Double-Blind Quantum Identity Authentication Protocol Based on Scalar Product Computation

Sheng Wang[1(✉)], Xiaodong Zhou[1], Bao Feng[2], Zewen Chen[1], and Yan Xia[3]

[1] State Grid Fujian Electric Power Co., Ltd. Information and Communication Branch, Fuzhou 350000, China
496079373@qq.com
[2] Nanjing NARI Information and Communication Technology Co., Nanjing 211100, China
[3] Department of Physics, Fuzhou University, Fuzhou 350116, China

Abstract. Quantum identity authentication (QIA) can theoretically realize the unconditional security of identity information. The current QIA protocols generally assume that the pre-agreed keys are not leaked. However, the keys themselves may be compromised. In this paper, a double-blind quantum identity authentication protocol based on scalar product computation is proposed. In the key generation stage, the scalar product of the two keys is stored in the database of a third-party platform. The two parties calculate the scalar product of their keys using a quantum private query (QPQ) protocol and compare the results with the expected results for authentication. Our protocol allows the two parties to be double-blind, i.e., they do not know each other's key. In this way, even if one party's key is leaked, the other party's key cannot be obtained.

Keywords: Double-blind · Quantum Identity Authentication · Scalar Product

1 Introduction

In modern network communication, it is an extremely important issue for two parties to securely verify the identity of the other party without disclosing their respective identity information to any eavesdroppers. Traditionally, people rely on classical cryptographic techniques for identity authentication. However, quantum computing poses a serious threat to classical cryptography, such as cracking the RSA scheme [1] and accelerating the analysis of symmetric ciphers [2, 3]. Utilizing the inherent properties of quantum communication, such as unconditional security, for identity authentication, i.e., quantum identity authentication (QIA), has become a current hotspot.

Since Crepeau et al. [4] proposed the first QIA scheme using Oblivious Transfer (OT) in 1995, many QIA protocols have emerged. For example, some schemes [5–7] are based on the properties of entangled states. Other schemes [8–11], based on single photons or separable states. Most schemes are based on specific quantum cryptography technologies, such as quantum key distribution [12–13], quantum teleportation [14], quantum secret sharing [15–16], quantum direct communication [17–18], blind quantum computation [19, 20], etc. However, these QIA protocols mainly focus on protecting

Y. Zhang et al. (Eds.): CENet 2023, LNEE 1126, pp. 72–80, 2024.
https://doi.org/10.1007/978-981-99-9243-0_8

identity information during the authentication process, and generally assume that the pre-shared keys are not leaked. However, after the key sharing is completed, it will still be stored in the hardware, which inevitably leads to the possibility of the key itself being stolen in advance.

In this paper, we propose a double-blind quantum identity authentication protocol using the principle of scalar product calculation between bit strings. When generating keys, the scalar product results between the keys are only stored in the database of the third-party platform, and the authentication participants are not aware of it. When authenticating the identity, the authentication participants use the phase-encoded quantum private query protocol [21] for scalar product calculation, and compare it with the expected results known only to third-party platforms to authenticate the identity. The nature of phase-encoded query allows two participants involved in authentication to be unaware of each other's keys, thus achieving double blindness. In this way, even if one party's key is leaked, the other party's key cannot be obtained.

The rest of this paper is arranged as follows. In Sect. 2, we introduce the quantum operations to be used, the scalar product of bit strings, and the phase-encoded quantum query protocol. In Sect. 3, we present our quantum identity authentication protocol. The protocol is analyzed in Sect. 4. The paper is concluded in Sect. 5.

2 Preliminary

2.1 Quantum Operations

The quantum operations we will use are shown here.

- Pauli X gate $X : |a\rangle \rightarrow |a \oplus 1\rangle, a \in \{0, 1\}$;
- Pauli Z gate $Z : |a\rangle \rightarrow (-1)^a |a\rangle, a \in \{0, 1\}$;
- Hadamard gate $H : |0\rangle \rightarrow |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |1\rangle \rightarrow |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$;
- XOR gate $XOR : |a\rangle|b\rangle \rightarrow |a\rangle|a \oplus b\rangle$, where "$\oplus$" means bit-wise XOR. Especially, $\mathbf{0}$ represents a bit string composed of multiple single bits 0;
- Phase-flip gate $F : |a\rangle \rightarrow \begin{cases} |a\rangle, a = \mathbf{0} \\ -|a\rangle, a \neq \mathbf{0} \end{cases}$;

2.2 Scalar Product of Bit Strings

For each two n-bit strings $a = a_1 \| \ldots \| a_n$, $b = b_1 \| \ldots \| b_n$ ("$\|$" means the connection of bits), the scalar product $a \cdot b$ is defined as $a \cdot b = \oplus_{i=1}^{n} a_i b_i$. If $a \neq \mathbf{0}$, $c \in \{0, 1\}$, the probability that $a \cdot b = c$ holds is $\frac{1}{2}$.

2.3 Phase-Encoded Quantum Private Query [21]

Assume that a sever SE has N bits $d(x) \in \{0, 1\}$, numbered as $x = 1, ..., N-1$. A client CL wants to query SE's x-th bit $d(x)$, but does not want SE to learn the query index x. They completed the private query by following the steps below.

Step 1 Denote $n = \lceil \log_2 N \rceil$, $S_x = \{i | x_i \neq 0, i = 1, \ldots, M\}$. Cl prepares an n-qubit particle t initiated as $|\mathbf{0}\rangle$, then performs H gate on the k-th qubit t_k, where $k \in S_x$ is the least element of S_x. Now $\forall j \in S_x, j \neq k$, Cl applies *XOR* gate on t_k and t_j:

$$XOR : \frac{|0\rangle_{t_k} + |1\rangle_{t_k}}{\sqrt{2}} \otimes_{j \in S_x, j \neq k} |0\rangle_{t_j} \rightarrow \frac{|0\rangle_{t_k} \otimes_{j \in S_x, j \neq k} |0\rangle_{t_j} + |1\rangle_{t_k} \otimes_{j \in S_x, j \neq k} |1\rangle_{t_j}}{\sqrt{2}}, \quad (1)$$

to prepare a superposition state $|x_+\rangle_t = \frac{|\mathbf{0}\rangle_t + |x\rangle_t}{\sqrt{2}}$.

Step 2 Cl now sends his particle t to SE via a verified quantum channel. After receiving it, SE performs an Oracle operator on t:

$$U : |a\rangle \rightarrow \begin{cases} |a\rangle, a = \mathbf{0} \\ (-1)^{d(a)}|a\rangle, a \neq \mathbf{0} \end{cases}, \quad (2)$$

$$U : \frac{|\mathbf{0}\rangle_t + |x\rangle_t}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_t + (-1)^{d(x)}|x\rangle_t}{\sqrt{2}}. \quad (3)$$

Now SE sends t to Cl.

Step 3 $\forall j \in S_x, j \neq k$, Cl applies *XOR* gate again:

$$XOR : \frac{|\mathbf{0}\rangle_t + (-1)^{d(x)}|x\rangle_t}{\sqrt{2}} \rightarrow \frac{|0\rangle_{t_k} + (-1)^{d(x)}|1\rangle_{t_k}}{\sqrt{2}} \otimes_{i \neq k} |0\rangle_{t_i}, \quad (4)$$

then performs H gate on t_k again, and measures t_k. If $|0\rangle$ is obtained, then $d(x) = 0$, otherwise $d(x) = 1$.

A simple description of the above process is: Cl prepares $\frac{|\mathbf{0}\rangle_t + |x\rangle_t}{\sqrt{2}}$ and sends t to SE; SE flips its phase: $\frac{|\mathbf{0}\rangle_t + (-1)^{d(x)}|x\rangle_t}{\sqrt{2}}$, and returns it to Cl; Cl measures it on base $|x_\pm\rangle_t = \frac{|\mathbf{0}\rangle_t \pm |x\rangle_t}{\sqrt{2}}$. To prevent attacks, Shi et al. [22] introduce an additional particle h, and use *XOR* gate to entangle it with t: $\frac{|\mathbf{0}\rangle_h|\mathbf{0}\rangle_t + |x\rangle_h|x\rangle_t}{\sqrt{2}}$. Cl holds h, and then he can detect cheating if the returned t is not entangled with h.

3 Double-Blind Quantum Identity Authentication Protocol Based on Scalar Product Computation

Assume that there are three parties: Alice and Bob are the two parties involved in authentication, where Alice wants to prove her identity to Bob. Charlie is a third-party platform. Our QIA protocol consists of a key generation stage and an authentication stage, and the specific process is as follows.

3.1 Key Generation Stage

Step 1 Alice, Bob and Charlie first agree on three integers q, m, n. Alice prepares mq pairs n-qubit particles $\left(h^1, t^1\right), \left(h^2, t^2\right), \ldots, \left(h^{mq}, t^{mq}\right)$, where $h^j = \left(h_1^j, \ldots, h_n^j\right)$, $t^j =$

$\left(t_1^j, \ldots, t_n^j\right)$. $\forall j = 1, ..., mq$, she prepares state $\left|z_+^j\right\rangle_{h^j}$, where $z^j \in \{0, 1\}^n$ is selected randomly. She uses *XOR* gate to entangle h^j, t^j:

$$XOR : \frac{|\mathbf{0}\rangle_{h^j} + \left|z^j\right\rangle_{h^j}}{\sqrt{2}} |\mathbf{0}\rangle_{t^j} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}}, \tag{5}$$

and inserts several decoy qubits in randomly selected states ($|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$) into t^j. Then she sends all t^j to Charlie.

Step 2 Charlie now performs eavesdropper testing: Alice tells Charlie the details of those decoy qubits, then Charlie measures them. If the accuracy of the results is not enough, this communication will be terminated. After the testing, Charlie selects mq bits $b^j \in \{0, 1\}$ randomly. $\forall j = 1, \ldots, mq$, if $b^j = 1$, he performs F gate on t^j:

$$F^{b^j} : \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + (-1)^{b^j} \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}}. \tag{6}$$

Now he inserts several decoy qubits as well and then sends t^j to Bob.

Step 3 After eavesdropper testing, Bob selects mq strings $s^j \in \{0, 1\}^n$. For each bit s_i^j of s^j, if $s_i^j = 1$, he performs Z gate on the i-th qubit t_i^j of t^j:

$$Z^{s^j} : \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + (-1)^{b^j} \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + (-1)^{b^j \oplus (z^j \cdot s^j)} \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}}. \tag{7}$$

Then he inserts decoy qubits too, and then sends t^j to Alice.

Step 4 After eavesdropper testing, Alice first applies *XOR* gate on h^j, t^j again:

$$XOR : \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + (-1)^{b^j \oplus (z^j \cdot s^j)} \left|z^j\right\rangle_{h^j} \left|z^j\right\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} + (-1)^{b^j \oplus (z^j \cdot s^j)} \left|z^j\right\rangle_{h^j}}{\sqrt{2}} |\mathbf{0}\rangle_{t^j}, \tag{8}$$

then measure t^j. If obtaining $|\mathbf{0}\rangle$, continues; Otherwise, terminates the protocol.

Step 5 Alice measures h^j on base $\left|z_\pm^j\right\rangle_{h^j}$. If $\left|z_+^j\right\rangle$ is obtained, she takes z^j as a part of her key; Otherwise, she discards it. When m valid n-bit strings z^j are obtained, she tells Charlie and Bob the indexes j of these strings.

Step 6 Alice, Bob and Charlie hold their z^j, s^j, b^j respectively.

3.2 Authentication Stage

Step 1 Bob prepares m pairs n-qubit particles $\left(h^1, t^1\right), \ldots, (h^m, t^m)$. $\forall j = 1, ..., m$, he prepares $\left|s_+^j\right\rangle_{h^j}$ and uses *XOR* gate on h^j, t^j:

$$XOR : \frac{|\mathbf{0}\rangle_{h^j} + \left|s^j\right\rangle_{h^j}}{\sqrt{2}} |\mathbf{0}\rangle_{t^j} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} |\mathbf{0}\rangle_{t^j} + \left|s^j\right\rangle_{h^j} \left|s^j\right\rangle_{t^j}}{\sqrt{2}}, \tag{9}$$

then inserts several decoy qubits into t^j and sends it to Charlie.

Step 2 After eavesdropper testing, if $b^j = 1$, Charlie performs F gate on t^j:

$$F^{b^j} : \frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j} + |s^j\rangle_{h^j}|s^j\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j} + (-1)^{b^j}|s^j\rangle_{h^j}|s^j\rangle_{t^j}}{\sqrt{2}}. \tag{10}$$

Now he inserts several decoy qubits as well and then sends t^j to Alice.

Step 3 After eavesdropper testing, for each bit z_i^j of z^j, if $z_i^j = 1$, Alice performs Z gate on the i-th qubit t_i^j of t^j:

$$Z^{z^j} : \frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j} + (-1)^{b^j}|s^j\rangle_{h^j}|s^j\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j} + (-1)^{b^j\oplus(z^j\cdot s^j)}|s^j\rangle_{h^j}|s^j\rangle_{t^j}}{\sqrt{2}}. \tag{11}$$

Then she inserts decoy qubits and sends them to Bob.

Step 4 After eavesdropper testing, Bob first applies *XOR* gate on h^j, t^j again:

$$XOR : \frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j} + (-1)^{b^j\oplus(z^j\cdot s^j)}|s^j\rangle_{h^j}|s^j\rangle_{t^j}}{\sqrt{2}} \rightarrow \frac{|\mathbf{0}\rangle_{h^j} + (-1)^{b^j\oplus(z^j\cdot s^j)}|s^j\rangle_{h^j}}{\sqrt{2}}|\mathbf{0}\rangle_{t^j}, \tag{12}$$

then measures t^j. If obtaining $|\mathbf{0}\rangle$, continues; Otherwise, terminates the protocol.

Step 5 Bob measures h^j on base $\left|s_{\pm}^j\right\rangle_{h^j}$.

Step 6 They perform the above process again and obtain another group of results. If these two groups are the same, continue; Otherwise, terminate the protocol.

Step 7 If $\forall j = 1, \ldots, m$, the result is $\left|s_{+}^j\right\rangle$, then Alice is successfully authenticated.

4 Protocol Analysis

4.1 Correctness

In the key generation stage, if $\left|z_{+}^j\right\rangle_{h^j}$ is obtained, then $z^j \cdot s^j = b^j$; Otherwise, $z^j \cdot s^j \neq b^j$. As the same, in the authentication stage, if Bob gets $\left|s_{+}^j\right\rangle_{h^j}$, it means $z^j \cdot s^j = b^j$, i.e., Alice is authenticated. To ensure that they can generate m pairs of $z^j \cdot s^j$, $q = O(1)$, since $\Pr\left(z^j \cdot s^j = b^j\right) = \frac{1}{2}$.

4.2 Security

Key generation stage. In this stage, Alice, Bob and Charlie all do not want the others, or any external attackers, to learn their own information z^j, s^j, b^j, respectively. We first consider an external attacker Eve who may try the following attacks:

Intercept-and-resend attack. When any party sends particle t^j, Eve may intercept and measure it. Then she prepares a forged particle $t^{j\prime}$ and resends it to the expected receiver. However, since the states of the decoy qubits in t^j are randomly selected, she cannot prepare a correct forged particle, and the receiver will detect it.

Entangle-and-measure attack. Eve may intercept particle t^j, but only entangle it with an additional particle e, and send t^j to the receiver. She will measure e at one point. Assume two decoy qubits in t^j is $|0\rangle_{d_1}, |+\rangle_{d_2}$. To ensure that each $|0\rangle_{d_1}$ will still be measured as $|0\rangle$, the entangling operation should be as:

$$U : |a\rangle_{t^j}|\mathbf{0}\rangle_e \to |a\rangle_{t^j}|\varepsilon(a)\rangle_e. \tag{13}$$

However, the other qubit $|+\rangle_{d_2}$ will be entangled as $\frac{1}{\sqrt{2}}\big(|0\rangle_{d_2}|\psi_0\rangle + |1\rangle_{d_2}|\psi_1\rangle\big)$. If the receiver measures it on base $|+\rangle_{d_2}, |-\rangle_{d_2}$, then

$$\frac{1}{\sqrt{2}}\big(|0\rangle_{d_2}|\psi_0\rangle + |1\rangle_{d_2}|\psi_1\rangle\big) = \frac{1}{\sqrt{2}}\big(|+\rangle_{d_2}|\phi_0\rangle + |-\rangle_{d_2}|\phi_1\rangle\big), \tag{14}$$

where $|\phi_a\rangle = \frac{1}{2}\big(|\psi_0\rangle + (-1)^a|\psi_1\rangle\big)$. Then the receiver can obtain $|-\rangle_{d_2}$ with probability $p_- = \frac{1}{2}|\langle\phi_1 \mid \phi_1\rangle|^2 > 0$. Therefore, this attack can be detected.

Now we consider insider attacks. Alice may try the following attacks:

Measurement attack. When Charlie performs his phase-flip operation on t^j, Alice measures h^j on base $\left|z_+^j\right\rangle_{h^j}, \left|z_-^j\right\rangle_{h^j}$ to learn b^j. However, since the state is:

$$\frac{1}{\sqrt{2}}\left|z_+^j\right\rangle_{h^j}\frac{|\mathbf{0}\rangle_{t^j} + (-1)^{b^j}\left|z^j\right\rangle}{\sqrt{2}} + \frac{1}{\sqrt{2}}\left|z_-^j\right\rangle_{h^j}\frac{|\mathbf{0}\rangle_{t^j} - (-1)^{b^j}\left|z^j\right\rangle}{\sqrt{2}}, \tag{15}$$

she will obtain $\left|z_+^j\right\rangle_{h^j}$ or $\left|z_-^j\right\rangle_{h^j}$ with half probability, and get no information.

Forgery attack. Alice may prepare a forged state. However, since Bob or Charlie will only perform phase-flip, she can only prepare a superposition state of multiple inputs $\frac{1}{\sqrt{l+1}}(|0\rangle + |a_1\rangle + |a_2\rangle + \ldots + |a_l\rangle)$. Then she will obtain

$$\frac{1}{\sqrt{l+1}}\Big(|0\rangle + (-1)^{b^j\oplus(a_1\cdot s^j)}|a_1\rangle + (-1)^{b^j\oplus(a_2\cdot s^j)}|a_2\rangle + \ldots + (-1)^{b^j\oplus(a_l\cdot s^j)}|a_l\rangle\Big). \tag{16}$$

However, if $l > 1$, she cannot extract a piece of valid information, since the two states $\frac{1}{\sqrt{l+1}}(|0\rangle + |a_1\rangle + \ldots \pm |a_l\rangle)$ are not orthogonal. Therefore, this attack is ineffective.

Now we consider the attack from Charlie. He may do the following:

Intercept-and-resend attack. When Charlie receives the particle t^j from Alice, he may intercept it and resend a forged particle $|a\rangle_{t^{j\prime}}$ to Bob. Then he will measure t^j, and obtain z^j with probability $\frac{1}{2}$. However, the entanglement between t^j and h^j is broken. When Alice receives $t^{j\prime}$, she will perform *XOR* gate on them:

$$XOR : \left|z^j\right\rangle_{h^j}|a\rangle_{t^{j\prime}} \to \left|z^j\right\rangle_{h^j}\left|a\oplus z^j\right\rangle_{t^{j\prime}}. \tag{17}$$

To ensure that the measured result of $t^{j\prime}$ is $|\mathbf{0}\rangle$, $|a\rangle = \left|z^j\right\rangle$ must hold. Now

$$\left|z^j\right\rangle_{h^j} = \frac{1}{\sqrt{2}}\left|z^j_+\right\rangle_{h^j} + \frac{1}{\sqrt{2}}\left|z^j_-\right\rangle_{h^j}. \tag{18}$$

After the measurement, Alice will get $\left|z^j_+\right\rangle_{h^j}$, $\left|z^j_-\right\rangle_{h^j}$ in a uniform probability. Since $z^j \cdot s^j = b^j$ doesn't hold, this key cannot be used to authenticate.

Entangle-and-measure attack. Charlie may intercept particle t^j, but only entangle it with an additional particle e, and send t^j to Bob. After Bob performs his phase-flip operation, Charlie will measure e to steal s^j. Considering that Alice will use *XOR* gate and check if the measured result is $|\mathbf{0}\rangle$, the entanglement should be as

$$U : |a\rangle_{t^j}|\mathbf{0}\rangle_e \rightarrow |a\rangle_{t^j}|\varepsilon(a)\rangle_e, \tag{19}$$

After Bob's phase-flip, t^j changes to

$$\frac{|\mathbf{0}\rangle_{h^j}|\mathbf{0}\rangle_{t^j}|\varepsilon(\mathbf{0})\rangle_e + (-1)^{z^j\cdot s^j}\left|z^j\right\rangle_{h^j}\left|z^j\right\rangle_{t^j}\left|\varepsilon\left(z^j\right)\right\rangle_e}{\sqrt{2}}. \tag{20}$$

Charlie cannot obtain s^j by measurement, the same as Alice's measurement attack.

Now consider Bob's attack. He may do the following attacks:

Intercept-and-resend attack. When Bob receives t^j from Charlie, he may intercept it and resend a forged particle $|a\rangle_{t^j}$, to Alice. He measures t^j, and obtains z^j with probability $\frac{1}{2}$. Just like Charlie, the z^j Bob gets cannot be used for authentication.

Entangle-and-measure attack. This attack is the same as Charlie's, i.e., he cannot get any valid information of Charlie, and therefore, the z^j Bob gets is invalid.

Authentication stage. In this stage, in addition to protect the three parties' information, Alice should not be impersonated also.

Impersonation attack. Eve wants to impersonate the real Alice. She randomly prepares a group of forged keys z^j and performs the authentication. However, since the probability of $z^j \cdot s^j = b^j$ is $\frac{1}{2}$, the probability that all z^j is correct is $\frac{1}{2^m}$.

Other external and insider attacks is similar to the key generation stage, only except for Charlie or Alice's intercept-and-resend attack, and Alice's entangle-and-measure attack. The decisive loophole lies in Bob's result, as a random selection between $\left|s^j_\pm\right\rangle_{h^j}$. However, because of Step 6, if they perform the above attacks, the two groups of results cannot be the same, and Bob will detect it.

4.3 Complexity

At first, the complexity of all the operations in Sect. 2.1 is $O(n)$ at most. For example, F gate can be realized as follows: first, using n times X to invert all the qubits of $|a\rangle$, then $|a\rangle = |1\rangle^{\otimes n}$ only if $a = \mathbf{0}$. Prepare an additional qubit $|1\rangle_g$, then perform X on g controlled by all the qubits of $|a\rangle$, and perform Z on g.

Since $q = O(1)$, the phase-encoded query is performed $O(m)$ times, the complexity is $O(mn) = O(M)$, where $M = mn$. Consider M as the length of a key.

5 Conclusion

In this paper, we propose a double-blind quantum identity authentication protocol based on scalar product computation. We realize the double blindness by using phase-encoded quantum private query and introducing a third-party platform. Our protocol allows two participants involved in authentication to be unaware of each other's keys. Even if one party's key is leaked, the other party's key cannot be obtained.

Acknowledgments. This work is supported by the Project from State Grid FuJian Electric Power Company Limited under Grant No. 52130M21N001.

References

1. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput.Comput. **26**(5), 1484–1509 (1997)
2. Grover, L.K.: Quantum mechanics helps in searching for a needle in a haystack. Phys. Rev. Lett. **79**(2), 325–328 (1997)
3. Simon, D.R.: On the power of quantum computing. SIAM J. Comput.Comput. **26**(5), 1474–1483 (1997)
4. Crépeau, C., Salvail, L.: Quantum oblivious mutual identification. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, pp. 133–146. Springer, Saint-Malo, France, Berlin Heidelberg (1995)
5. Li, X., Barnum, H.: Quantum authentication using entangled states. Int. J. Found. Comput. Sci.Comput. Sci. **15**(04), 609–617 (2004)
6. Wang, I., Zhang, Q., Tang, C.J.: Multiparty simultaneous quantum identity authentication based on entanglement swapping. Chin. Phys. Lett. **23**(9), 2360–2363 (2006)
7. Zhang, S., Chen, Z.K., Shi, R.H., Liang, F.Y.: A novel quantum identity authentication based on Bell states. Int. J. Theor. Phys.Theor. Phys. **59**(1), 236–249 (2020)
8. Hong, C.H., Heo, J., Jang, J.G., Kwon, D.: Quantum identity authentication with single photon. Quantum Inf. Process. **16**(10), 236 (2017)
9. Zawadzki, P.: Quantum identity authentication without entanglement. Quantum Inf. Process. **18**(1), 1–12 (2018). https://doi.org/10.1007/s11128-018-2124-2
10. Zhu, H., Wang, L., Zhang, Y.: An efficient quantum identity authentication key agreement protocol without entanglement. Quantum Inf. Process. **19**(10), 381 (2020)
11. Rao, B.D., Jayaraman, R.: A novel quantum identity authentication protocol without entanglement and preserving pre-shared key information. Quantum Inf. Process. **22**(2), 92 (2023)
12. Sobota, M., Kapczynski, 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, pp. 799–802, IEEE, Prague, Czech Republic (2011)
13. Liu, B., Gao, Z., Xiao, D., Huang, W., Zhang, Z., Xu, B.J.: Quantum identity authentication in the counterfactual quantum key distribution protocol. Entropy **21**(5), 518 (2019)
14. Ma, H., Huang, P., Bao, W., Zeng, G.: Continuous-variable quantum Identity authentication based on quantum teleportation. Quantum Inf. Process. **15**(6), 2605–2620 (2016)
15. Yang, Y.G., Wen, Q., Zhang, X.: Multiparty simultaneous quantum identity authentication with secret sharing. Sci. China, Ser. G **51**(3), 321–327 (2008)

16. Abulkasim, H., Hamad, S., Khalifa, A., El Bahnasy, K.: Quantum secret sharing with identity authentication based on Bell states. Int. J. Quantum Inf. **15**(04), 1750023 (2017)
17. 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. **13**(11), 2535–2549 (2014)
18. Dutta, A., Pathak, A.: Controlled secure direct quantum communication inspired scheme for quantum identity authentication. Quantum Inf. Process. **22**(1), 13 (2023)
19. Li, Q., Li, Z., Chan, W.H., Zhang, S., Liu, C.: Blind quantum computation with identity authentication. Phys. Lett. A **382**(14), 938–941 (2018)
20. Quan, J., Li, Q., Liu, C., Shi, J., Peng, Y.: A simplified verifiable blind quantum computing protocol with quantum input verification. Quantum Eng. **3**(1), e58 (2021)
21. Olejnik, L.: Secure quantum private information retrieval using phase-encoded queries. Phys. Rev. AA **84**(2), 022313 (2011)
22. Shi, R.H., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Privacy-preserving point-inclusion protocol for an arbitrary area based on phase-encoded quantum private query. Quantum Inf. Process. **16**(1), 8 (2017)