnan Normal University, Xianqianzhi St, Zhangzhou, 363000, Fujian, P.R. China
[2]Key Laboratory of Data Science and Intelligence Application, Fujian Province University, Xianqianzhi St, Zhangzhou, 363000, Fujian, P.R. China
†Equal contributors

Abstract

In this work, we propose a bit-oriented QIA protocol based on special properties of quantum rotation and the public key cryptographic framework. The proposed protocol exhibited good resistance to both forward search and measure-resend attacks, whereby its security performance was directly related to the length of the authentication code. From our analysis, it was demonstrated that the protocol has good performance, in terms of quantum bit efficiency. In addition, the protocol is well-expandable. The developed protocol is resource-efficient and can be also applied in quantum computing networks.

Keywords: Quantum identity authentication; Qubit rotation; High-dimensional quantum state

1 Introduction

Quantum rotation is considered a basic mathematical tool for representing binary quantum states. More specifically, an angular parameter is used to describe the vector state on the Bloch sphere [1, 2]. Since the objects discussed in this paper are not limited to binary qubit, it will be referred to as quantum rotation in this work.

Quantum rotation, with its unique properties, is regarded as the most fundamental concept of quantum computing, especially in variational quantum circuits [3] and quantum neural computing [4]. The dimension of quantum rotation refers to the dimension of the quantum state that is affected by quantum rotation. From a geometric point of view, the process by which quantum rotation produces its effect is similar to describing a plane rectangular coordinate system in polar coordinates. Combined with the Bloch ball, this can be easily spotted.

Although there are substantial applications in quantum computing and quantum physics, the implementation of quantum rotation in quantum cryptography is much rarer. An important application of quantum rotation can be found in quantum public key cryptography (QPKC). In 2008, Nikolopoulos designed a bit-oriented deterministic QPKC protocol using quantum one-way functions constructed by quantum rotation [5] and proposed a series of improvements over the next few years [6–8]. In our previously reported work [9], the superposition of *two*-dimensional quantum rotation and extended quantum

rotation to *three*-dimensions was demonstrated. These works provide an initial demonstration of the flexibility of quantum rotation in protocol design. The security of these protocols can be also greatly enhanced as the parameters can be set over a wide range. Hence, the protocol for using quantum rotation deserves undoubtedly further research. On the other hand, a large number of experimental works on the preparation and control of quantum states are based on quantum rotation [10, 11], which provides a realistic basis for the feasibility of the above-mentioned protocols and future expansion.

The underlying principle of the quantum identity authentication (QIA) protocol is to verify the identity of the legitimate user to protect quantum communication networks from total breakdown [12]. In the QIA protocol, an authenticating party (Bob) uses quantum means to verify an authenticated party's (Alice) knowledge of a pre-shared key (identification code) [13]. In view of this nature, the means to achieve QIA are numerous, while a general approach is to transform other quantum information protocols to be used for identity authentication. Since the first QIA protocol [14] was proposed in 1995, quantum key distribution (QKD) and quantum entanglement have been widely used to design QIA protocols. Although the QKD-based protocol [15–17] can be easier implemented in reality, the limitations of the QKD protocol itself prevent further security improvements [18, 19]. Quantum entanglement provides high security [20–22], multi-party authentication [23, 24], and semi-quantum authentication [25, 26] for some QIA protocols. However, obviously, these protocols must use quantum memory. As a minor protocol, QIA should be used as little as possible to ensure that it does not burden the major protocol in quantum communication networks. Some other protocols [27–29] face a similar problem of using too many resources for additional purposes, which seem to deviate from the original intent of QIA.

By considering the fundamental role of quantum rotation in quantum circuits, quantum rotation can be used to design a QIA protocol with low resource consumption and high security. On the other hand, it is feasible to convert a QPKC protocol into a QIA protocol and retain the high security and scalability features of the QPKC protocol. Along these lines, in this work, our previous research was first extended by expanding quantum rotation to N-dimensions. On this foundation, a QIA protocol was designed, drawing on the basic ideas of the QPKC protocol, and the security and efficiency of our protocol were systematically analyzed.

The rest of this work is organized as follows. In Section II, the basic properties of quantum rotation were introduced and expanded on the dimensions. In Section III, a detailed description of the proposed QIA protocol was provided. Section IV analyzed the proposed protocol in terms of security and efficiency, and discussed outstanding issues and protocol expansions. Finally, in Section V, the main conclusions are presented.

2 Expansion of quantum rotation

In our previously reported work, quantum rotation was expanded to *three*-dimensional situations [9]. The main focus was led on the unique property of the quantum rotation parameter, namely superposition, which is the basis for many subsequent application protocols. In this section, the dimensionality of quantum rotation will be further expanded.

Table 1 Geometric significance of quantum rotation

Initial state	Rotation direction[1]	Final quantum state[2]
$\|0\rangle$	Clockwise	$R(\theta)\|0\rangle = \cos(\frac{\theta}{2})\|0\rangle + \sin(\frac{\theta}{2})\|1\rangle$
$\|0\rangle$	Anti-clockwise	$R(-\theta)\|0\rangle = \cos(\frac{\theta}{2})\|0\rangle - \sin(\frac{\theta}{2})\|1\rangle$
$\|1\rangle$	Clockwise	$R(\theta)\|1\rangle = -\sin(\frac{\theta}{2})\|0\rangle + \cos(\frac{\theta}{2})\|1\rangle$
$\|1\rangle$	Anti-clockwise	$R(-\theta)\|1\rangle = -\sin(\frac{\theta}{2})\|0\rangle - \cos(\frac{\theta}{2})\|1\rangle$

[1] Rotation direction refers to the direction in the quantum state rotates on the Bloch circle, which takes the direction of $-y$ as the line of sight.
[2] To better explain the geometric significance of quantum rotation, we denote $s\theta_n$ as θ and set $\theta > 0$ in this table.

2.1 Properties of two-dimensional quantum rotation

A binary quantum state $|\psi_s(\theta_n)\rangle$ on the *xoz* Bloch plane can be expressed as follows:

$$\left|\psi_s(\theta_n)\right\rangle \equiv R(s\theta_n)|0\rangle = \cos\left(\frac{s\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s\theta_n}{2}\right)|1\rangle, \tag{1}$$

where, $n \in \mathbb{N}, s \in \mathbb{Z}_n := \{0, 1, 2, \ldots, n-1 | n \in \mathbb{N}\}, \theta_n = \frac{\pi}{2^{n-1}}$. On a quantum circuit, a quantum rotation $R(s\theta_n)$ can regarded as a quantum gate with control parameter $s\theta_n$. n and s are set to limit the control parameters to $[0, \frac{\pi}{2}]$ to avoid ambiguities caused by angles that differ by one phase. Geometrically, $R(s\theta_n)$ causes the quantum state to rotate $s\theta_n$ around the y-axis start $|0\rangle$ on the *xoz* plane in Bloch ball.

Superposition is about the important nature of the control parameters and is the basis of the series protocol. For any $\alpha\theta_n$ and $\beta\theta_n$,

$$R(\alpha\theta_n)R(\beta\theta_n)|0\rangle = R(\alpha\theta_n + \beta\theta_n)|0\rangle. \tag{2}$$

Superposition can be intuitively expressed as multiple control parameters of the quantum rotations can be superimposed. This is a property similar to homomorphic encryption. The detailed proof of superposition is shown in Ref [9]. Superposition in the *two*-dimensional can be proved by using the quantum gate and the trigonometric function property.

The superposition of quantum rotation has two important corollaries as follows:

$$R(\alpha\theta_n)R(\beta\theta_n)|0\rangle = R(\beta\theta_n)R(\alpha\theta_n)|0\rangle, \tag{3}$$

$$R(\alpha\theta_n)^{\dagger} = R(\alpha\theta_n)^{-1} = R(-\alpha\theta_n). \tag{4}$$

By combining the geometric meaning of quantum rotation, it can be concluded that the positive or negative of the parameter affects the direction rotation of the vector state on the Bloch sphere. Tables 1 presents the geometric significance of quantum rotation. Together with the two important corollaries that were above-mentioned, it provides the basic tools for application protocols design.

The process of constructing quantum states by using *two*-dimensional quantum rotation is similar to the transformation between a plane rectangular coordinate system, and a polar coordinate system. Referring to this relationship, the conversion factor between the spherical coordinate and the spatial rectangular coordinate systems can be introduced to construct *three*-dimensional quantum rotation. by taking the three conversion factors $\{\overline{x}_1, \overline{x}_2, \overline{x}_3\}$ as the coefficients in front of the *three*-dimensional standard orthogonal basis

in natural number order, the following expression for *three*-dimensional quantum rotation can be obtained:

$$\begin{aligned}\left|\psi_{s_1,s_2}(\theta_n)\right\rangle &= R(s_1\theta_n, s_2\theta_n)_{(\Omega)}|0\rangle \\ &= \overline{x}_1|0\rangle + \overline{x}_2|1\rangle + \overline{x}_3|2\rangle \\ &= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle \\ &\quad + \sin\left(\frac{s_1\theta_n}{2}\right)\sin\left(\frac{s_2\theta_n}{2}\right)|2\rangle,\end{aligned} \tag{5}$$

where, the subscript Ω of $R(s_1\theta_n, s_2\theta_n)_{(\Omega)}$ represents the Hilbert space where $|0\rangle, |1\rangle, |2\rangle$ is located. The Equation (5) can be varied as follows:

$$\begin{aligned}&R(s_1\theta_n, s_2\theta_n)_{(\Omega)}|0\rangle \\ &= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\sin\left(\frac{s_2\theta_n}{2}\right)|2\rangle \\ &= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\left\{\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle + \sin\left(\frac{s_2\theta_n}{2}\right)|2\rangle\right\} \\ &= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)R(s_2\theta_n)_{(\omega_{12})}|1\rangle \\ &= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)|\xi\rangle \\ &= R(s_1\theta_n)_{(\omega_{0\xi})}|0\rangle.\end{aligned} \tag{6}$$

The proof of superposition in the *three*-dimensional requires the introduction of auxiliary quantum rotation. $R(s_2\theta_n)_{(\omega_{12})}$ denotes a quantum rotation that occurs in Hilbert plane ω_{12} determined by $|1\rangle$ and $|2\rangle$. Geometrically, plane ω_{12} is orthogonal to $|0\rangle$. Then, as a vector on plane ω_{12}, $R(s_2\theta_n)_{(\omega_{12})}|1\rangle$ was also orthogonal to $|0\rangle$. For the sake of formal simplicity, $R(s_2\theta_n)_{(\omega_{12})}|1\rangle$ was noted as $|\xi\rangle$. It can be found that the rewritten equation fits the definition of a quantum rotation that occurs in Hilbert plane $\omega_{0\xi}$ determined by $|0\rangle$ and $|\xi\rangle$. Thus, it can be concluded that *three*-dimensional quantum rotation also satisfies superposition.

From the point of view of quantum circuits, a *three*-dimensional quantum rotation can be viewed as two times *two*-dimensional quantum rotations in different Hilbert plane. This idea provides valuable insights for expanding quantum rotation to N-dimensional.

2.2 *N*-dimensional quantum rotation

In this section, the quantum rotation was extended to N-dimensions and the construction method was summarized.

The coordinate conversion factors of the N-dimensional Cartesian coordinate system and the hyper-spherical coordinate system can be introduced to construct N-dimensional quantum rotation [30]. The conversion factor [31] between the two coordinate systems

can be defined as follows:

$$\begin{aligned} x_1 &= r\cos(\phi_1), \\ x_2 &= r\sin(\phi_1)\cos(\phi_2), \\ &\dots \\ x_{N-1} &= r\sin(\phi_1)\dots\sin(\phi_{N-2})\cos(\phi_{N-1}), \\ x_N &= r\sin(\phi_1)\dots\sin(\phi_{N-2})\sin(\phi_{N-1}), \end{aligned} \tag{7}$$

where, $\{\phi_1, \phi_2, \dots, \phi_{N-1}\}$ represents the angle of rotation from the corresponding coordinate axis. Let $r = 1, \phi_i = \frac{s_i\theta_n}{2}$, the factors can be expressed as follows:

$$\begin{aligned} \overline{x}_1 &= \cos\left(\frac{s_1\theta_n}{2}\right), \\ \overline{x}_2 &= \sin\left(\frac{s_1\theta_n}{2}\right)\cos\left(\frac{s_2\theta_n}{2}\right), \\ &\dots \\ \overline{x}_{N-1} &= \sin\left(\frac{s_1\theta_n}{2}\right)\cdot\sin\left(\frac{s_{n-2}\theta_n}{2}\right)\cos\left(\frac{s_{n-1}\theta_n}{2}\right), \\ \overline{x}_N &= \sin\left(\frac{s_1\theta_n}{2}\right)\cdot\sin\left(\frac{s_{n-2}\theta_n}{2}\right)\sin\left(\frac{s_{n-1}\theta_n}{2}\right), \end{aligned} \tag{8}$$

Obviously, $\sum_{i=1}^{N}(\overline{x}_i)^2 = 1$.

Taking $\{\phi_1, \phi_2, \dots, \phi_{N-1}\}$ as the coefficient before $N-1$ standard orthogonal bases in natural number order, then the following expression can be derived:

$$\begin{aligned} \left|\psi_{s_1,s_2,\dots,s_{N-1}}(\theta_n)\right\rangle &= R(s_1\theta_n, s_2\theta_n, \dots, s_{N-1}\theta_n)|0\rangle \\ &= \overline{x}_1|0\rangle + \overline{x}_2|1\rangle + \cdots + \overline{x}_{N-1}|N-2\rangle + \overline{x}_N|N-1\rangle \\ &= \sum_{i=0}^{N-1}\overline{x}_{i+1}|i\rangle. \end{aligned} \tag{9}$$

With reference to the situation in *three*-dimensional, the superposition of N-dimensional quantum rotation can be proved.

Similar to Equation (6), Equation (9) can be transformed into the following form:

$$\begin{aligned} &R(s_1\theta_n, s_2\theta_n, \dots, s_{N-1}\theta_n)|0\rangle \\ &= x_1|0\rangle + x_2|1\rangle + \cdots + x_{N-1}|N-2\rangle + x_N|N-1\rangle \\ &= \cos\left(\frac{s_1\theta_1}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_1}{2}\right)\cos\left(\frac{s_2\theta_2}{2}\right)|1\rangle + \cdots \\ &\quad + \sin\left(\frac{s_1\theta_1}{2}\right)\dots\sin\left(\frac{s_{n-2}\theta_{n-2}}{2}\right)\cos\left(\frac{s_{n-1}\theta_{n-1}}{2}\right)|N-2\rangle \\ &\quad + \sin\left(\frac{s_1\theta_1}{2}\right)\dots\sin\left(\frac{s_{n-2}\theta_{n-2}}{2}\right)\sin\left(\frac{s_{n-1}\theta_{n-1}}{2}\right)|N-1\rangle \end{aligned} \tag{10}$$

$$= \cos\left(\frac{s_1\theta_1}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_1}{2}\right)\left\{\cos\left(\frac{s_2\theta_2}{2}\right)|1\rangle + \cdots + \sin\left(\frac{s_{n-2}\theta_{n-2}}{2}\right)\left\{\cos\left(\frac{s_{n-1}\theta_{n-1}}{2}\right)|N-2\rangle + \sin\left(\frac{s_{n-1}\theta_{n-1}}{2}\right)|N-1\rangle\right\}\right\}\ldots\Big\}\Big\},$$

where $\{|0\rangle, |1\rangle, \ldots, |N-2\rangle, |N-1\rangle\}$ is a set of standard orthogonal bases, and all quantum states are orthogonal to each other. Thus, the above-mentioned equations can be converted step by step into a series of quantum rotations starting from $\cos(\frac{s_{n-1}\theta_{n-1}}{2})|N-2\rangle + \sin(\frac{s_{n-1}\theta_{n-1}}{2})|N-1\rangle$.

Note that the quantum rotation results with s_i as $|\xi_{s_i}\rangle$, namely

$$|\xi_{s_i}\rangle = R(s_i\theta_n)|a\rangle = \cos\left(\frac{s_i\theta_n}{2}\right)|a\rangle + \sin\left(\frac{s_i\theta_n}{2}\right)|b\rangle, \tag{11}$$

where $|a\rangle$ orthogonal to $|b\rangle$.

As a result, Equation (10) can be expressed as follows:

$$\begin{aligned}
&R(s_1\theta_n, s_2\theta_n, \ldots, s_{(n-1)}\theta_n)|0\rangle \\
&= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\left\{\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle + \cdots \right. \\
&\quad + \sin\left(\frac{s_{n-2}\theta_n}{2}\right)\left\{\cos\left(\frac{s_{n-1}\theta_n}{2}\right)|N-2\rangle \right. \\
&\quad \left.\left. + \sin\left(\frac{s_{n-1}\theta_n}{2}\right)|N-1\rangle\right\}\right\}\ldots\Big\}\Big\} \\
&= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\left\{\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle + \cdots \right. \\
&\quad \left. + \sin\left(\frac{s_{n-2}\theta_n}{2}\right)|\xi_{s_{N-1}}\rangle\right\}\ldots\Big\}\Big\} \\
&\cdots \\
&= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)\left\{\cos\left(\frac{s_2\theta_n}{2}\right)|1\rangle + \sin\left(\frac{s_2\theta_n}{2}\right)|\xi_{s_{N-1,N-2,\ldots,3}}\rangle\right\} \\
&= \cos\left(\frac{s_1\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_1\theta_n}{2}\right)|\xi_{s_{N-1,N-2,\ldots,3,2}}\rangle
\end{aligned} \tag{12}$$

Obviously, $|0\rangle$ is orthogonal to $|\xi_{s_{N-1,N-2,\ldots,3,2}}\rangle$. N-dimensional quantum rotation is equivalent to a quantum rotation, where the control parameter is also determined by $\{s_{N-1}, s_{N-2}, \ldots, s_3, s_2\}$. In other words, the impact N-dimensional quantum rotation acting on $|0\rangle$ is equivalent to the impact of $N-1$ *two*-dimensional quantum rotations acting on $|0\rangle$ successively in proper order. Therefore, the N-dimensional quantum rotation also satisfies the superposition.

This proof process can be seen as a method of dimensionality reduction. High-dimensional quantum rotation can play an important role in the design of quantum circuits and mixed-value quantum computing. In addition, it is feasible to design quantum cryptography protocols with higher security and higher efficiency using quantum rotation.

3 Quantum identity authentication protocol based on quantum rotation

As was explained in the Introduction, a common way to construct QIA is to transform other protocols for authentication. Quantum public key cryptography (QPKC), as a class of protocols with more research, focuses on high security and efficiency in encryption and decryption [32]. These features of QPKC meet both the security needs of QIA and the resource savings that QIA should have as a minor protocol. By combining our research on quantum rotation and the main idea of QPKC, the QIA protocol was formally presented based on quantum rotation in this section.

The main difference between QPKC and QIA is that the former requires accurate ciphertext, while the latter only needs to verify that the ciphertext meets expectations. Following this idea, the QIA protocol was constructed to detect whether an encrypted quantum state meets expectations after a series of quantum rotations act on it.

The detailed steps of QIA are shown in the following.

Public parameter. Authenticating party Bob and authenticated party Alice share authentic n-bit strings k_{ide} as Bob's identification code for authentication in the communication network. k_{ide} was chosen independently from $\mathbb{Z}_n$ and distributed as evenly as possible. Note i-th position as k_{ide}^i. k_{ide} and n are private, and one-to-one correspondence is required between the users in the multiuser network.

Step 1. Bob initiates an authentication request for Alice. Bob prepares a string l that is n long, and notes i-th position as $l_i \in \{0,1\}$. Bob prepares k_b based on Alice's k_{ide}^i, and note the i-th position as k_b^i satisfied

$$k_b^i = \begin{cases} 2^{n-1} - k_{\text{ide}}^i, & l_i = 1, \\ -k_{\text{ide}}^i, & l_i = 0. \end{cases} \tag{13}$$

Step 2. Bob prepares an authentication application k_{app} with the corresponding check code k_{ver}. k_{app}^i and k_{ver}^i in i-th satisfy the following conditions

$$k_b^i = k_{\text{app}}^i + k_{\text{ver}}^i, \qquad \left|k_{\text{app}}^i\right| \in \mathbb{Z}_n, \qquad \left|k_{\text{ver}}^i\right| \in \mathbb{Z}_n. \tag{14}$$

The following quantum states were prepared from $|0\rangle^{\otimes n}$ by using quantum rotation as follows:

$$\left|\Psi_{\text{app}}(\theta_n)\right\rangle = \bigotimes_{i=1}^{n} R\left(k_{\text{app}}^i \theta_n\right)|0\rangle. \tag{15}$$

Bob sends $|\Psi_{\text{app}}(\theta_n)\rangle$ to Alice as an authentication request.

Step 3. Alice responded to the request. Alice receives the quantum state and acts $R(k_{\text{ide}}^i \theta_n)$ on the i-th position, obtain

$$\begin{aligned} \left|\Psi_{\text{ide}}(\theta_n)\right\rangle &= \bigotimes_{i=1}^{n} R\left(k_{\text{ide}}^i \theta_n\right)\left|\Psi_{\text{app}}(\theta_n)\right\rangle_{(i)} \\ &= \bigotimes_{i=1}^{n} R\left(k_{\text{ide}}^i \theta_n\right) R\left(k_{\text{app}}^i \theta_n\right)|0\rangle. \end{aligned} \tag{16}$$

and sends $|\Psi_{\text{ide}}(\theta_n)\rangle$ back to Bob as a reply.

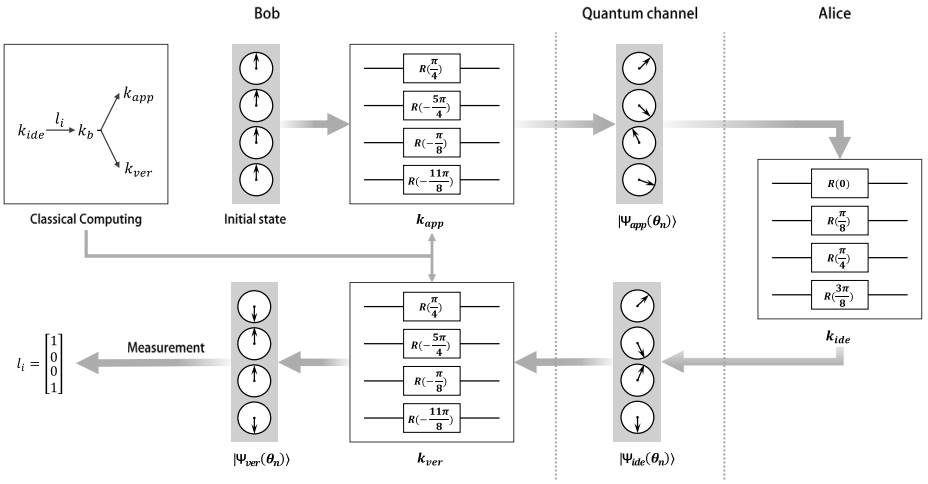

Figure 1 Flowchart of the QIA protocol combining the examples in Table 2. In the flowchart, the quantum state is represented as a vector in the *xoz*, and the quantum rotation is denoted as a quantum variational circuit. Inputting a quantum state into the circuit means that a quantum rotation is applied to a quantum state. The parameters in the three quantum variational circuits are determined by k_{app}, k_{ide} and k_{ver} according to the quantum rotation expressions

Step 4. Bob checks for a reply. Bob acts $R(k^i_{\mathrm{ide}}\theta_n)$ on the i-th position gives $|\Psi_{\mathrm{ver}}(\theta_n)\rangle$ and measure bit by bit using $\{|0\rangle, |1\rangle\}$. If Bob gets the corresponding measurement result $|l_i\rangle$, the authentication results in success. In practical cases, this judging condition could be loosened to an acceptable error threshold according to the channel noise environment. Otherwise, authentication fails.

According to the superposition of quantum rotation, the correctness of the QIA protocol is presented as follows. The protocol is a bit-based deterministic protocol and qubits are discrete and independent. For this reason, j-th position was selected for analysis. Following the protocol steps, the j-th quantum $|\Psi_{\mathrm{ver}}(\theta_n)\rangle_{(j)}$ before Bob makes the measurement is as follows:

$$\begin{aligned}
\left|\Psi_{\mathrm{ver}}(\theta_n)\right\rangle_{(j)} &= R\left(k^j_{\mathrm{ver}}\theta_n\right)R\left(k^j_{\mathrm{ide}}\theta_n\right)R\left(k^j_{\mathrm{app}}\theta_n\right)|0\rangle \\
&= R\left[\left(k^j_{\mathrm{ver}} + k^j_{\mathrm{ide}} + k^j_{\mathrm{app}}\right)\theta_n\right]|0\rangle \\
&= R\left[\left(k^j_{\mathrm{ide}} + k^j_{b}\right)\theta_n\right]|0\rangle \\
&= \begin{cases} R(2^{n-1}\theta_n)|0\rangle = \sin(\frac{\pi}{2})|1\rangle = |1\rangle, & l_i = 1, \\ R(0)|0\rangle = \cos(0)|1\rangle = |0\rangle, & l_i = 0. \end{cases}
\end{aligned} \tag{17}$$

Obviously, the final output of the protocol is $|l_i\rangle$, which can show Alice's identity whether to meets expectations. Figure 1 and Table 2 depict the protocol process when the authentication credential $n = 4$, $k_{\mathrm{ide}} = \{0, 1, 2, 3\}$.

Special attention should be also paid to the fact that the authentication credentials k_{ide} of the different users in a communication network cannot be multiplicative, such as $\{1, 1, 2, 2\}$ and $\{2, 2, 4, 4\}$. This has the potential to cause two users to exhibit exactly the same behavior during a authentication process. Obviously, this situation can be easily avoided when distributing k_{ide} for users.

Table 2 QIA protocol example when $n = 4$

Initial state	k_{ide}	l_i	k_b	k_{app}	k_{ver}	$\|\Psi_{\text{app}}(\theta_n)\rangle$	$\|\Psi_{\text{ide}}(\theta_n)\rangle$	$\|\Psi_{\text{ver}}(\theta_n)\rangle$	Results
$\|0\rangle$	0	1	8	2	6	$R(\frac{\pi}{4})\|0\rangle$	$R(\frac{\pi}{4})\|0\rangle$	$R(\pi)\|0\rangle$	$\|1\rangle$
$\|0\rangle$	1	0	−1	−10	9	$R(-\frac{5\pi}{4})\|0\rangle$	$R(-\frac{9\pi}{8})\|0\rangle$	$R(0)\|0\rangle$	$\|0\rangle$
$\|0\rangle$	2	0	−2	−1	−1	$R(-\frac{\pi}{8})\|0\rangle$	$R(\frac{\pi}{8})\|0\rangle$	$R(0)\|0\rangle$	$\|0\rangle$
$\|0\rangle$	3	1	5	−11	16	$R(-\frac{11\pi}{8})\|0\rangle$	$R(-\pi)\|0\rangle$	$R(\pi)\|0\rangle$	$\|1\rangle$

4 Analysis and discussion

In this section, the protocol and future development will be thoroughly analyzed.

4.1 Security analysis

The security of the proposed QIA protocol will be examined. The purpose of the external attacker, Eve, is to try to fake Alice's identity and make Bob believe that she is Alice. Furthermore, Eve attempts to obtain Alice's authentication code and disguise her identity for a long time. The resistance of the protocol to impersonation attacks, known plaintext attacks, measure-resend attacks, and entangle-discriminate attacks will be also investigated.

(1) Impersonation attack. In this kind of attack, Eve tries to impersonate the legal user Alice and pass the authentication process. A general approach to impersonation is to measure the unknown quantum states on the channel and attempt to distinguish quantum states. The density matrix and the Heisenberg uncertainty principle were used to calculate the trace distance to distinguish the two quantum states on the channel to see if they can be distinguished.

For the simplicity of the calculation, the case when a single quantum state is transmitted over a quantum channel was considered. The control parameter of the quantum rotation that determines the state of the quantum state, assume as ξ, leads to the quantum state as $|\psi(\xi)\rangle = R(\xi)|0\rangle$. Then, its density matrix can be expressed as follows:

$$\begin{aligned}
\big|\psi(\xi)\big\rangle\big\langle\psi(\xi)\big| &= \left[\cos\left(\frac{\xi}{2}\right)|0\rangle + \sin\left(\frac{\xi}{2}\right)|1\rangle\right]\left[\cos\left(\frac{\xi}{2}\right)\langle 0| + \sin\left(\frac{\xi}{2}\right)\langle 1|\right] \\
&= \cos^2\left(\frac{\xi}{2}\right)|0\rangle\langle 0| + \cos\left(\frac{\xi}{2}\right)\sin\left(\frac{\xi}{2}\right)|0\rangle\langle 1| \\
&\quad + \cos\left(\frac{\xi}{2}\right)\sin\left(\frac{\xi}{2}\right)|1\rangle\langle 0| + \sin^2\left(\frac{\xi}{2}\right)|1\rangle\langle 0| \\
&= \begin{pmatrix} \cos^2(\frac{\xi}{2}) & \cos(\frac{\xi}{2})\sin(\frac{\xi}{2}) \\ \cos(\frac{\xi}{2})\sin(\frac{\xi}{2}) & \sin^2(\frac{\xi}{2}) \end{pmatrix}.
\end{aligned} \tag{18}$$

It was also assumed that the two quantum states on the channel are determined by the parameters ξ_1 and ξ_2, respectively. According to the theorems of quantum state discrimination [33], the minimum error of discriminating the two states above is given by the following equation:

$$\begin{aligned}
P_{\text{err}} &= \frac{1}{2}\left(1 - \text{Tr}\left(\left|\frac{1}{2}\rho_{\xi 2} - \frac{1}{2}\rho_{\xi 1}\right|\right)\right) \\
&= \frac{1}{2}(1-0) = \frac{1}{2}.
\end{aligned} \tag{19}$$

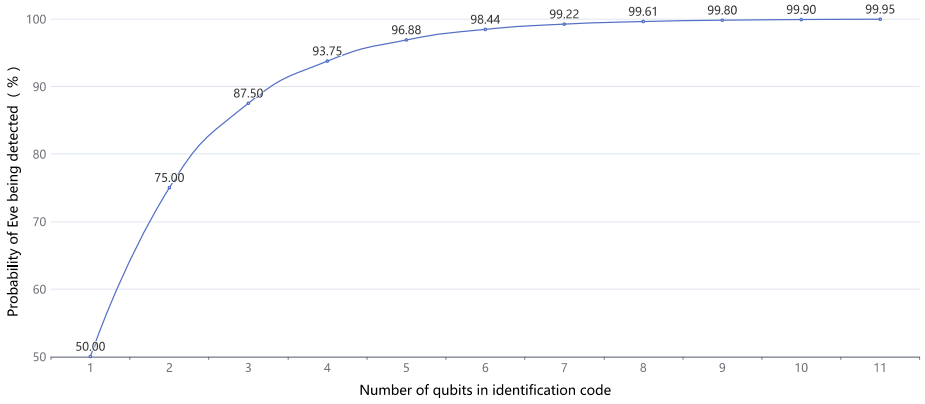

Figure 2 The probability of Eve's impersonation being detected varies with n. The x-axis stands for the number of bits of the authentication code k_{ide}, namely n. The y-axis represents the probability of Eve's impersonation attack being detected. It should be noted that the protocol does not work when $n = 1$. However, for a complete demonstration of the trend of the probability of Eve being found, this figure retains this case

Therefore, when the code have n bits, the probability of an adversary passing Alice's test is at most

$$(1 - P_{\text{err}})^n = \frac{1}{2^n}. \tag{20}$$

Compared to some QIA protocols [34] based on the mutually unbiased bases (MUBs), Eve's probability of passing detection has an extremely fast rate of decline. As can be observed from Fig. 2, the probability of Eve's impersonation being detected increases exponentially with the number of bits of the authentication code n.

When $n = 10$, the probability of Eve being found is greater than 99.9%. This is a very good performance, which comes from the incorporation of quantum rotation into the protocol design. Another comparative advantage of introducing quantum rotation, in terms of security, is that the performance of security protection for authentication code is greatly improved. When the authentication code is long enough, the key can be selected in a very wide space, namely $\mathbb{Z}_n$, and the probability that Eve obtains the authentication credentials by random selection is $\frac{1}{n^n}$, which is about 0.002% when $n = 6$. This security protection is also reflected in the defense against other attacks.

(2) Forward search attack. In the above-mentioned attack, Eve wanted to disguise her identity to pass Bob's test. In the next series of attacks, Eve will try to steal as much information as possible about the authentication code. A forward search attack is known to be a very effective way of attacking QPKC and derived protocols. Particularly, the basic idea of the attack is to use a two-bit quantum gate, such symmetry-test circuit, to compare the state of the quantum state before and after encryption to infer the ciphertext [6]. For the proposed QIA protocol, Eva can compare the authentication request received by Alice and the authentication reply sent by Alice to infer the authentication code.

Previously reported works in the literature have shown that using parity encoding with Hamming weight [6] or using probabilistic encryption [7] can prevent forward search attacks. However, the former brings a reduction in protocol efficiency, and the latter is associated with probabilistic decryption errors. In our previously reported work [9], it has

been shown that using *three*-dimensional quantum rotation can have good resistance to forward search attack without adding any plug-ins. Similarly, our QIA protocol is resistant to such types of attacks. On the one hand, the ciphertext of our protocol, namely the authentication code, is the quantum rotation parameter rather than $\{|0\rangle, |1\rangle\}$. Even if there exists a quantum circuit that can accurately compare whether two quantum states are different, it is not possible to infer the authentication code. On the other hand, there do exist some cases, such as $k_{\text{ide}} = 0$ and $k_{\text{app}} = 0$, forward search attacks are able to infer k_{ide}. Nevertheless, such cases obviously occur with very low probability and do not affect the overall security of our protocol. For Eve, since k_{app} was independently selected by Alice, she was also unable to confirm $k_{\text{app}} = 0$. In summary, the developed protocol has good resistance to forward search attacks. A large part of the security of the protocol comes from the random and decentralized selection of k_{app} and l_i. The selection process should be independent in each authentication.

(3) Measure-resend attack. In this attack strategy, Eve will use carefully designed POVM to measure the quantum state on the quantum channel, and send new states to Bob depending upon the measurement result. Without loss of generality, it was assumed that Eve performs a measure-resend attack on Alice's reply to Bob. Regardless of how Eve designs the measurement base to obtain more information, the maximum amount of information Eve can extract from the quantum channel can be calculated by using Holevo bound [35].

The maximum amount of information that can be obtained from the quantum channel satisfies the following inequality

$$S(\rho) - \sum_x p_x S(\rho_x) \leq H(X), \tag{21}$$

where, $\rho = \sum_x p_x \rho_x$.

In the proposed protocol, both k_{ide} and k_{app} were selected at complete random on $\mathbb{Z}_n$. Then the quantum state on the channel with a $\frac{1}{n}$ probability is in

$$R(i\theta_n)|0\rangle = R\left(\frac{i\pi}{2^{n-1}}\right)|0\rangle = \cos\left(\frac{i\pi}{2^n}\right)|0\rangle + \sin\left(\frac{i\pi}{2^n}\right)|1\rangle, \tag{22}$$

where, $i \in \mathbb{Z}_n$. Then the density matrix of quantum states is

$$\begin{pmatrix} \cos^2(\frac{i\pi}{2^n}) & \cos(\frac{i\pi}{2^n})\sin(\frac{i\pi}{2^n}) \\ \cos(\frac{i\pi}{2^n})\sin(\frac{i\pi}{2^n}) & \sin^2(\frac{i\pi}{2^n}) \end{pmatrix}. \tag{23}$$

In summary, it can be obtained:

$$\rho = \sum_{i=1}^{n} \frac{1}{n} \begin{pmatrix} \cos^2(\frac{i\pi}{2^n}) & \cos(\frac{i\pi}{2^n})\sin(\frac{i\pi}{2^n}) \\ \cos(\frac{i\pi}{2^n})\sin(\frac{i\pi}{2^n}) & \sin^2(\frac{i\pi}{2^n}) \end{pmatrix}. \tag{24}$$

A simple calculation leads to the eigenvalues of ρ, which is a function of n. From this, relationship between Holevo bound for the quantum state on the channel and n can be derived as Fig. 3.

During the increase in n, the amount of information available to Eve decreased rapidly and fell below 0.000311 bit at n greater than 10. In the protocol setting, $n \gg 1$ should be satisfied. Therefore, the protocol has good resistance to measure-resend attacks.

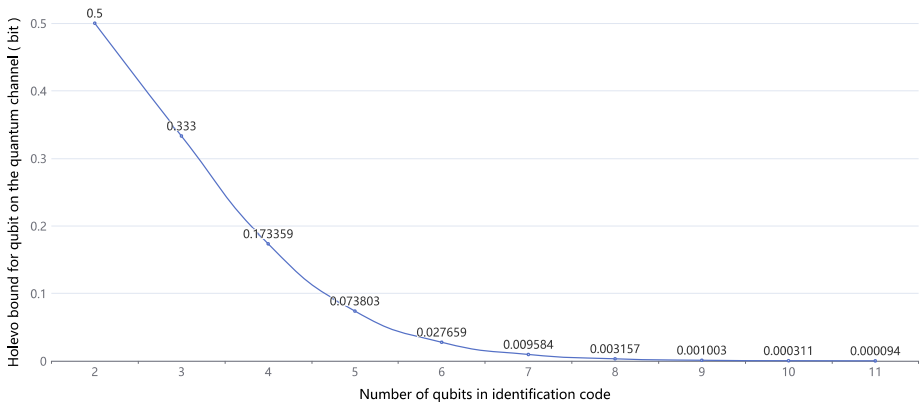

Figure 3 The Holevo bound varies with n. The x-axis stands for n. The y-axis denotes Holevo bound for the quantum state on the channel. The protocol does not work when $n = 1$, therefore in the figure $n \geq 2$

It is worth noting that when $n = 2$, the protocol uses on the channel only $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. At this point, the protocol degenerates to a BB84-like protocol. From the perspective of protocol design, the developed QIA protocol can be seen as a generalization of the BB84-based QIA protocol. From the perspective of the quantum gates used, H used in the BB84 protocol equals to $R(\frac{\pi}{2})$. Quantum rotation, and a set of universal quantum gates were used in our protocol, which greatly extends the flexibility of the protocol when encrypting and decrypting.

Additionally, a special feature of this protocol is that, as a quantum bit-oriented protocol, each bit of quantum state is phase independent (this is supported by the analysis of the impersonation attack). However, its security will change as the number of quantum bits increases. This stems from the association of the quantum rotation parameter with the authentication code in the protocol design. Combined with the analysis of the impersonation attack, as the number of bits is increased, spoofing becomes more difficult, and stealing useful information from the channel becomes more difficult, which increases the security of the protocol in general. When n is large enough, the probability of success of Eve's measure-resend attack will be lower than the probability of directly guessing the authentication code.

(4) Entangle-discriminate attack. In this attack, Eve entangles the quantum state on the channel with her own probe register. After, Bob has executed the authentication protocol, the probe is measured and potentially useful information is obtained. On this basis, Eve can draw information on the state of the quantum in the quantum channel [36].

A brief demonstration of the flow of Eva's attack using $\overline{CNOT}$ is presented here. Eve uses $\overline{CNOT}$ to establish entanglement between $|\psi\rangle = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$ on the channel and preserved quantum state $|\chi\rangle$. The state of the quantum system after establishing entanglement is as follows:

$$|\psi\rangle|\chi\rangle \xrightarrow{\overline{CNOT}} \cos(\theta)|\psi\rangle|\chi\rangle + \sin(\theta)\overline{X}|\psi\rangle|\chi\rangle, \tag{25}$$

where, $\overline{X} = |1\rangle\langle 0| + |0\rangle\langle 1|$. Afterwards, Eve measures the probe register based on her knowledge of $|\chi\rangle$ and infers θ based on the probability of the measurement result. Eve can infer the quantum state structure step by step by repeating this attack many times.

This attack is very effective against QIA protocols where the authentication code does not change, especially BB84-like protocols that use MUBs. In addition to that, this attack also works for QKD and quantum secret sharing. Moreover, the entangle-discriminate attack can also be combined with a forward search attack based on symmetry-test quantum circuits [6] to produce a higher attack effect.

However, such types of attacks are of little use to our QIA protocols. In this attack scenario, the first difficulty Eve faces come from the final stage of the protocol: Bob will apply k_{ver} before measuring. k_{ver} can have an unintended impact on the established entanglement. Thus, the possible structure of the channel quantum states directly from the measurements can difficult to be inferred.

In the most ideal case, Eve can get $k_{\text{app}} + k_{\text{ide}}$ in an authentication. Eve can fall back on the second best attempt to use $k_{\text{app}} + k_{\text{ide}}$ to cheat Bob. Then, Eve will face a second difficulty. k_{app} and l_i used by Bob in each authentication process are randomly assigned and both are selected independently. The random process makes $k_{\text{app}} + k_{\text{ide}}$ change in each communication, and the number of possible changes is linearly related to n. It is difficult for Eve to cheat Bob in the next authentication. This result approximates the influence of key updating, namely, making it difficult for an attacker to accumulate an advantage in each attack. In a practical scenario, a key-update threshold can be set for the developed protocol to further strengthen the security of the authentication code. Compared to protocols that actually use a key-update policy, the proposed protocol is more convenient. Because the authentication code of Alice in the protocol is practically unchanged, no additional quantum operations are required, and Alice can secure the protocol by simply executing an identical circuit. In reality, Eve needs to trade off the amount of information available and the induced error rate resulting from different entanglement strategies and detection state discrimination techniques. Eve may causes a disturbance to the channel in the establishment of entanglement, which can be detected in the final measurement detection in combination with l_i.

4.2 Efficiency analysis

Afterwards, the efficiency performance of our protocol will be analyzed and some existing protocols will be compared. Quantum bit efficiency [37] is considered one of the most commonly used criteria to analyze the efficiency of quantum protocols. The quantum bit efficiency is given by the following expression:

$$\eta = \frac{b_s}{q_t + b_t} \times 100\%, \tag{26}$$

where b_s represents the number of useful quantum bits and classical bits, q_t denotes the total number of quantum bits, b_t stands for the total number of quantum bits.

In the proposed protocol, the length of the authentication code is n. The length of the classical l_i used for listening detection is n, namely $b_t = n$. Besides, the total number of quantum bits used is $q_t = n$, and the protocol finally authenticates the $q_t = n$ bit authentication code. Therefore, the lower bound of quantum bit efficiency for our protocol is calculated as follows:

$$\eta_0 = \frac{n}{n + n} \times 100\% = 50\%. \tag{27}$$

Table 3 Comparison of protocol performance

Protocol	Realization method[1]	Length of identification code	Quantum bit efficiency (%)[2]	Note[3]
[38]	Bell states	n	15	two-way certification
[39]	Bell states	$2n$	33.3	key-update
[40]	Bell states	$6n$	33.3	two-way certification
[41]	Bell states	$2n$	≤ 88.9	two-way certification
[42]	Cluster state	n	16.7	two-way certification
[43]	Cluster state	$4n$	33.3	–
[44]	QKD with Mubs	n	33.3	–
[45]	QKD with Mubs	n	50	–
[46]	QKD with Mubs	n	50	key-update
[47]	QKD with Mubs	$9n$	≥ 45	key-update
[48]	QKD with Bell state	$2n$	50	two-way certification
[49]	Error avoidance code	n	25	–
[21]	Shared secret	n	33.3	key-update
[50]	QPKC	n	50	–
[29]	Quantum walks	n	––	two-way certification
Our	Quantum rotation	n	≥ 50	–

[1] Realization method refers to the most significant quantum resources used by the protocol, and some auxiliary resources are not marked.
[2] Quantum bit efficiency stands for the approximate value calculated from the Equation (26) in the ideal state. The quantum bit efficiency of some protocols is variable, and the range is given in this table. Among them, [29] cannot evaluate the quantum bit efficiency due to the use of quantum walks.
[3] Note denotes additional purposes that can be achieved by QIA protocol. Some protocols enable multi-party authentication. In some protocols, only part of the authentication code changes after each authentication or equivalently achieves key-update, which is also marked as achieving key-update.

Although quantum bit efficiency is a more general evaluation criterion, this criterion is inaccurate for the introduced protocol. The vast majority of quantum communication protocols use quantum bits $\{|0\rangle, |1\rangle\}$ and classical bits $\{0, 1\}$. Nonetheless, in the proposed protocol, the object being authenticated is $k_{\text{ide}} \in \mathbb{Z}_n$, carrying more information than the classical bits. For example, the binary of an integer 10, $1010_{(2)}$, requires 4 bits of classical bits for storage, and integer 100 requires 7 classical bits. Thus, fewer classical bits are used here to authenticate content that requires a large number of classical bits for storage. Equation (27) gives the quantum bit efficiency of the protocol when $n = 2$, namely $k_{\text{ide}} \in \{0, 1\}$. As n is increased, the number of useful classical bits $N(n)$ also is increased and $\min N(n) = n$. In summary, the quantum bit efficiency can be expressed as follows:

$$\eta = \frac{N(n)}{2n} \times 100\% \geq 50\%. \tag{28}$$

The precise evaluation of the efficiency of the developed protocols is still a matter of discussion.

A simple comparison with similar QIA protocols in structure and steps from the aspects of realization method, length of identification code, and quantum bit efficiency is presented in Table 3.

Table 3 shows some of the QIA protocols with similar structure and steps, namely, the certified party reproducing information about the certification code to the quantum state for authentication request reply in a round of communication.

By comparison, it can be found that the protocols that achieve two-way authentication basically use quantum entanglement and have good performance in terms of quantum bit efficiency. However, it is clear that protocols that use quantum entanglement, especially many-body entanglement and other special quantum resources, have difficulties in

the physical implementation. As was stated in the Introduction, this is contrary to QIA's positioning as a minor protocol. Most of the QKD-based protocols achieve high quantum bit efficiency, while QKD protocols using MUBs are vulnerable to various types of attacks, such as entangle-discriminate attacks. The proposed protocol strikes a good balance between security and efficiency. More specifically, only quantum rotation is used as a fundamental component of quantum computing and can be directly embedded in security protocols related to quantum computing, such as quantum federation learning [51] or other cloud-based quantum machine learning. In addition, during multiple runs of the proposed protocol, Alice does not need to change its own quantum circuitry frequently to ensure the protocol security, which can reduce the technical requirements of Alice with only limited quantum capabilities in realistic scenarios. These advantages suggest that the developed protocol can be better applied in future quantum big data scenarios.

4.3 Discussion

In this section, some unresolved issues in our QIA protocol will be discussed, and further expansions will be provided. In real scenarios, imperfections in the quantum channel and detection primitives can have a direct impact on the authentication accuracy and security of a QIA protocol. As a bit-oriented QIA protocol, dark counts and channel loss can cause authentication failures or give Eva the opportunity to hide in the noise for attacks. The analysis of security in this work assumes an ideal environment. Hence, the attacker Eva's strategy of faking Alice's identity with the help of noise will be discussed, while Bob's countermeasures will be covered in future work. Several works in the literature [45, 46] have conducted noise analysis for QKD-based QIA and have shown good performance. In further work, we will use quantum simulation tools for analysis of the protocol. Moreover, as was explained in the efficiency analysis, the precise evaluation of the efficiency is an unresolved issue for our protocol. This problem can be extended to evaluate the efficiency of multi-valued or even mixed-valued quantum circuits.

For the future expansion of the protocol, it should be noted that some protocols that do not use entanglement [46, 47] are able to achieve key-updates using quantum gates. The proposed QIA protocol is also capable of working with multiple quantum gates to enable key updates. It can be also simply modified to add more quantum bits and one quantum communication for achieving two-way authentication while avoiding the use of entanglement. In addition, it can be combined with entanglement to extend a more secure multi-party authentication protocol [52].

Fundamental concepts from quantum computing are also applied to the design of quantum cryptography protocols. This shows that quantum circuits and computational tasks in quantum computing, such as universal quantum circuits or blind quantum computing, can be introduced into the design of quantum protocols. Quantum homomorphic encryption (QHE) is a kind of protocol that combines quantum computing with quantum cryptography. The homomorphic nature of quantum rotation and their properties as quantum universal gates seem to be used to design a QHE protocol, which is one of our future research.

In terms of structure, the proposed QIA protocol has similarities with Nikolopoulos's QPKC protocol [5], namely quantum rotation works as a special quantum one-way function. The corresponding quantum rotations can be easily constructed using classical parameters, while it is very difficult to reduce the classical parameters from unknown quantum rotations. This is the source of the ability to be below multiple attacks. Based on this

idea, using the expansion of quantum rotation in dimensionality, high-dimensional QIA protocols can be designed to further increase security. According to the relationship between the high-dimensional quantum rotation and *two*-dimensional quantum rotation, a high-dimensional QIA protocol is equivalent to multiple *two*-dimensional QIA protocols working together, which can further improve security.

In summary, in addition to its good performance, in terms of security and efficiency, our protocol has good expandability.

5 Conclusion

In this work, the geometric properties of quantum rotations were first summarized based on previous work and were expanded on the dimensionality. These property works provide the basis for protocols based on quantum rotation. By combining the QPKC framework with the superposition of quantum rotation, a bit-oriented QIA protocol was proposed. After performing security analysis using the theorems of quantum state discrimination and Holevo bound, it was demonstrated that the proposed protocol has high security and good resistance to multiple attacks. This enhanced security comes from treating quantum rotation as a one-way function. Moreover, as a bit-oriented protocol, each bit of quantum state in the protocol is independent. However, the security of each bit is directly related to the length of the authentication code, which is a special feature of the developed protocol. Authentication code length is regarded as a key factor affecting protocol security. In terms of efficiency, the proposed protocol has good performance and demonstrates advantages in comparison with other protocols. In addition to that, the introduced protocols are well-expandable. The proposed protocol is based on quantum rotation and no additional quantum resources are used, which can be well applied to quantum computing networks and other protocols based on quantum rotation.

Appendix: Symbol definition table

Table A1 Symbol definition table

Symbol[1]	Definition and Description
$\mathbb{N}$	$\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}$	$\{0, 1, 2, \dots, n-1 \mid n \in \mathbb{N}\}$
θ_n	$\frac{\pi}{2^{n-1}} n \in \mathbb{N}$
$R(s\theta_n)$	A quantum rotation, where $s \in \mathbb{Z}_n$
$R(s_1\theta_n, s_2\theta_n)_{(\Omega)}$	Ternary quantum rotation occurring in Hilbert space Ω
$\lvert\xi_{s_i}\rangle$	The quantum rotation results with s_i
n in protocol	Number of bits of authentication code
$k_{\mathbf{ide}}$	String of authentication code
$k_{\mathbf{app}}$	String of authentication application, $\lvert k^i_{\mathbf{app}}\rvert \in \mathbb{Z}_n$
$k_{\mathbf{ver}}$	String of authentication verification, $\lvert k^i_{\mathbf{ver}}\rvert \in \mathbb{Z}_n$
$k^i_{\mathbf{ide}}$	The i-th bit of the string, $k^i_{\mathbf{ide}} \in \mathbb{Z}_n$
l	Auxiliary binary string
l_i	The i-th bit of the auxiliary string, $l_i \in \{0, 1\}$
η	Quantum bit efficiency

[1] Only the main symbols are listed in this table. Some regional symbols are not listed here, please refer to the definitions and descriptions of these symbols before use.

Acknowledgements
We acknowledge the financial supports from the Natural Science Foundation of Fujian Province, China (Grant No. 2020J01812).

Funding
Not applicable. The study has no funding.

Abbreviations
QIA, Quantum Identity Authentication; QKD, Quantum Key Distribution; QPKC, Quantum Public Key Cryptography; MUBs, Mutually Unbiased Bases.

Availability of data and materials
All data generated or analysed during this study are available and included in this published article.

Declarations

Ethics approval and consent to participate
Not applicable. There are no relevant problems in our research.

Consent for publication
We agree to publish our paper by Springer Nature.

Competing interests
The authors declare no competing interests.

Author contributions
Geng Chen and Yuqi Wang wrote the main manuscript text. All authors reviewed the manuscript.

Received: 24 April 2022 Accepted: 19 April 2023 Published online: 25 April 2023

References

1. Nielsen MA, Chuang I. Quantum computation and quantum information. American Association of Physics Teachers; 2002.
2. Ambruş VE, Winstanley E. Rotating quantum states. Phys Lett B. 2014;734:296–301.
3. Cerezo M, Arrasmith A, Babbush R, Benjamin SC, Endo S, Fujii K, McClean JR, Mitarai K, Yuan X, Cincio L et al. Variational quantum algorithms. Nat Rev Phys. 2021;3(9):625–44.
4. Schuld M, Sinayskiy I, Petruccione F. The quest for a quantum neural network. Quantum Inf Process. 2014;13:2567–86.
5. Nikolopoulos GM. Applications of single-qubit rotations in quantum public-key cryptography. Phys Rev A. 2008;77(3):032348.
6. Nikolopoulos GM, Ioannou LM. Deterministic quantum-public-key encryption: forward search attack and randomization. Phys Rev A. 2009;79(4):042327.
7. Seyfarth U, Nikolopoulos G, Alber G. Symmetries and security of a quantum-public-key encryption based on single-qubit rotations. Phys Rev A. 2012;85(2):022342.
8. Shang T, Tang Y, Chen R, Liu J. Full quantum one-way function for quantum cryptography. Quantum Eng. 2020;2(1):32.
9. Wang Y, Chen G, Jian L, Zhou Y, Liu S. Ternary quantum public-key cryptography based on qubit rotation. Quantum Inf Process. 2022;21(6):197.
10. Kis Z, Renzoni F. Qubit rotation by stimulated Raman adiabatic passage. Phys Rev A. 2002;65(3):032318.
11. Nadj-Perge S, Frolov S, Bakkers E, Kouwenhoven LP. Spin–orbit qubit in a semiconductor nanowire. Nature. 2010;468(7327):1084–7.
12. Pirandola S, Andersen UL, Banchi L, Berta M, Bunandar D, Colbeck R, Englund D, Gehring T, Lupo C, Ottaviani C et al. Advances in quantum cryptography. Adv Opt Photonics. 2020;12(4):1012–236.
13. Dutta A, Pathak A. A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice? Quantum Inf Process. 2022;21(11):369.
14. Crépeau C, Salvail L. Quantum oblivious mutual identification. In: Advances in cryptology—EUROCRYPT'95: international conference on the theory and application of cryptographic techniques Saint-malo, France, May 21–25. Proceedings 14. vol. 1995. France: Springer; 1995. p. 133–46.
15. Sobota M, Kapczyński A, Banasik A. Application of quantum cryptography protocols in authentication process. In: Proceedings of the 6th IEEE international conference on intelligent data acquisition and advanced computing systems. vol. 2. New York: IEEE Press; 2011. p. 799–802.
16. Chen Z, Zhou K, Liao Q. Quantum identity authentication scheme of vehicular ad-hoc networks. Int J Theor Phys. 2019;58:40–57.
17. Huang Y, Xu G, Song X. An improved efficient identity-based quantum signature scheme. Quantum Inf Process. 2023;22(1):1–11.
18. Zawadzki P. Quantum identity authentication without entanglement. Quantum Inf Process. 2019;18(1):7.
19. González-Guillén CE, González Vasco MI, Johnson F, Pérez del Pozo ÁL. An attack on Zawadzki's quantum authentication scheme. Entropy. 2021;23(4):389.
20. Curty M, Santos DJ. Quantum authentication of classical messages. Phys Rev A. 2001;64(6):062309.
21. Abulkasim H, Hamad S, Khalifa A, El Bahnasy K. Quantum secret sharing with identity authentication based on bell states. Int J Quantum Inf. 2017;15(04):1750023.

22. He Y-F, Pang Y, Di M. Mutual authentication quantum key agreement protocol based on bell states. Quantum Inf Process. 2022;21(8):290.
23. Chang Y, Xu C, Zhang S, Yan L. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. Chin Sci Bull. 2014;59:2541–6.
24. Ma H, Huang P, Bao W, Zeng G. Continuous-variable quantum identity authentication based on quantum teleportation. Quantum Inf Process. 2016;15:2605–20.
25. Wen X-J, Zhao X-Q, Gong L-H, Zhou N-R. A semi-quantum authentication protocol for message and identity. Laser Phys Lett. 2019;16(7):075206.
26. Xu Y-P, Gao D-Z, Liang X-Q, Xu G-B. Semi-quantum voting protocol. Int J Theor Phys. 2022;61(3):78.
27. Li W, Shi R, Guo Y. Blind quantum signature with blind quantum computation. Int J Theor Phys. 2017;56:1108–15.
28. Gao W, Yang L, Zhang D, Liu X. Quantum identity-based encryption from the learning with errors problem. Cryptography. 2022;6(1):9.
29. Lou X, Wang S, Ren S, Zan H, Xu X. Quantum identity authentication scheme based on quantum walks on graphs with ibm quantum cloud platform. Int J Theor Phys. 2022;61(2):40.
30. Nasir RN, Shaari JS, Mancini S. Mutually unbiased unitary bases of operators on d-dimensional Hilbert space. Int J Quantum Inf. 2020;18(01):1941026.
31. Knirk DL. Approach to the description of atoms using hyperspherical coordinates. J Chem Phys. 1974;60(1):66–80.
32. Tsai C-W, Yang C-W, Lin J, Chang Y-C, Chang R-S. Quantum key distribution networks: challenges and future research issues in security. Appl Sci. 2021;11(9):3767.
33. Barnett SM, Croke S. Quantum state discrimination. Adv Opt Photonics. 2009;1(2):238–78.
34. Liu B, Gao Z, Xiao D, Huang W, Liu X, Xu B. Quantum identity authentication in the orthogonal-state-encoding qkd system. Quantum Inf Process. 2019;18:1–16.
35. Holevo AS. Bounds for the quantity of information transmitted by a quantum communication channel. Probl Pereda Inf. 1973;9(3):3–11.
36. Brandt HE. Quantum-cryptographic entangling probe. Phys Rev A. 2005;71(4):042312.
37. Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett. 2000;85(26):5635.
38. Lin C-Y, Yang C-W, Hwang T. Authenticated quantum dialogue based on bell states. Int J Theor Phys. 2015;54:780–6.
39. Zhang Z, Zeng G, Zhou N, Xiong J. Quantum identity authentication based on ping-pong technique for photons. Phys Lett A. 2006;356(3):199–205.
40. Zhang S, Chen Z-K, Shi R-H, Liang F-Y. A novel quantum identity authentication based on bell states. Int J Theor Phys. 2020;59:236–49.
41. Jiang S, Zhou R-G, Hu W. Semi-quantum mutual identity authentication using bell states. Int J Theor Phys. 2021;60:3353–62.
42. Shen D-S, Ma W-P, Wang L-L. Two-party quantum key agreement with four-qubit cluster states. Quantum Inf Process. 2014;13:2313–24.
43. Zha X, Yuan C, Zhang Y. Generalized criterion for a maximally multi-qubit entangled state. Laser Phys Lett. 2013;10(4):045201.
44. Hong C, Heo J, Jang JG, Kwon D. Quantum identity authentication with single photon. Quantum Inf Process. 2017;16:1–20.
45. Liu B, Gao Z, Xiao D, Huang W, Zhang Z, Xu B. Quantum identity authentication in the counterfactual quantum key distribution protocol. Entropy. 2019;21(5):518.
46. Yuan H, Liu Y-M, Pan G-Z, Zhang G, Zhou J, Zhang Z-J. Quantum identity authentication based on ping-pong technique without entanglements. Quantum Inf Process. 2014;13:2535–49.
47. Zhu H, Wang L, Zhang Y. An efficient quantum identity authentication key agreement protocol without entanglement. Quantum Inf Process. 2020;19:1–14.
48. Yang Y-G, Huang R-C, Zhou Y-H, Shi W-M, Xu G-B, Li D. Multiparty blind quantum computation protocol with deterministic mutual identity authentication. Phys A, Stat Mech Appl. 2023;609:128396.
49. Qu Z, Liu X, Wu S. Quantum identity authentication protocol based on three-photon quantum error avoidance code in edge computing. Trans Emerg Telecommun Technol. 2022;33(6):3945.
50. Zhang X. One-way quantum identity authentication based on public key. Chin Sci Bull. 2009;54(12):2018–21.
51. Yun WJ, Kim JP, Jung S, Park J, Bennis M, Kim J. Slimmable quantum federated learning. ArXiv preprint. arXiv:2207.10221 (2022).
52. Dutta A, Pathak A. Controlled secure direct quantum communication inspired scheme for quantum identity authentication. Quantum Inf Process. 2022;22(1):13.

Publisher's Note