

2016

# Quantum private set intersection cardinality and its application to anonymous authentication

Runhua Shi
*University of Wollongong*, rshi@uow.edu.au

Yi Mu
*University of Wollongong*, ymu@uow.edu.au

Hong Zhong
*Anhui University*

Shun Zhang
*Anhui University*

Jie Cui
*Anhui University*

## Publication Details

Shi, R., Mu, Y., Zhong, H., Zhang, S. & Cui, J. (2016). Quantum private set intersection cardinality and its application to anonymous authentication. Information Sciences, 370-371 147-158.

# Quantum private set intersection cardinality and its application to anonymous authentication

**Abstract**
In this paper, we proposed an unconditionally secure quantum Private Set Intersection Cardinality (PSI-CA) protocol. Compared with classical PSI-CA protocols, the proposed protocol can dramatically reduce the communication complexity, because it only requires O(1) communication cost, which is fully independent of the size of the sets. Furthermore, based on the proposed quantum PSI-CA protocol, we constructed a novel anonymous authentication scheme. This scheme can not only achieve two basic secure goals: secure authentication and anonymity, but can also dynamically update the authorized clients. When revoking any authorized client or adding a new client, it only needs to simply compute several set operations without any complex cryptographic operation, and thus it is very suitable for applications in some dynamic environments, e.g., large-scale client-server networks.

**Keywords**
its, application, private, anonymous, set, authentication, intersection, cardinality, quantum

**Disciplines**
Engineering | Science and Technology Studies

**Publication Details**
Shi, R., Mu, Y., Zhong, H., Zhang, S. & Cui, J. (2016). Quantum private set intersection cardinality and its application to anonymous authentication. Information Sciences, 370-371 147-158.

# Quantum Private Set Intersection Cardinality and its Application to Anonymous Authentication

Run-hua Shi[1,2,*] Yi Mu[2] Hong Zhong[1] Shun Zhang[1] Jie Cui[1]

1.School of Computer Science and Technology, Anhui University, Hefei City, 230601, China
2.Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia
(*the corresponding author's email: shirh@ahu.edu.cn)

**Abstract**. In this paper, we proposed an unconditionally secure quantum Private Set Intersection Cardinality (PSI-CA) protocol. Compared with classical PSI-CA protocols, the proposed protocol can dramatically reduce the communication complexity, because it only requires $O(1)$ communication cost, which is fully independent of the size of the sets. Furthermore, based on the proposed quantum PSI-CA protocol, we constructed a novel anonymous authentication scheme. This scheme can not only achieve two basic secure goals: secure authentication and anonymity, but can also dynamically update the authorized clients. When revoking any authorized client or adding a new client, it only needs to simply compute several set operations without any complex cryptographic operation, and thus it is very suitable for applications in some dynamic environments, e.g., large-scale client-server networks.

**Keywords**: Quantum Computation; Quantum Communication; Private Set Intersection; Anonymous Authentication

## 1. Introduction

Private Set Intersection (PSI) is a primitive of secure multi-party computation [5,17] that enables two parties, a client and a server, to jointly compute the intersection of their respective sets without disclosing any private information about their inputs [11]. There are many practical applications of PSI especially in some both privacy-preserving and information-sharing settings [26]. However, for certain settings with higher privacy requirements (e.g., privacy-preserving Data Analysis & Statistics), PSI reveals too much information (i.e., the partial or full content of the sets). Private Set Intersection Cardinality (PSI-CA) [7] just right meets these requirements, because of outputting only the cardinality, not any content of the intersection.

Due to its important and wide applications, there appeared many PSI-CA protocols [7,4,8,13,16,27]. In these existing protocols, the most efficient PSI-CA protocol requires $O(n_c + n_s)$ costs in communication complexity [7], which increases linearly with both the client's set size, $n_c$, and the server's set size, $n_s$. This may not be efficient enough for some applications involved in Big Data.

Furthermore, the security of most existing PSI-CA protocols is based on the computational complexity assumptions, which are strongly challenged by the increasing capability of computation or algorithms [12,23]. Especially, most computational assumptions are vulnerable to attack by the quantum computer. On the other hand, quantum cryptography can provide the unconditional security, which is guaranteed by physical principles of quantum mechanics. Compared to classical cryptography, the most important advantage of quantum cryptography is that an eavesdropper can easily be detected by using the characteristics of quantum mechanics.

In addition, quantum mechanics offers novel algorithms that make it possible to speed up the solution of specific computational tasks, such as quantum factoring [23] and quantum search [12]. To the best of our knowledge, there is no any quantum protocol for PSI-CA. In this paper, we follow some ideas from quantum search and quantum counting [1,2,9,19,20], and present an unconditionally secure quantum PSI-CA protocol with only $O(1)$ communication complexity.

Anonymous authentication [21,24,25], authenticating the client without revealing his/her identity, is another important issue in some novel network environments, such as wireless mobile networks [15], wireless body area networks [18], client-server networks [6,10,22] and cloud environments [28]. Because of its importance, many

anonymous authentication schemes have been proposed [15,18,21,22,24,25,28]. However, most existing schemes utilized classical cryptographic technologies. As mentioned previously, classical cryptosystems cannot ensure the unconditional security.

Based on the proposed quantum PSI-CA protocol, we further construct a novel anonymous authentication scheme. The biggest advantage of our proposed scheme is that it can efficiently update (revoke or add) the authorized clients without employing complex cryptographic operations, and thus it is very suitable for the authentication of protecting the privacy of the clients in large-scale client-server networks or Cloud environments.

**Paper organization**: Next section gives some basic conceptions of quantum computing, and an informal definition of PSI-CA. Furthermore, we present an efficient quantum PSI-CA protocol in Section 3, and construct a novel anonymous authentication scheme in Section 4. In addition, the security analysis and performance comparisons are shown in Section 5. Finally, we conclude this paper in Section 6,

## 2. Preliminaries

### *2.1 Basic Conceptions of Quantum computing*

Quantum computing is a field at the junction of theoretical modern physics and theoretical computer science. In the following section, we first review some basic conceptions of quantum computing [20].

#### *2.1.1 Quantum bits*

The bit is the fundamental concept of classical computation and classical information. Quantum computation and quantum information are built upon an analogous concept, the quantum bit, or qubit for short. Just as a classical bit has a state – either 0 or 1 – a qubit also has a state. Accordingly, two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$, where $|0\rangle$ and $|1\rangle$ are two orthogonal unit vectors in 2-dimensional Hilbert space and further form a perfect complete orthogonal basis (later also called the computational basis). Here, notation like '$|\ \rangle$' is called the Dirac notation, which is the standard notation for states in quantum mechanics. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form linear combinations of states, often called superpositions:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1}$$

where $\alpha$ and $\beta$ are complex numbers, and $|\alpha|^2 + |\beta|^2 = 1$. Furthermore, it can be naturally generalized to multiple qubits. For example, an $n$-qubit system can exist in any superposition of the $2^n$ basis states

$$|\Psi\rangle = \alpha_0|00\ldots00\rangle + \alpha_1|00\ldots01\rangle + \alpha_2|00\ldots10\rangle + \cdots + \alpha_{2^n-1}|11\ldots11\rangle, \tag{2}$$

with $\sum_{i=0}^{2^n-1}|\alpha_i|^2 = 1$, where the states $|00\ldots00\rangle$, $|00\ldots01\rangle$,…, $|11\ldots10\rangle$ and $|11\ldots11\rangle$ form a perfect complete orthogonal basis in $n$-dimensional Hilbert space.

#### *2.1.2 Quantum measurement*

A measurement is described by an Hermitian operator (observable), $M = \sum_m mP_m$, where $P_m$ is the projector onto the eigenspace of $M$ with eigenvalue $m$. After the measurement the state will be $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$ with probability $p(m) = \langle\psi|P_m|\psi\rangle$.

For example, $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ are a set of projector operators in 2-dimensional Hilbert space, where

$$\begin{aligned} P_0|\psi\rangle &= |0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|0\rangle\langle 0|0\rangle + \beta|0\rangle\langle 0|1\rangle \\ &= \alpha|0\rangle, \end{aligned} \tag{3}$$

$$\begin{aligned} P_1|\psi\rangle &= |1\rangle\langle 1|(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha|1\rangle\langle 1|0\rangle + \beta|1\rangle\langle 1|1\rangle \\ &= \beta|1\rangle, \end{aligned} \tag{4}$$

$$
\begin{aligned}
p(0) &= \langle\psi|P_0|\psi\rangle \\
&= (\alpha^*\langle 0| + \beta^*\langle 1|)P_0(\alpha|0\rangle + \beta|1\rangle) \\
&= (\alpha^*\langle 0| + \beta^*\langle 1|)\alpha|0\rangle \\
&= |\alpha|^2, \qquad (5) \\
p(1) &= \langle\psi|P_1|\psi\rangle \\
&= (\alpha^*\langle 0| + \beta^*\langle 1|)P_1(\alpha|0\rangle + \beta|1\rangle) \\
&= (\alpha^*\langle 0| + \beta^*\langle 1|)\beta|1\rangle \\
&= |\beta|^2. \qquad (6)
\end{aligned}
$$

In other words, if we make a measurement on the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the basis $\{|0\rangle, |1\rangle\}$, $|\psi\rangle$ will be collapsed into the state $|0\rangle$ or $|1\rangle$, with respective probabilities $|\alpha|^2$ and $|\beta|^2$. Similarly, measuring $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \cdots + \alpha_{2^n-1}|2^n - 1\rangle$ in the computational basis $\{|1\rangle, |2\rangle,\ldots, |2^n - 1\rangle\}$ gives $|i\rangle$ with probability $|\alpha_i|^2$.

### *2.1.3 Quantum transformation*

In quantum mechanics, the evolution of a closed system is described by a unitary transformation (or unitary operation), $|\psi\rangle = U|\phi\rangle$ (i.e., input a state $|\phi\rangle$, and output a different state $U|\phi\rangle$), where $|\phi\rangle$ is the initial state of the system and $|\psi\rangle$ is the final state of the system after applying the unitary transformation $U$. We say that $U$ is unitary if $U^+U = I$, where $U^+$ is the conjugate transpose of $U$ and $I$ is the identity operator.

A quantum logical gate is an elementary quantum device which performs a unitary operation on qubits. A simple example of one-qubit quantum gate is *NOT* gate, which maps $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$. The *Hadamard* gate is another very useful one-qubit quantum gate, defined by,

$$
\begin{aligned}
H|0\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\
H|1\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \qquad (7)
\end{aligned}
$$

The most useful multi-qubit quantum logic gate is the *controlled-NOT* or *CNOT* gate: $|00\rangle \to |00\rangle$, $|01\rangle \to |01\rangle$, $|10\rangle \to |11\rangle$ and $|11\rangle \to |10\rangle$, where the first qubit is the control qubit, and the second qubit is the target qubit. That is, if the control qubit is set to 0, then the target qubit is left alone. If the control qubit is set to 1, then the target qubit is flipped.

In addition, an important quantum transformation which we shall use later is the quantum Fourier transform. The quantum Fourier transform is a linear transformation on qubits, and is the quantum version of the standard discrete Fourier transform. For $x \in \{0,1,\ldots,M-1\}$, the quantum Fourier transform and the inverse quantum Fourier transform are defined as follows [9]:

$$
QFT : |x\rangle \ \to \ \tfrac{1}{\sqrt{M}}\textstyle\sum_{y=0}^{M-1} e^{2\pi i\frac{x}{M}y}|y\rangle, \qquad (8)
$$

$$
QFT^{-1} : |x\rangle \ \to \ \tfrac{1}{\sqrt{M}}\textstyle\sum_{y=0}^{M-1} e^{-2\pi i\frac{x}{M}y}|y\rangle. \qquad (9)
$$

Clearly,

$$
\begin{aligned}
QFT^{-1}(QFT|x\rangle) &= QFT^{-1}\left(\tfrac{1}{\sqrt{M}}\textstyle\sum_{y=0}^{M-1} e^{2\pi i\frac{x}{M}y}|y\rangle\right) \\
&= \tfrac{1}{\sqrt{M}}\textstyle\sum_{y=0}^{M-1} e^{2\pi i\frac{x}{M}y} QFT^{-1}\,|y\rangle \\
&= \tfrac{1}{\sqrt{M}}\textstyle\sum_{y=0}^{M-1} e^{2\pi i\frac{x}{M}y}(\tfrac{1}{\sqrt{M}}\textstyle\sum_{j=0}^{M-1} e^{-2\pi i\frac{y}{M}j}|j\rangle) \\
&= \tfrac{1}{M}\textstyle\sum_{j=0}^{M-1}\sum_{y=0}^{M-1} e^{2\pi i\frac{y}{M}(x-j)}|j\rangle \\
&= \tfrac{1}{M}\textstyle\sum_{y=0}^{M-1}|x\rangle + \tfrac{1}{M}\sum_{j=0:j\neq x}^{M-1}(\sum_{y=0}^{M-1} e^{2\pi i\frac{y}{M}(x-j)})|j\rangle
\end{aligned}
$$

$$= |x\rangle. \tag{10}$$

### *2.1.4 Quantum Parallelism*

Quantum parallelism allows a quantum computer (or a quantum circuit) to perform multiple computations simultaneously. The term was coined by physicist David Deutsch, so as to distinguish it from classical parallel computation in standard computers.

In classical settings, parallel computing is performed by having several processors linked together, so that each processor performs one computation while the other processors are performing other computations.

In quantum settings, a single quantum processor is able to perform multiple computations on its own by utilizing the fact that the qubit exists in the superposition of multiple states. This gives a quantum computer much greater raw computation ability than a traditional computer.

For example, we consider a two-qubit quantum circuit, which performs a quantum transformation $U_f$, defined by

$$U_f\colon\ |x\rangle|y\rangle \ \ \rightarrow \ \ |x\rangle|y \oplus f(x)\rangle, \tag{11}$$

where $f(x)\colon \{0,1\} \rightarrow \{0,1\}$ is a classical function, and $\oplus$ denotes the addition module 2. If $y = 0$, then the final state of the second qubit is just the value $f(x)$. That is, $U_f\colon\ |x\rangle|0\rangle \rightarrow |x\rangle|f(x)\rangle$. Furthermore, if $|x\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, then

$$\begin{aligned} U_f \frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle &= U_f \frac{|0\rangle|0\rangle+|1\rangle|0\rangle}{\sqrt{2}} \\ &= \frac{U_f|0\rangle|0\rangle+U_f|1\rangle|0\rangle}{\sqrt{2}} \\ &= \frac{|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle}{\sqrt{2}}. \end{aligned} \tag{12}$$

That is, the quantum transformation $U_f$ computes $f(0)$ and $f(1)$ simultaneously. It can easily be generalized to a more powerful $U_f$ that implements a more general function $f(x)\colon \{0,1\}^n \rightarrow \{0,1\}$, such that $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, where the qubit lengths of the states $|x\rangle$ and $|y\rangle$ are $n$ and 1, respectively. Similarly, consider the case where $|x\rangle = H^{\otimes n}|0\rangle^{\otimes n}$ and $|y\rangle = |0\rangle$. Then

$$\begin{aligned} U_f|x\rangle|0\rangle &= U_f H^{\otimes n}|0\rangle^{\otimes n}|0\rangle \\ &= U_f[\tfrac{|0\rangle+|1\rangle}{\sqrt{2}}]^{\otimes n}|0\rangle \\ &= U_f(\tfrac{1}{\sqrt{2^n}}\textstyle\sum_{i=0}^{2^n-1}|i\rangle)|0\rangle \\ &= \tfrac{1}{\sqrt{2^n}}\textstyle\sum_{i=0}^{2^n-1}|i\rangle\,|f(i)\rangle. \end{aligned} \tag{13}$$

From Eq.13, we can clearly see that the quantum transformation $U_f$ computes $f(i)$ s for all values of $i$ simultaneously. However, there is no immediate way of seeing them all together, because once the output state is measured, only one value of $f(i)$ is revealed and the rest vanish.

### *2.2 Private Set Intersection Cardinality*

Here, we give an informal definition of PSI-CA.

**Definition 1**. Private Set Intersection Cardinality (PSI-CA) - There are two parties, a client and a server. The client inputs a private set $A$ and the server inputs a private set $B$. After running a PSI-CA protocol, the client outputs the cardinality of their intersection, i.e., $|A \cap B|$, but the server gets nothing. In addition, PSI-CA should meet the following privacy requirements:

***Server Privacy***. The client learns no information about the set elements of the server except knowing the set size, $|B|$.

***Client Privacy***. The server cannot get any private information about the client's set.

There are many important applications of PSI-CA in privacy-preserving settings. For instance, PSI-CA can be used in social networking [3], e.g., when two parties want to privately determine the number of common connections in order to decide whether or not to become friends.

### 3. Quantum Private Set Intersection Cardinality

In this section, we follow some ideas from Grover's search algorithm [1,12] and quantum counting algorithms [2,9,19,20], take advantage of quantum parallelism, and present a novel quantum PSI-CA protocol. Suppose the client's private set $A = \{a_1, a_2, \cdots, a_{n_c}\}$ and the server's private set $B = \{b_1, b_2, \cdots b_{n_s}\}$, and all elements of the sets $A$ and $B$ lie in $\mathbb{Z}_N$, where $\mathbb{Z}_N = \{0,1,2, \dots, N-1\}$ and $N = 2^n$ (i.e., $n = \log N$). In addition, we assume that $n_c + n_s < \frac{N}{2}$, and $N$ and $n_s$ are public. The proposed protocol consists of 5 steps, which are described in detail as follows.

**Step 1.** The client prepares an initial state $|\varphi_0\rangle$ in $|0\rangle^{\otimes n}$, further applies $H^{\otimes n}$ to the state $|\varphi_0\rangle$, and then gets the resultant state $|\varphi_1\rangle$. That is, $|\varphi_1\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$. Then the client sends $|\varphi_1\rangle$ to the server through the quantum channel.

**Step 2.** After receiving the state $|\varphi_1\rangle$, the server prepares an ancillary state $|r\rangle$, where $r$ is a random integer in $\{0,1\}$. Furthermore, the server performs an oracle transformation $U_{f_s}$ on the state $|\varphi_1\rangle \otimes |r\rangle$, where $U_{f_s}$ is and works as follows:

$$f_s(x) = \begin{cases} 1 & if\ x \in B \\ 0 & if\ x \notin B \end{cases}, \tag{14}$$

$$U_{f_s}:\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r\rangle \ \rightarrow\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x)\rangle\ . \tag{15}$$

Here, we call the resultant state $|\varphi_2\rangle$, i.e., $|\varphi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x)\rangle$. Then the server sends $|\varphi_2\rangle$ back to the client through the quantum channel.

**Step 3.** After receiving the state $|\varphi_2\rangle$, the client performs another oracle transformation $U_{f_c}$ on it, where the transformation $U_{f_c}$ is described as follows:

$$f_c(x) = \begin{cases} 1 & if\ x \in A \\ 0 & if\ x \notin A \end{cases}, \tag{16}$$

$$U_{f_c}:\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x)\rangle \ \rightarrow\ \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x) \oplus f_c(x)\rangle. \tag{17}$$

Here, the resultant state is called $|\varphi_3\rangle$, that is, $|\varphi_3\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x) \oplus f_c(x)\rangle$. Please note, $f_s(x) \oplus f_c(x) \Leftrightarrow (x \in B) \oplus (x \in A)$, so the state $|\varphi_3\rangle$ has carried the classical information about the cardinality of their intersection.

**Step 4.** In order to extract the intersection cardinality from the state $|\varphi_3\rangle$, the client prepares another quantum state in $\frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle$, where $M$ is a big enough integer, so that the value of $\frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N-2t|$ is small enough ($t$ is later defined in Step 5). Let $|\varphi_4\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes |\varphi_3\rangle$. Furthermore, the client applies a quantum operator $C_F$ to the state $|\varphi_4\rangle$, and then gets the state $|\varphi_5\rangle$, where $C_F$ is defined as follows:

$$\begin{aligned} C_F:|\varphi_4\rangle \ &\rightarrow |\varphi_5\rangle, \\ C_F:\frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes |\varphi_3\rangle \ &\rightarrow\ \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes G^y|\varphi_3\rangle, \\ |\varphi_5\rangle &= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes G^y|\varphi_3\rangle, \end{aligned} \tag{18}$$

$$= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes G^y\left(\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x) \oplus f_c(x)\rangle\right). \tag{19}$$

Here, $G$ is the amplitude amplification operator, defined by

$$G = U_{\varphi_3} U_{f_r} , \tag{20}$$

$$U_{f_r}|x\rangle|r\rangle = \begin{cases} -|x\rangle|1\rangle & if\ r = 1 \\ |x\rangle|0\rangle & if\ r = 0 \end{cases}, \tag{21}$$

$$U_{\varphi_3} = 2|\varphi_3\rangle\langle\varphi_3| - I, \tag{22}$$

where $I$ is the identity operator.

**Step 5.** The client applies $QFT^{-1}$ to the first log$M$ qubits of the state $|\varphi_5\rangle$ and then measures the first log$M$ qubits in the computational basis to obtain $|x\rangle$. Finally, he/she outputs $Nsin^2(\frac{x}{M}\pi)$ as the estimation of $t$, which is the number of the items that the last one qubit of the state $|\varphi_3\rangle$ is in $|1\rangle$, i.e., the number of the items just like $|x\rangle|1\rangle$ in the state $|\varphi_3\rangle$. If $t < N/2$, then the client outputs $\frac{(n_c+n_s)-t}{2}$, that is, $|A \cap B| = \frac{(n_c+n_s)-t}{2}$; otherwise, $\frac{(n_c+n_s+t)-N}{2}$, that is, $|A \cap B| = \frac{(n_c+n_s+t)-N}{2}$.

In addition, in order to check eavesdropping in the quantum channel, we can use the decoy technology. That is, the sender randomly inserts several decoy particles into the qubit sequence to be transmitted, where every decoy particle is prepared randomly with either Z-basis (i.e., $\{|0\rangle, |1\rangle\}$ or X-basis (i.e., $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$). After confirming that the receiver has received the transmitted sequence, the sender announces the positions of the decoy particles and the corresponding measurement basis. The receiver measures the decoy particles according to the sender's announcements and tells the sender his (her) measurement results. The sender compares the measurement results of the receiver with the initial states of the decoy particles in the transmitted sequence and analyzes the security of the transmissions. If the error rate is higher than the threshold determined by the channel noise, they cancel this protocol and restarts; or else they continue to the next step.

**The correctness proof.** Starting from the state $|\varphi_3\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x) \oplus f_c(x)\rangle$, we define

$$|\alpha\rangle = \frac{1}{\sqrt{t}}\sum|x\rangle|1\rangle , \tag{23}$$

$$|\beta\rangle = \frac{1}{\sqrt{N-t}}\sum|x\rangle|0\rangle . \tag{24}$$

Obviously, the state $|\varphi_3\rangle$ can be re-expressed as

$$|\varphi_3\rangle = \sqrt{\frac{N-t}{N}}|\beta\rangle + \sqrt{\frac{t}{N}}|\alpha\rangle . \tag{25}$$

In other words, $|\varphi_3\rangle$ is the uniform superposition of all product states, $|\alpha\rangle$ is the uniform superposition of these product states satisfying $r \oplus f_s(x) \oplus f_c(x) = 1$, and $|\beta\rangle$ the counterpart of $|\alpha\rangle$. Obviously, $|\alpha\rangle \perp |\beta\rangle$. Choose $\theta \in (0, \frac{\pi}{2})$ such that $sin^2\theta = \frac{t}{N}$. We have $sin\theta = \sqrt{\frac{t}{N}}$ and $cos\theta = \sqrt{\frac{N-t}{N}}$, and thus $|\varphi_3\rangle = cos\theta|\beta\rangle + sin\theta|\alpha\rangle$. Then, we can easily obtain the following equations:

$$\begin{aligned} G|\beta\rangle &= U_{\varphi_3}U_{f_r}|\beta\rangle = U_{\varphi_3}|\beta\rangle \\ &= (2|\varphi_3\rangle\langle\varphi_3| - I)|\beta\rangle \\ &= 2|\varphi_3\rangle\langle\varphi_3|\beta\rangle - |\beta\rangle \\ &= 2cos\theta|\varphi_3\rangle - |\beta\rangle \\ &= 2cos\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) - |\beta\rangle \\ &= (2cos^2\theta - 1)|\beta\rangle + 2sin\theta cos\theta|\alpha\rangle \\ &= cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle , \\ G|\alpha\rangle &= U_{\varphi_3}U_{f_r}|\alpha\rangle = U_{\varphi_3}(-|\alpha\rangle) \\ &= (2|\varphi_3\rangle\langle\varphi_3| - I)(-|\alpha\rangle) \end{aligned} \tag{26}$$

$$
\begin{aligned}
&= -2|\varphi_3\rangle\langle\varphi_3|\alpha\rangle + |\alpha\rangle \\
&= -2sin\theta|\varphi_3\rangle + |\alpha\rangle \\
&= -2sin\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) + |\alpha\rangle \\
&= -2sin\theta cos\theta|\beta\rangle + (1 - 2sin^2\theta)|\alpha\rangle \\
&= -sin2\theta|\beta\rangle + cos2\theta|\alpha\rangle\ . \qquad (27)
\end{aligned}
$$

Obviously, $G$ is a rotation operator of angle $2\theta$ oriented from $|\beta\rangle$ to $|\alpha\rangle$ in the two-dimensional subspace spanned by $|\alpha\rangle$ and $|\beta\rangle$. If we start from the state $|\varphi_3\rangle$, each application of $G$ rotates it toward $|\alpha\rangle$ by $2\theta$. Thus, repeated application of $G$ rotates it close to $|\alpha\rangle$. Furthermore, we define two orthogonal states as follows:

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle)\ , \qquad (28)$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle + i|\alpha\rangle)\ . \qquad (29)$$

Then,

$$
\begin{aligned}
G|\phi_+\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle - iG|\alpha\rangle) \\
&= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle + isin2\theta|\beta\rangle - icos2\theta|\alpha\rangle \ \text{(by Eqs.(26) and (27))} \\
&= \frac{e^{i2\theta}}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle) \quad (\text{by } e^{i2\theta} = cos2\theta + isin2\theta) \\
&= e^{i2\theta}|\phi_+\rangle, \qquad (30) \\
G|\phi_-\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle + iG|\alpha\rangle) \\
&= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle - isin2\theta|\beta\rangle + icos2\theta|\alpha\rangle \ \text{(by Eqs.(26) and (27))} \\
&= \frac{e^{-i2\theta}}{\sqrt{2}}(|\beta\rangle + i|\alpha\rangle) \quad (\text{by } e^{-i2\theta} = cos2\theta - isin2\theta) \\
&= e^{-i2\theta}|\phi_-\rangle\ . \qquad (31)
\end{aligned}
$$

That is, $|\phi_+\rangle$ and $|\phi_-\rangle$ are eigenvectors of $G$ with eigenvalues $e^{2i\theta}$ and $e^{-2i\theta}$, respectively. Let $\theta = \pi\omega$, then $|\varphi_3\rangle = cos\theta|\beta\rangle + sin\theta|\alpha\rangle = \frac{e^{i\pi\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\phi_-\rangle$. If we apply $G$ to $|\varphi_3\rangle$ for $y$ times, then

$$G^y\ |\varphi_3\rangle = \frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle. \qquad (32)$$

Thus, we get

$$
\begin{aligned}
|\varphi_5\rangle &= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes G^y|\varphi_3\rangle \\
&= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}[|y\rangle\otimes(\frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle)] \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{-i2\pi y\omega}|y\rangle|\phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}|y\rangle|\phi_-\rangle\ . \qquad (33)
\end{aligned}
$$

After applying $QFT^{-1}$ to the first $\log M$ qubits of the state $|\varphi_5\rangle$, we have

$$
\begin{aligned}
QFT^{-1}|\varphi_5\rangle &= QFT^{-1}[\frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}|y\rangle|\phi_-\rangle] \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}(QFT^{-1}|y\rangle)|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}(QFT^{-1}|y\rangle)|\phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}(\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}e^{-i2\pi\frac{y}{M}x}|x\rangle)|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}(\frac{1}{\sqrt{M}}\sum_{x=0}^{M-1}e^{-i2\pi\frac{y}{M}x}|x\rangle)|\phi_-\rangle
\end{aligned}
$$

$$= \frac{e^{i\pi\omega}}{\sqrt{2}} \sum_{x=0}^{M-1} \{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega - \frac{x}{M})}\} |x\rangle |\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}} \sum_{x=0}^{M-1} \{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y[(1-\omega) - \frac{x}{M}]}\} |x\rangle |\phi_-\rangle$$

$$= \frac{e^{i\pi\omega}}{\sqrt{2}} |\tilde{x}_+\rangle |\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}} |\tilde{x}_-\rangle |\phi_-\rangle \,, \tag{34}$$

with

$$|\tilde{x}_+\rangle = \sum_{x=0}^{M-1} \{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega - \frac{x}{M})}\} |x\rangle \,, \tag{35}$$

$$|\tilde{x}_-\rangle = \sum_{x=0}^{M-1} \{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y[(1-\omega) - \frac{x}{M}]}\} |x\rangle \,. \tag{36}$$

If we make a measurement on $|\tilde{x}_+\rangle$ in the computational basis $\{|0\rangle, |1\rangle, \ldots, |M-1\rangle\}$, we will get $|x\rangle$ with the probability of $\left|\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega - \frac{x}{M})}\right|^2$. So,

$$\begin{aligned}
P\left(\left|\frac{x}{M} - \omega\right| \le \frac{1}{M}\right) &= P(|x - M\omega| \le 1) \\
&= P(x = \lfloor M\omega \rfloor) + P(x = \lceil M\omega \rceil) \\
&= \left|\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega - \frac{\lfloor M\omega \rfloor}{M})}\right|^2 + \left|\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega - \frac{\lceil M\omega \rceil}{M})}\right|^2 \\
&= \left|\frac{1 - e^{i2\pi M(\omega - \frac{\lfloor M\omega \rfloor}{M})}}{M(1 - e^{i2\pi(\omega - \frac{\lfloor M\omega \rfloor}{M})})}\right|^2 + \left|\frac{1 - e^{i2\pi M(\omega - \frac{\lceil M\omega \rceil}{M})}}{M(1 - e^{i2\pi(\omega - \frac{\lceil M\omega \rceil}{M})})}\right|^2 \\
&= \left|\frac{\sin[\pi M\left(\omega - \frac{\lfloor M\omega \rfloor}{M}\right)]}{M \sin[\pi\left(\omega - \frac{\lfloor M\omega \rfloor}{M}\right)]}\right|^2 + \left|\frac{\sin[\pi M\left(\omega - \frac{\lceil M\omega \rceil}{M}\right)]}{M \sin[\pi\left(\omega - \frac{\lceil M\omega \rceil}{M}\right)]}\right|^2 \\
&= \frac{\sin^2[\pi M\left(\omega - \frac{\lfloor M\omega \rfloor}{M}\right)]}{M^2 \sin^2[\pi\left(\omega - \frac{\lfloor M\omega \rfloor}{M}\right)]} + \frac{\sin^2[\pi M\left(\omega - \frac{\lceil M\omega \rceil}{M}\right)]}{M^2 \sin^2[\pi\left(\omega - \frac{\lceil M\omega \rceil}{M}\right)]} \\
&\ge \frac{1}{M^2 \sin^2\left(\frac{\pi}{2M}\right)} + \frac{1}{M^2 \sin^2\left(\frac{\pi}{2M}\right)} \\
&= \frac{2}{M^2 \sin^2\left(\frac{\pi}{2M}\right)} \\
&> \frac{2}{M^2 \left(\frac{\pi}{2M}\right)^2} \\
&= \frac{8}{\pi^2} \,.
\end{aligned} \tag{37}$$

It shows that after measuring, $\frac{x}{M}$ is close or equal to $\omega$ with high probability. In detail, if we make a measurement on $|\tilde{x}_+\rangle$, the probability of getting either $\lfloor M\omega \rfloor$ or $\lceil M\omega \rceil$, providing an estimation for $\omega$ within the error $\frac{1}{M}$, is at least $\frac{8}{\pi^2}$. Similarly, if we make a measurement on $|\tilde{x}_-\rangle$, the probability of getting either $\lfloor M(1-\omega) \rfloor$ or $\lceil M(1-\omega) \rceil$, providing an estimation for $(1-\omega)$ within the error $\frac{1}{M}$, is at least $\frac{8}{\pi^2}$. That is, $\frac{x}{M}$ is close or equal to $1-\omega$ with high probability. Since $\theta = \pi\omega$ and $sin^2\theta = \frac{t}{N}$, $t = Nsin^2\pi\omega$. For the first case (i.e., $|\tilde{x}_+\rangle$), $\omega \approx \frac{x}{M}$, so $t \approx Nsin^2(\pi\frac{x}{M})$; for the second case (i.e, $|\tilde{x}_-\rangle$), $\omega \approx 1 - \frac{x}{M}$, so $t \approx Nsin^2\left(\pi - \pi\frac{x}{M}\right) = Nsin^2(\pi\frac{x}{M})$. In both cases, it gives the same estimation of $t$.

**Theorem 1** [9]. $\forall M \in \mathbb{Z}$, $|t - \tilde{t}| \le \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N - 2t|$ with probability at least $\frac{8}{\pi^2}$, where $\tilde{t}$ is an estimation of $t$. That is, the error $\varepsilon \le \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N - 2t|$.

Furthermore, we analyze the relations of $t$ and $|A \cap B|$, which are listed in Table 1 and 2.

**Table 1**. The relation of $t$ and $|A \cap B|$ in the case of $r = 1$

| $x$ | $f_c(x)$ | $f_s(x)$ | $r$ | $r \oplus f_s(x) \oplus f_c(x)$ | Cardinality |
|---|---|---|---|---|---|
| $x \notin A \wedge x \notin B$ | 0 | 0 | 1 | 1 | $N - \|A \cup B\|$ |
| $x \notin A \wedge x \in B$ | 0 | 1 | 1 | 0 | $\|B\| - \|A \cap B\|$ |
| $x \in A \wedge x \notin B$ | 1 | 0 | 1 | 0 | $\|A\| - \|A \cap B\|$ |
| $x \in A \wedge x \in B$ | 1 | 1 | 1 | 1 | $\|A \cap B\|$ |

Given from Table 1, obviously, we can get

$$\begin{aligned} t &= (N - |A \cup B|) + |A \cap B| \\ &= (N - (|A| + |B| - |A \cap B|)) + |A \cap B| \\ &= N - (n_c + n_s) + 2|A \cap B| \,. \end{aligned} \tag{38}$$

It implies $t > \frac{N}{2}$, since $n_c + n_s < \frac{N}{2}$. Furthermore, the following equation clearly holds,

$$|A \cap B| = \tfrac{(n_c + n_s + t) - N}{2} \,. \tag{39}$$

**Table 2**. The relation of $t$ and $|A \cap B|$ in the case of $r = 0$

| $x$ | $f_c(x)$ | $f_s(x)$ | $r$ | $r \oplus f_s(x) \oplus f_c(x)$ | Cardinality |
|---|---|---|---|---|---|
| $x \notin A \wedge x \notin B$ | 0 | 0 | 0 | 0 | $N - \|A \cup B\|$ |
| $x \notin A \wedge x \in B$ | 0 | 1 | 0 | 1 | $\|B\| - \|A \cap B\|$ |
| $x \in A \wedge x \notin B$ | 1 | 0 | 0 | 1 | $\|A\| - \|A \cap B\|$ |
| $x \in A \wedge x \in B$ | 1 | 1 | 0 | 0 | $\|A \cap B\|$ |

Given from Table 2, clearly, we can obtain

$$\begin{aligned} t &= (|B| - |A \cap B|) + (|A| - |A \cap B|) \\ &= |A| + |B| - 2|A \cap B| \\ &= n_c + n_s - 2|A \cap B| \,. \end{aligned} \tag{40}$$

It implies $t < \frac{N}{2}$, since $n_c + n_s < \frac{N}{2}$. Furthermore, the following equation obviously holds,

$$|A \cap B| = \tfrac{(n_c + n_s) - t}{2} \,. \tag{41}$$

In Step 5, it can clearly and rightly get the estimation of $t$ with the high probability $p$ ($p \geq \frac{8}{\pi^2}$) and the small error $\varepsilon$, where $\varepsilon \leq \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N - 2t|$ (e.g., if $N = 2^6$, $t = 20$ and $M = 2^{10}$, then $\varepsilon \leq 0.182$). Furthermore, if $t < N/2$, then $|A \cap B| = \frac{(n_c + n_s) - t}{2}$; otherwise, $|A \cap B| = \frac{(n_c + n_s + t) - N}{2}$. Therefore, the proposed quantum PSI-CA protocol can give a good estimation of $|A \cap B|$ with the same high probability $p$ and the same small error $\varepsilon$.

**4. Anonymous Authentication**

In this section, we present a novel anonymous authentication scheme for large-scale client-server networks based on the quantum PSI-CA protocol designed above. The proposed anonymous authentication scheme mainly includes four phases: Initialization Phase, Registration Phase, Anonymous Authentication Phase, and Updating Phase. The detailed description is as follows:

**Initialization Phase:** Suppose that there is a trusted third party (TTP), and all system parameters are generated by the TTP.

**Step 1**. The TTP selects a large integer, $N$, and two small integers, $n$ and $k$, such that $0 < k < n \ll N$.

**Step 2**. The TTP randomly generates a private set $S$ ($S \subset \mathbb{Z}_N$), such that $|S|$ is close to $\frac{N}{2}$ but $|S| + n < \frac{N}{2}$ (to meet the assumption of the proposed quantum PSI-CA protocol), and computes its complement $\bar{S} = \mathbb{Z}_N - S$.

**Step 3**. Then the TTP publishes the public parameters $\{N, n, k\}$, and privately sends the set $S$ to the server.

**Registration Phase:** Each client is required to first register at the server for subscribing the future services and to further apply for an authentication warrant to the TTP with the permission of the server.

**Step 1**. During the registration, the server checks the authenticity and legality of the client $\boldsymbol{c}_i$. After confirming his/her authenticity and legality, the server informs the TTP to generate an authentication warrant for the client $\boldsymbol{c}_i$.

**Step 2**. After receiving the permission of the server, the TTP randomly generates a ***unique*** set $C_i$ for the authorized client $\boldsymbol{c}_i$: $C_i = K_i \cup R_i$, where $K_i \subset S$ and $R_i \subset \bar{S}$, and $|K_i| = k$ and $|R_i| = n - k$. Obviously, $|C_i| = n$ and $|C_i \cap S| = k$. In addition, please note that $C_i \cap C_j = \emptyset$ if $i \neq j$. Then, the TTP privately sends the set $C_i$ to the client $\boldsymbol{c}_i$.

**Step 3**. After receiving the set $C_i$, the client $\boldsymbol{c}_i$ verifies its validity by calling a quantum PSI-CA protocol with the help of the server to compute the intersection cardinality of the sets, $C_i$ and $S$, where the client is the initiator of the quantum PSI-CA protocol. If it satisfies the condition of $k - \varepsilon \leq |C_i \cap S| \leq k + \varepsilon$, the client accepts the set $C_i$ as his/her authentication warrant for the future services, where $\varepsilon = \frac{2\pi}{M}\sqrt{t(N-t)} + \frac{\pi^2}{M^2}|N - 2t|$.

**Step 4**. Suppose that in all there are $l$ authorized clients. Finally, the TTP computes $K = \bigcup_{i=1}^{l} K_i$ and $R = \bigcup_{i=1}^{l} R_i$, which will be utilized to revoke or add the authorized clients in future.

**Anonymous Authentication Phase:** In this phase, suppose that the remote client $\boldsymbol{c}_i$ requests the server to authenticate his/her legality in order to get certain resources or services, but he/she wants to protect the privacy of his/her identity. As an authorized client, he/she must have privately owned an authentication warrant, i.e., the set $C_i$, which is generated by the TTP in advance. After receiving the authentication request of the client, the server asks the client to collaboratively execute a quantum PSI-CA protocol to compute the intersection cardinality of their respective private sets, where the server is the initiator. That is, the server and the client privately input the sets, $S$ and $C_i$, respectively, and finally the server gets an estimation of $|S \cap C_i|$ with a high probability and a small error, but the client nothing. If it satisfies that $k - \varepsilon \leq |S \cap C_i| \leq k + \varepsilon$, the authentication passes successfully, otherwise it fails.

**Updating Phase:** The updating phase includes two cases: revoking any authorized client and adding a new client.

***Revoking any client***. Suppose that the server wants to revoke the client $\boldsymbol{c}_j$. Then the server requests the TTP to announce the authentication warrant of the client $\boldsymbol{c}_j$ (i.e., $C_j$). After getting $C_j$, the server computes $K_j = S \cap C_j$, and updates his privet set $S = S - K_j$. In addition, the TTP also updates $S = S - K_j$ and $\bar{S} = \bar{S} - R_j$ by computing $K_j = S \cap C_j$ and $R_j = C_j - K_j$, and further updates $K = K - K_j$ and $R = R - R_j$. Other authorized clients' authentication warrants (i.e., private sets) keep unchanged.

***Adding a new client***. Suppose that a new client $\boldsymbol{c}_{l+1}$ requests the server to join into the client-server networks. If the server agrees his/her joining, then he informs the TTP to generate an authentication warrant for the new client. After

getting the permission of the server, the TTP randomly generates two new sets, $K_{l+1} \subset S - K$ and $R_{l+1} \subset \bar{S} - R$, where $|K_{l+1}| = k$ and $|R_{l+1}| = n - k$. Furthermore, the TTP computes $C_{l+1} = K_{l+1} \cap R_{l+1}$ and privately sends $C_{l+1}$ to the client $\boldsymbol{c}_{l+1}$. After verifying its validity, the client $\boldsymbol{c}_{l+1}$ accepts $C_{l+1}$ as his/her authentication warrant. Finally, the TTP updates $K = K \cup K_{l+1}$ and $R = R \cup R_{l+1}$. Similarly, other authorized clients' authentication warrants (i.e., private sets) keep unchanged.

## 5. Analysis

We have proved the correctness of the proposed quantum PSI-CA protocol in Section 3. In this section, we continue to analyze its security, which sees Theorem 2 and 3 in detail.

**Theorem 2** (***Server Privacy***). In our proposed quantum PSI-CA protocol, the client learns no information about the set elements of the server except knowing the set size, $n_s$.

**Proof.** In proposed quantum PSI-CA protocol, the server only sends a quantum state, $|\varphi_2\rangle$, to the client, without any other classical information. Though the classical information about $f_s(x)$ is embedded into the state $|\varphi_2\rangle$, the client cannot directly extract it from $|\varphi_2\rangle$. Suppose that the whole quantum system of the sate $|\varphi_2\rangle$ consists of two subsystems: the $n$-qubit subsystem $\tilde{C}$ and the 1-qubit ancillary system $\tilde{S}$. For a dishonest client, if he/she makes a projective measurement on the state $|\varphi_2\rangle$, he/she will get $|x\rangle|r \oplus f_s(x)\rangle$ for any $x$ with the probability of $\frac{1}{N}$. Thus, the ancillary system $\tilde{S}$ can be characterized by the quantum ensemble $\mathcal{E} \equiv \{p_x, \rho_{\tilde{S}}(x)\}$, where $p_x = \frac{1}{N}$ and

$$\begin{aligned} \rho_{\tilde{S}}(x) &= Tr_{\tilde{C}}(|x\rangle|r \oplus f_s(x)\rangle\langle r \oplus f_s(x)|\langle x|) \\ &= |r \oplus f_s(x)\rangle\langle r \oplus f_s(x)|. \end{aligned} \tag{42}$$

Furthermore, $|\varphi_2\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle|r \oplus f_s(x)\rangle$, so the ancillary system $\tilde{S}$ can also be described by the following density operator,

$$\begin{aligned} \rho_{\tilde{S}} &= Tr_{\tilde{C}}(|\varphi_2\rangle\langle\varphi_2|) \\ &= \langle 0|\varphi_2\rangle\langle\varphi_2|0\rangle + \langle 1|\varphi_2\rangle\langle\varphi_2|1\rangle + \cdots + \langle N-1|\varphi_2\rangle\langle\varphi_2|N-1\rangle \\ &= \tfrac{N-t}{N}|0\rangle\langle 0| + \tfrac{t}{N}|1\rangle\langle 1|. \end{aligned} \tag{43}$$

That is, $\rho_{\tilde{S}}$ is the average state of the ancillary system $\tilde{S}$. By the Holevo bound [14], we obtain

$$\begin{aligned} I \le \mathcal{X}(\mathcal{E}) &= S(\rho_{\tilde{S}}) - \tfrac{1}{N}\textstyle\sum_{x=0}^{N-1} S(\rho_{\tilde{S}}(x)) \\ &= S(\rho_{\tilde{S}}) \\ &= S\left(\tfrac{N-t}{N}|0\rangle\langle 0| + \tfrac{t}{N}|1\rangle\langle 1|\right), \end{aligned} \tag{44}$$

which attains the maximum value at $t = \frac{N}{2}$. That is,

$$I \le S\left(\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|\right) = 1. \tag{45}$$

It is the upper bound of the client's accessible information from the ancillary system through the measurement. However, the client does not know any prior knowledge about $r$ because it is selected randomly by the server, so $H(r) = 1$ (Please note that $H(\cdot)$ and $S(\cdot)$ denote Shannon entropy and Von Neumann entropy, respectively). That is, it is equivalent to encrypt the classical information $f_s(x)$ by using the random integer $r$ in the one-time pad method. So, only from the state $|\varphi_2\rangle$, the client cannot get any information about $f_s(x)$.

In addition, if the client does not honestly execute this protocol, he can send a fake state $|x\rangle$ to the server, instead of the state $|\varphi_1\rangle$. Accordingly, the returned state from the server will be $|x\rangle|r \oplus f_s(x)\rangle$, not $|\varphi_2\rangle$. Due to the random number $r$, obviously the client can still not get any information about $f_s(x)$.

In short, regardless of the sent states, the client cannot get any secret information about $f_s(x)$ from the returned state accordingly, due to the random number $r$. Therefore, in our proposed quantum PSI-CA protocol, the client learns no information about the set elements of the server except knowing his set size $n_s$, which is public.

**Theorem 3** (***Client Privacy***). In our proposed quantum PSI-CA protocol, the server cannot get any private information about the client's set.

**Proof**. In our proposed quantum PSI-CA protocol, the server only receives the state $|\varphi_1\rangle$ from the client without any classical information. However, the state $|\varphi_1\rangle$, which is fully independent of the client's set, does not carry any private information of the client. Therefore, the server cannot get any private information about the client's set.

In addition, the security of the quantum channel is guaranteed by the decoy-particle checking technology. From Theorem 2 and 3, combined with the security of the quantum channel, it clearly shows that our proposed quantum PSI-CA protocol achieves the unconditional security.

Furthermore, we analyze the security of the proposed anonymous authentication scheme. In general, anonymous authentication has two secure goals: Secure authentication and Anonymity. In the following section, we will prove that our scheme can achieve the two secure goals.

**Theorem 4** (***Secure authentication***). In our proposed anonymous authentication scheme, no unauthorized client can successfully pass the authentication of the server.

**Proof**. If an attacker wants to successfully pass the authentication of the server, he must generate an $n$-element set $C^*$ over $\mathbb{Z}_N$ satisfying $|C^* \cap S| = k$. However, the probability of generating a qualified set $C^*$ is about $\frac{\binom{N/2}{k}\binom{N/2}{n-k}}{\binom{N}{n}}$ (suppose that $|S| = N/2$ and $|\bar{S}| = N/2$), where $0 < k < n \ll N$. For example, if $N = 100$, $k = 2$ and $n = 10$, then $\frac{\binom{50}{2}\binom{50}{8}}{\binom{100}{10}} \approx 0.038$; if $N = 100$, $k = 2$ and $n = 20$, then $\frac{\binom{50}{2}\binom{50}{18}}{\binom{100}{20}} \approx 4.126 \times 10^{-5}$. Therefore, in our proposed anonymous authentication scheme, no unauthorized client can successfully pass the authentication of the server except with very small probability, which is ignorable.

Please note that $n$ and $k$ should be determined by the value of $\frac{\binom{N/2}{k}\binom{N/2}{n-k}}{\binom{N}{n}}$ for a given $N$, such that $\frac{\binom{N/2}{k}\binom{N/2}{n-k}}{\binom{N}{n}}$ is small enough.

**Theorem 5** (***Anonymity***). In our proposed anonymous authentication scheme, the server cannot know any information about the identity of the authenticated client.

**Proof**. The quantum PSI-CA protocol guarantees the anonymity of the proposed anonymous authentication scheme, because the server only know the cardinality of the intersection, but not the set elements of the intersection. Furthermore, the intersection cardinality of any authorized client and the server is equal to the same value, $k$, which is fully independent of his/her identity. Therefore, in our proposed anonymous authentication scheme, the server cannot know any information about the identity of the authenticated client.

Besides achieving two basic secure goals, the proposed anonymous authentication scheme can easily update the authorized clients (i.e., revoke any authorized client or add a new client), where the main computation costs of updating are several set operations. However, in most existing anonymous authentication schemes, revoking an authorized client is a very complex task. Before each authentication it usually needs to add an extra revocation test to check whether the client is in the revocation list, which consumes lots of cryptographic operations.

Finally, we analyze the communication costs of the proposed protocol and scheme. For the quantum PSI-CA protocol, we can easily see that the client and the server only exchange two quantum messages (i.e., $|\varphi_1\rangle$ and $|\varphi_2\rangle$) without any classical message, where the size of each quantum message is about $\log N$ qubits. However, the most efficient classical PSI-CA protocol needs to exchange at least $(n_c + n_s)$ classical messages [7], where the bit length of each classical message is also $\log N$. Compared with these classical protocols with $O(n_c + n_s)$ communication complexity, obviously the communication complexity of our proposed quantum PSI-CA protocol is constant, $O(1)$,

since the number of exchanged messages is independent of the numbers of the set elements, $n_c$ and $n_s$. For the anonymous authentication scheme, the main cost of each authentication is to execute one quantum PSI-CA protocol. Accordingly its communication complexity is also $O(1)$.

## 6. Conclusion

In this paper, we presented an efficient quantum protocol to privately compute the cardinality of set intersection, which is called the quantum PSI-CA protocol. The proposed quantum PSI-CA protocol achieves the unconditional security, which is guaranteed by the basic principle of quantum mechanics. In addition, compared with the classical PSI-CA protocols, the proposed protocol can reduce the communication complexity, since it only requires $O(1)$ communication cost, which is fully independent of the size of the sets. Furthermore, based on the proposed quantum PSI-CA protocol, we constructed a novel anonymous authentication scheme. Similarly, this scheme has the unconditional security in communications, which is guaranteed by the quantum PSI-CA protocol. In addition, there is a good advantage of our proposed scheme that it is very simple to deal with dynamic updating, because it only needs to simply compute several set operations when revoking any authorized client or adding a new client. Thus it is very suitable for applications in large-scale client-server networks or Cloud environments.

**Acknowledgment**

This work was supported by National Natural Science Foundation of China (Nos 61572001, 61173187 and 11301002), the Ministry of Education institution of higher learning doctor discipline and scientific research fund aids a project financially (No.20133401110004), Natural Science Foundation of Anhui Province (No. 1408085QF107), and the 211 Project of Anhui University (Nos 33190187 and 17110099).

## References

[1] M. Boyer, G.Brassard, P. HØyer, and A. Tapp, Tight bounds on quantum searching, http://arxiv.org/abs/quant-ph/9605034. (1996)

[2] G. Brassard, P. HØyer, and A. Tapp, Quantum Counting, in: Proc. 25th ICALP, Springer, LNCS 1443, 1998, pp.820-831.

[3] F. Buccafurri, L. Fotia, G. Lax, V. Saraswat, Analysis-preserving protection of user privacy against information leakage of social-network Likes, Inform. Sci. 328 (2016) 340-358.

[4] J. Camenisch and G. M. Zaverucha, Private Intersection of Certified Sets, in: Proc. 13th International Conference, Financial Cryptography and Data Security (FC 2009), Springer, LNCS 5628, 2009, pp. 108-127.

[5] X.B. Chen, Y. Su, G. Xu, Y. Sun, Y.X. Yang, Quantum state secure transmission in network communications, Inform. Sci. 276 (2014) 363-376.

[6] C.H. Chou, K.Y. Tsai, C.F. Lu, Two ID-based authenticated schemes with key agreement for mobile environments, J. Supercomput. 66 (2013) 973–988.

[7] E.D. Cristofaro, P.Gasti, G. Tsudik, Fast and Private Computation of Cardinality of Set Intersection and Union, in: Proc. Cryptology and Network Security (CANC 2010), Springer, LNCS 7712, 2012, pp. 218-231.

[8] S.K. Debnath, R. Dutta, Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter, in: Proc. Information Security (ISC 2015), Springer, LNCS 9290, 2015, pp. 209-226.

[9] Z.J. Diao, C.F. Huang, K. Wang, Quantum Counting: Algorithm and Error Distribution, Acta Appl Math 118 (2012) 147-159.

[10] M. S. Farash, M. A. Attari, A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks, J. Supercomput. 69 (2014) 395-411.

[11] M.J. Freedman, K. Nissim, B. Pinkas, Efficient Private Matching and Set Intersection, in: Proc. EUROCRYPT, Springer, LNCS 3027, 2004, pp. 1–19.

[12] L. K. Grover, A fast quantum mechanical algorithm for database search, in: Proc. 28th Annual ACM Symposium on Theory of Computing, ACM, 1996, pp.212-219.

[13] S. Hohenberger and S. Weis, Honest-verifier private disjointness testing without random oracles, in: Proc. Privacy Enhancing Technologies (PET 2006), Springer, LNCS 4258, 2006, pp. 277-294.

[14] A. Holevo, Probabilistic and Statistical Aspects of Quantum Theory, Publications of the Scuola Normale Superiore, Springer, 2011.

[15] H.J. Jo, J.H. Paik and D.H. Lee, Efficient Privacy-Preserving Authentication in Wireless Mobile Networks, IEEE Trans. Mob. Comput. 13 (2014) 1469-1481.

[16] L. Kissner and D. Song, Privacy-preserving set operations, in: Proc. Advances in Cryptology - Crypto 2005, Springer, LNCS 3621, 2005, pp. 241-257.
[17] S.D. Li, C.Y. Wu, D.S. Wang, Y.Q. Dai, Secure multiparty computation of solid geometric problems and their applications, Inform. Sci. 282 (2014) 401-413.
[18] J.W. Liu, Z.H. Zhang, X.F. Chen, and K.S. Kwak, Certificateless Remote Anonymous Authentication Schemes for Wireless Body Area Networks, IEEE Trans. Parallel Distrib. Syst. 25 (2014) 332-342.
[19] M. Mosca, Counting by quantum eigenvalue estimation, Theor. Comput. Sci. 264 (2001) 139-153.
[20] M.A. Nielsen & I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, Cambridge, 2010.
[21] Z.G. Qin, H. Xiong, G.B. Zhu, Z. Chen, Certificate-free ad hoc anonymous authentication, Inform. Sci. 268 (2014) 447-457.
[22] R.H. Shi, H. Zhong and L.S. Huang, A novel anonymous authentication scheme without cryptography, Trans. Emerg. Telecomun. Technol. 25 (2014) 875-880.
[23] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in: Proc. 35th Annual Symposium on the Foundations of Computer Science, IEEE, 1994, pp.124-134.
[24] D. Wang, D.B. He, P. Wang, C.H. Chu, Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment, IEEE Trans. Dependable Sec. Comput. 12 (2015) 428-442.
[25] D. Wang, N. Wang, P. Wang, S.H. Qing, Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity, Inform. Sci. 321 (2015) 162-178.
[26] M.E. Wu, S.Y. Chang, C.J. Lu, H.M. Sun, A communication-efficient private matching scheme in Client-Server model, Inform. Sci. 275 (2014) 348-359.
[27] J. Vaidya and C. Clifton, Secure set intersection cardinality with application to association rule mining, J. Comput. Secur. 13 (2005) 593-622.
[28] Z.H. Zhang, J.J. Li, W. Jiang, Y. Zhao, B. Gong, A new anonymous authentication scheme for cloud computing, in: Proc. 7th International Conference on Computer Science and Education (ICCSE), Melbourne, IEEE, 2012, pp. 896-898.