IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 22, 2018, accepted September 15, 2018, date of publication October 1, 2018,
date of current version December 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872741

Efficient Quantum Protocol for Private Set Intersection Cardinality

RUN-HUA SHI
School of Control and Computer Engineering, North China Electric Power University, Beijing 102206, China
Corresponding author: Run-Hua Shi (rhshi@ncepu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 61772001.

ABSTRACT Recently, we proposed a quantum solution to the problem of private set intersection cardinality (PSI-CA) (Information Sciences 370-371 (2016) 147-158). Compared to classical solutions, the proposed quantum PSI-CA protocol achieves an exponential reduction in communication complexity, since it only needs $O(1)$ communication cost. However, this protocol requires two additional assumptions about the cardinalities of the sets, which may limit its wider applications. In this paper, we successfully discard these assumptions and present a stronger quantum PSI-CA protocol without any limitation. The new protocol ensures the parties' private security, i.e., unconditionally secure server privacy and statistically secure client privacy, and it achieves the constant computation and communication complexities, which are independent of the size of the sets. Therefore, it is more suitable for practical applications with big data sets.

INDEX TERMS Quantum computation, quantum communication, secure multi-party computation, private set intersection cardinality.

I. INTRODUCTION

Secure Multi-party Computation (SMC) allows a number of mutually distrustful parties to compute a joint function of their inputs without leaking any information about their respective private inputs [1], [2]. Due to its important military and business values, SMC has raised widespread concerns and has been extensively researched in the cryptographic community, since it was first introduced by Yao [3].

Private Set Intersection Cardinality (PSI-CA) is a primitive of SMC that enables two parties, each with a private set, to jointly compute the cardinality of their intersection without disclosing any private information about their respective sets [4]. There are many important and practical applications of PSI-CA in privacy-preserving and information-sharing settings [5]. For instance, PSI-CA can be used in anonymous authentication [4], authenticating a remote user without revealing his/her identity, e.g., when a remote user requests the server to authenticate his/her legality, the server asks the user to jointly execute a PSI-CA protocol and further verifies whether the intersection cardinality of their respective private sets is equal to a constant, which is assigned by a trusted third party in advance. Moreover, PSI-CA is useful in social networks [6], e.g., when two parties want to privately determine the number of common connections in order to decide whether it exceeds a threshold value and further decide whether or not to become friends, it only needs to jointly run a PSI-CA protocol, where each element of their respective private sets represents a connection. In addition, as an important block, PSI-CA can also be utilized to privately compute the length of the longest common subsequence of two physically separate parties, where the longest common subsequence is the longest common part of two sequences by deleting zero or more characters from two sequences. For example, how to privately determine the similarity of two DNA sequences. Other applications of PSI-CA still include privacy-preserving data mining [7], location sharing [8], the Hamming distance [9], etc.

Due to its important and wide applications, there appeared many PSI-CA protocols [9]–[16] in classical settings. In these existing protocols, the most efficient PSI-CA protocol requires the linear communication complexity [9]. Obviously it is infeasible for new applications involved in Big Data (e.g., DNA sequences). In addition, 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. Especially, most computational assumptions are vulnerable to attack by the quantum computer. Therefore, the researchers for PSI-CA still focus on two important factors: the higher security and the lower communication complexity.

In order to improve the security and reduce the communication complexity, we first tried to solve the PSI-CA problem by using a quantum approach in [4]. Compared to classical solutions, the proposed quantum PSI-CA protocol achieves an exponential reduction in communication complexity, since it only needs $O(1)$ communication cost. However, the proposed quantum PSI-CA protocol requires two additional assumptions about the cardinality of the sets, which limit its wider applications.

In this paper, we further focus on quantum solution to PSI-CA and present an improved quantum protocol for PSI-CA without any assumption, which is suitable for practical applications with big data sets.

II. PRELIMINARIES

A. RELATED WORKS

In 2004, Freedman *et al.* [10] first considered several two-party set-intersection problems and presented private set intersection (PSI) protocols by using homomorphic encryption to evaluate a secret polynomial. In addition, they also first extended the proposed PSI protocols to the corresponding PSI-CA protocols. Subsequently, there appeared many PSI-CA protocols [11]–[16]. Furthermore, in 2012, Cristofaro *et al.* [9] presented a novel PSI-CA protocol with linear computation and communication complexity, which was the most efficient PSI-CA protocol in previously proposed PSI-CA protocols. Cristofaro *et al.* [9] subtly introduced Diffie-Hellman key exchange to blind the private information and further built an efficient PSI-CA protocol based on the difficulty assumption of the discrete logarithm problem, which indeed achieved linear complexities in the size of input sets. However, for some applications with big data sets, even the most efficient PSI-CA protocols are still not efficient enough due to their communication costs, which linearly increase with the size of data sets. Furthermore, the security of these existing PSI-CA protocols is based on unproven difficulty assumptions, which are vulnerable to attack by the quantum computer.

With the advent of fast quantum algorithms [17], [18], classical cryptosystems, including symmetric and asymmetric (i.e., public key) cryptosystems, are facing enormous threatens and challenges. On the other hand, quantum cryptography opens a new era. The security of quantum cryptography is based on the physical principles of quantum mechanics, so it can provide the unconditional security in theory. Since Bennett and Brassard presented the first quantum key distribution protocol [19], quantum cryptography has been widely studied and rapidly developed. Nowadays, a lot of results have been gained, such as quantum teleportation [20], quantum secret sharing [21], quantum secure direct communication [22], quantum signature [23], and so on.

At the same time, SMC was also studied extensively in quantum fields [24]–[26]. However, unfortunately, Lo [27], Colbeck [28] and Buhrman *et al.* [29] pointed out that unconditionally secure two-party quantum computations are impossible. But the existing achievements show that although there is not a perfectly secure two-party quantum computation, quantum protocols can still provide a reasonable security improvement over classical related protocols, such as quantum bit commitment [30] and quantum coin tossing [19].

Recently, we presented a probabilistic two-party quantum protocol computing PSI-CA [4], which can output a good estimator of the intersection cardinality with high probability and small error. Compared with the classical relevant protocols, our proposed quantum PSI-CA protocol has at least two good advantages: higher security and lower communication complexity. Especially, it achieves the communication complexity of $O(1)$, which is fully independent of the size of data sets. However, this protocol requires two additional assumptions: (1) $|C| + |S| < \frac{N}{2}$; (2)$|C|$ and $|S|$ are public, where C and S are the sets of the client and the server, respectively, and all elements of their respective sets belong to $Z_N = \{0, 1, 2, \ldots, N-1\}$. Obviously, these additional assumptions will certainly limit its wider applications. In this paper, we try to discard any unnecessary assumption to build a stronger quantum PSI-CA protocol without losing any good feature of the original protocol [4].

B. PRIVATE SET INTERSECTION CARDINALITY

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

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

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

The above definition gives the stronger privacy requirements than the original definition of [4], because there is no requirement or limitation about $|S|$ and $|C|$.

C. QUANTUM COUNTING

In later proposed quantum PSI-CA protocol, we will follow some ideas from quantum counting. So here we first review quantum counting. In [31], the counting problem is formulated mathematically: given an oracle function

$$f : \{1, 2, 3, \ldots, N\} \to \{0, 1\}, \tag{1}$$

where $N \in \mathbb{N}$, find t, the number of $x \in \{1, 2, 3, \ldots, N\}$ such that $f(x) = 1$. N is known, thus, finding t is equivalent to finding $p = \frac{t}{N}$, the probability of getting an x with $f(x) = 1$ when x is picked randomly. Based on quantum parallelism [4], clearly, the quantum counting approach [4], [31], [32] has higher efficiency than the classical one. In addition, the quantum counting approach achieves much faster convergence rate than the classical one [31]. Furthermore, we simply review

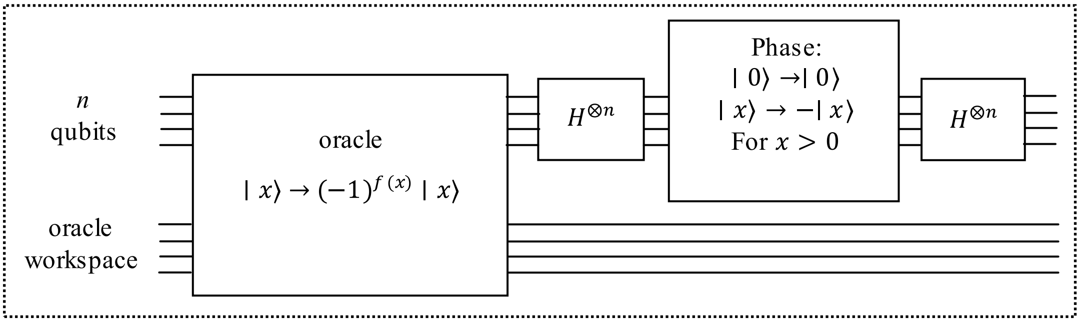
n
qubits
oracle
workspace
oracle
$| x\rangle \rightarrow (-1)^{f(x)} | x\rangle$
$H^{\otimes n}$
Phase:
$| 0\rangle \rightarrow | 0\rangle$
$| x\rangle \rightarrow -| x\rangle$
For $x > 0$
$H^{\otimes n}$

FIGURE 1. Circuit for the Grover iteration, *G*.

Algorithm 1 Quantum Counting Algorithm

```
1. Prepare two registers in the initial state $| \psi_0\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1} | y\rangle\otimes | s\rangle$,where $| s\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} | x\rangle$.
2. Apply $C_F$ on $| \psi_0\rangle$, which implements $| y\rangle\otimes | s\rangle \rightarrow | y\rangle \otimes G^y | s\rangle$. Call the resultant state $| \psi_1\rangle$.
3. Apply $QFT^{-1}$ on the first register of $| \psi_1\rangle$. Call the resultant state $| \psi_2\rangle$.
4. Measure the first register of $| \psi_2\rangle$ to obtain $| x\rangle$ and output $\tilde{p} = sin^2(\frac{x}{M}\pi)$, the quantum estimator of $p$.
```

quantum counting algorithm, and readers may refer to [4], [31], and [32] for details.

In the above algorithm, G is the amplitude amplification operator [4], [15], defined by

$$G = U_s U_f, \tag{2}$$

$$U_f \mid x\rangle = \begin{cases} - \mid x\rangle & if\ f(x) = 1, \\ \mid x\rangle & if\ f(x) = 0, \end{cases} \tag{3}$$

$$U_s = 2 \mid s\rangle\langle s \mid -I, \tag{4}$$

where I is the identity operator. Here, the amplitude amplification operator G is also known as the Grover iteration or Grover operator, whose quantum circuit is illustrated in fig 1 [17]. In addition, QFT^{-1} denotes inverse quantum Fourier transfer, which is defined by,

$$QFT : \ \mid x\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{2\pi i \frac{x}{M} j} \mid j\rangle, \tag{5}$$

$$QFT^{-1} : \ \mid x\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} e^{-2\pi i \frac{x}{M} j} \mid j\rangle. \tag{6}$$

Theorem 1 [4], [31]: $\forall M \in \mathbb{N}$, the quantum counting algorithm outputs $\tilde{p}$ such that $\mid p-\tilde{p} \mid\leq \frac{2\pi}{M}\sqrt{p(1-p)}+\frac{\pi^2}{M^2} \mid 1-2p \mid$ with probability at least $\frac{8}{\pi^2}$.

Corollary 1 [4], [31]: $\forall M \in \mathbb{N}, \mid t-\tilde{t} \mid\leq \frac{2\pi}{M}\sqrt{t(N-t)}+ \frac{\pi^2}{M^2} \mid N-2t \mid$ with probability at least $\frac{8}{\pi^2}$.

III. PROPOSED QUANTUM PSI-CA PROTOCOL

In the following protocol, suppose that the client's private set is C and the server's private set S. Without loss of generality, we assume that all components of the two sets lie in Z_N, where $Z_N = \{0, 1, 2, \ldots, N-1\}$ and $N = 2^n$. The proposed protocol consists of 4 steps, which are described in detail as follows.

IV. ANALYSIS AND COMPARISON

A. CORRECTNESS

By the encoding method, if $i \in C \wedge i \in S$, then $x_i = y_i = 1$. That is, $x_i \cdot y_i = 1$ if $i \in C \cap S$ and $x_i \cdot y_i = 0$ otherwise. So,

$$\mid C \cap S \mid= \sum_{i=0}^{N-1} x_i \cdot y_i. \tag{10}$$

Furthermore, based on the hiding method of the client, we can easily get

$$\begin{aligned} \sum_{i=0}^{N-1} x_i \cdot y_i &= \sum_{i=0}^{N-1}(x_{1,i}+x_{2,i}+\ldots+x_{m,i}) \cdot y_i \\ &= \sum_{i=0}^{N-1} x_{1,i} \cdot y_i + \sum_{i=0}^{N-1} x_{2,i} \cdot y_i \\ &\quad +\ldots+\sum_{i=0}^{N-1} x_{m,i} \cdot y_i. \end{aligned} \tag{11}$$

In addition, in Step 4 of the above proposed protocol, the server outputs $\tilde{t_j} = Nsin^2(\frac{\tilde{x_j}}{M}\pi)$ as an estimator of $\sum_{i=0}^{N-1} x_{j,i} \cdot y_i$. Accordingly, we further prove its correctness as follows:

Suppose that there are t_j components satisfying $x_{j,i} \cdot y_i = 1$ in the state $| \varphi_j\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} | i\rangle \mid x_{j,i}\rangle \mid y_i\rangle \mid x_{j,i} \cdot y_i\rangle$. Thus, $t_j = \sum_{i=0}^{N-1} x_{j,i} \cdot y_i$. Let $| \alpha\rangle = \frac{1}{\sqrt{t_j}}\sum \mid i\rangle \mid x_{j,i}\rangle \mid y_i\rangle \mid 1\rangle$ and $| \beta\rangle = \frac{1}{\sqrt{N-t_j}}\sum \mid i\rangle \mid x_{j,i}\rangle \mid y_i\rangle \mid 0\rangle$. That is,

$$| \varphi_j\rangle = \sqrt{\frac{N-t_j}{N}} \mid \beta\rangle + \sqrt{\frac{t_j}{N}} \mid \alpha\rangle. \tag{12}$$

Choose $\theta \in (0, \frac{\pi}{2})$ such that $sin^2\theta = \frac{t_j}{N}$. Accordingly, $sin\theta = \sqrt{\frac{t_j}{N}}$ and $cos\theta = \sqrt{\frac{N-t_j}{N}}$. So,

$$| \varphi_j\rangle = cos\theta \mid \beta\rangle + sin\theta \mid \alpha\rangle. \tag{13}$$

Algorithm 2 Quantum PSI-CA Protocol

Step 1-Encoding (by two parties)

(1) The client encodes his private set C into a private 0/1 vector $(x_0, x_1, \dots, x_{N-1})$ over F_2^N, where $x_i = 1$ if $i \in C$ and $x_i = 0$ otherwise, for $i = 0, 1, \dots, N-1$.

(2) The server encodes his private set S into a private 0/1 vector $(y_0, y_1, \dots, y_{N-1})$ over F_2^N, where $y_i = 1$ if $i \in S$ and $y_i = 0$ otherwise, for $i = 0, 1, \dots, N-1$.

For example, if $C = \{3, 6, 8, 9, 13\}$ over Z_{16} then $(x_0, x_1, \dots, x_{15}) = (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$, where the number of one in the vector is just equal to the cardinality of the set C.

Step 2-Hiding or secret splitting (by the client)

By the private encoded vector $(x_0, x_1, \dots, x_{N-1})$, the client generates m auxiliary vectors $(x_{1,0}, x_{1,1}, \dots, x_{1,N-1}), (x_{2,0}, x_{2,1}, \dots, x_{2,N-1}), \dots, (x_{m,0}, x_{m,1}, \dots, x_{m,N-1})$ as follows:

For $i = 0, 1, \dots, N-1$, if $x_i = 1$ all $x_{j,i}s$ are equal to 0 (i.e., $x_{1,i} = x_{2,i} = \cdots = x_{m,i} = 0$); if $x_i = 1$, he randomly picks k from the set $\{1, 2, \dots, m\}$, such that $x_{k,i} = 1$, and the other $x_{j,i} = 0 (j \neq k)$. That is, $x_i = \sum_{j=1}^{m} x_{j,i}$ for any i.

For example, $(x_0, x_1, \dots, x_{15}) = (0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0)$

$(x_{1,0}, x_{1,1}, \dots, x_{1,15}) = (0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$

$(x_{2,0}, x_{2,1}, \dots, x_{2,15}) = (0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0)$

$(x_{3,0}, x_{3,1}, \dots, x_{3,15}) = (0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0)$

$(x_{4,0}, x_{4,1}, \dots, x_{4,15}) = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$

Please note that the number of one in all m vectors ($m = 4$ in above example) is equal to the number of one in the original vector $(x_0, x_1, \dots, x_{N-1})$. That is, each digit "1" of the original vector is hided into one of m components. Obviously, the digits of "1" become dilute in each auxiliary vector.

Step 3-Quantum transformation and transmission (by the client)

(1) The client prepares m initial states $|\psi_0\rangle s$, which are all in $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle$.

(2) The client performs an oracle operator U_j on each initial state $|\psi_0\rangle$, which implements $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle$. Let $|\psi_j\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle$ for $j = 1$ to m.

(3) The client sends m quantum states $\{|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_m\rangle\}$ to the server through the quantum channel.

Step 4-Quantum transformation and quantum counting (by the server)

(1) The server performs a similar oracle operator U_s on each received state $|\psi_j\rangle$, which implements $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle |y_i\rangle$. Let $|\phi_j\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle |y_i\rangle$ for $j = 1$ to m.

(2) The server performs another oracle operator U_f on each state $|\phi_j\rangle$, which implements $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle |y_i\rangle \otimes |0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle |y_i\rangle |x_{j,i} \cdot y_i\rangle$. Let $|\varphi_j\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle |y_i\rangle |x_{j,i} \cdot y_i\rangle$ for $j = 1$ to m.

(3) The server runs quantum counting algorithms m times to count the number of the components satisfying $x_{j,i} \cdot y_i = 1$ in each $|\varphi_j\rangle$ as follows:

For $j = 1$ to m

{ Prepare two registers in the initial state $|R_0\rangle = \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1} |y\rangle \otimes |\varphi_j\rangle$.

Apply C_F on $|R_0\rangle$ which implements $|y\rangle \otimes |\varphi_j\rangle \rightarrow |y\rangle \otimes G^y |\varphi_j\rangle$, where G (see Figure 2) is defined by

$$G = U_{\varphi_j} U_{f_1}, \tag{7}$$

$$U_{f_1} |i\rangle |x_{j,i}\rangle |y_i\rangle |x_{j,i} \cdot y_i\rangle = \begin{cases} -|i\rangle |x_{j,i}\rangle |y_i\rangle |x_{j,i} \cdot y_i\rangle & if\ x_{j,i} \cdot y_i = 1 \\ |i\rangle |x_{j,i}\rangle |y_i\rangle |x_{j,i} \cdot y_i\rangle & if\ x_{j,i} \cdot y_i = 0, \end{cases} \tag{8}$$

$$U_{\varphi_j} = 2|\varphi_j\rangle\langle\varphi_j| - I, \tag{9}$$

Similarly, call the resultant state $|R_1\rangle$.

Apply QFT^{-1} on the first register of $|R_1\rangle$. Call the resultant state $|R_2\rangle$.

Measure the first register of $|R_2\rangle$ to obtain $|\tilde{x}_j\rangle$ and output $\tilde{t}_j = N sin^2(\frac{\tilde{x}_j}{M}\pi)$. }

(4) The server computes: $t = \sum_{j=1}^{m} \tilde{t}_j$, which is his final output of the intersection cardinality.

By the definition of the operator G (see Eqs. (7,8,9)), whose quantum circuit is illustrated in Figure 2, it can get,

$$\begin{aligned} G|\beta\rangle = U_{\varphi_j} U_{f_1} |\beta\rangle &= U_{\varphi_j} |\beta\rangle \\ &= (2|\varphi_j\rangle\langle\varphi_j| - I)|\beta\rangle \\ &= 2|\varphi_j\rangle\langle\varphi_j|\beta\rangle - |\beta\rangle \\ &= 2cos\theta|\varphi_j\rangle - |\beta\rangle \\ &= 2cos\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) - |\beta\rangle \\ &= (2cos^2\theta - 1)|\beta\rangle + 2sin\theta cos\theta|\alpha\rangle \\ &= cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle, \end{aligned} \tag{14}$$

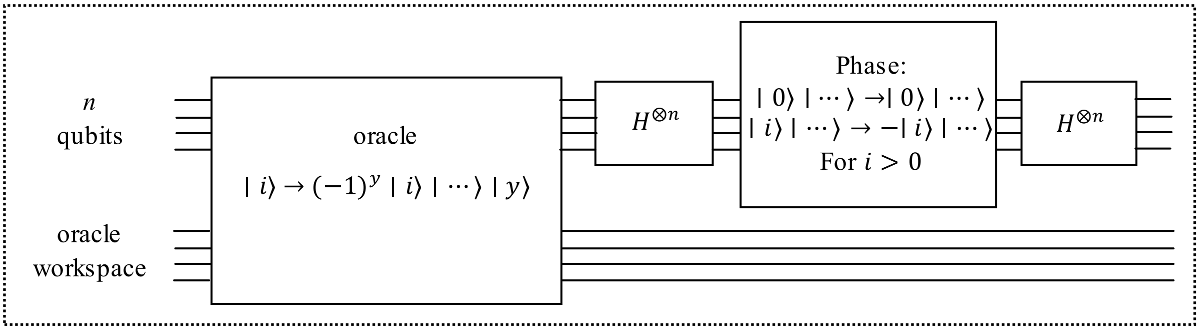
n
qubits
oracle
workspace
oracle
$|i\rangle \rightarrow (-1)^y|i\rangle|\cdots\rangle|y\rangle$
$H^{\otimes n}$
Phase:
$|0\rangle|\cdots\rangle \rightarrow |0\rangle|\cdots\rangle$
$|i\rangle|\cdots\rangle \rightarrow -|i\rangle|\cdots\rangle$
For $i > 0$
$H^{\otimes n}$

FIGURE 2. Circuit for the iteration, *G*, in Step 4.

$$\begin{aligned} G|\alpha\rangle &= U_{\varphi_j}U_{f_1}|\alpha\rangle = U_{\varphi_j}(-|\alpha\rangle)\\ &= (2|\varphi_j\rangle\langle\varphi_j| - I)(-|\alpha\rangle)\\ &= -2|\varphi_j\rangle\langle\varphi_j|\alpha\rangle + |\alpha\rangle\\ &= -2sin\theta|\varphi_j\rangle + |\alpha\rangle\\ &= -2sin\theta(cos\theta|\beta\rangle + sin\theta|\alpha\rangle) + |\alpha\rangle\\ &= -2sin\theta cos\theta|\beta\rangle + (1-2sin^2\theta)|\alpha\rangle\\ &= -sin2\theta|\beta\rangle + cos2\theta|\alpha\rangle. \end{aligned} \tag{15}$$

Furthermore, we define two orthogonal states as follows:

$$|\phi_+\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle), \tag{16}$$

$$|\phi_-\rangle = \frac{1}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle). \tag{17}$$

Then,

$$\begin{aligned} G|\phi_+\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle - iG|\alpha\rangle)\\ &= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle + isin2\theta|\beta\rangle\\ &\quad - icos2\theta|\alpha\rangle)\\ &\quad (by\ Eqs.(14)\ and\ (15))\\ &= \frac{e^{i2\theta}}{\sqrt{2}}(|\beta\rangle - i|\alpha\rangle)\\ &\quad (by\ e^{i2\theta} = cos2\theta + isin2\theta)\\ &= e^{i2\theta}|\phi_+\rangle, \end{aligned} \tag{18}$$

$$\begin{aligned} G|\phi_-\rangle &= \frac{1}{\sqrt{2}}(G|\beta\rangle + iG|\alpha\rangle)\\ &= \frac{1}{\sqrt{2}}(cos2\theta|\beta\rangle + sin2\theta|\alpha\rangle - isin2\theta|\beta\rangle\\ &\quad + icos2\theta|\alpha\rangle)\\ &\quad (\text{by Eqs. (14) and (15)})\\ &= \frac{e^{-i2\theta}}{\sqrt{2}}(|\beta\rangle + i|\alpha\rangle)\\ &\quad (by\ e^{-i2\theta} = cos2\theta - isin2\theta)\\ &= e^{-i2\theta}|\phi_-\rangle. \end{aligned} \tag{19}$$

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 $|\varphi_j\rangle = cos\theta|\beta\rangle + sin\theta|\alpha\rangle = \frac{e^{i\pi\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}}|\phi_-\rangle$.If we apply G to $|\varphi_j\rangle$ for y times, then

$$G^y|\varphi_j\rangle = \frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle + \frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle. \tag{20}$$

Accordingly, we will get

$$\begin{aligned} |R_1\rangle &= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}|y\rangle \otimes G^y|\varphi_j\rangle\\ &= \frac{1}{\sqrt{M}}\sum_{y=0}^{M-1}[|y\rangle \otimes (\frac{e^{i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_+\rangle\\ &\quad + \frac{e^{-i\pi(2y+1)\omega}}{\sqrt{2}}|\phi_-\rangle)]\\ &= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle\\ &\quad + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{-i2\pi y\omega}|y\rangle|\phi_-\rangle\\ &= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum\nolimits_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle\\ &\quad + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum\nolimits_{y=0}^{M-1}e^{i2\pi y(1-\omega)}|y\rangle|\phi_-\rangle. \end{aligned} \tag{21}$$

After applying QFT^{-1} to the first $logM$ qubits of the state $|R_1\rangle$, we have

$$\begin{aligned} &QFT^{-1} \otimes I|R_1\rangle\\ &= QFT^{-1} \otimes I[\frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}|y\rangle|\phi_+\rangle\\ &\quad + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}|y\rangle|\phi_-\rangle]\\ &= \frac{e^{i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y\omega}(QFT^{-1}|y\rangle)|\phi_+\rangle\\ &\quad + \frac{e^{-i\pi\omega}}{\sqrt{2M}}\sum_{y=0}^{M-1}e^{i2\pi y(1-\omega)}(QFT^{-1}|y\rangle)|\phi_-\rangle \end{aligned}$$

$$\begin{aligned}
&= \frac{e^{i\pi\omega}}{\sqrt{2M}} \sum_{y=0}^{M-1} e^{i2\pi y\omega}\Big(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-i2\pi \frac{y}{M}x} \mid x\rangle\Big) \mid \phi_+\rangle \\
&\quad + \frac{e^{-i\pi\omega}}{\sqrt{2M}} \sum_{y=0}^{M-1} e^{i2\pi y(1-\omega)}\Big(\frac{1}{\sqrt{M}} \sum_{x=0}^{M-1} e^{-i2\pi \frac{y}{M}x} \mid x\rangle\Big) \mid \phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2}} \sum_{x=0}^{M-1} \Big\{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega-\frac{x}{M})}\Big\} \mid x\rangle \mid \phi_+\rangle \\
&\quad + \frac{e^{-i\pi\omega}}{\sqrt{2}} \sum_{x=0}^{M-1} \Big\{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y[(1-\omega)-\frac{x}{M}]}\Big\} \mid x\rangle \mid \phi_-\rangle \\
&= \frac{e^{i\pi\omega}}{\sqrt{2}} \mid \tilde{x}_+\rangle \mid \phi_+\rangle + \frac{e^{-i\pi\omega}}{\sqrt{2}} \mid \tilde{x}_-\rangle \mid \phi_-\rangle, \qquad (22)
\end{aligned}$$

where

$$\mid \tilde{x}_+\rangle = \sum_{x=0}^{M-1} \Big\{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y(\omega-\frac{x}{M})}\Big\} \mid x\rangle, \qquad (23)$$

$$\mid \tilde{x}_-\rangle = \sum_{x=0}^{M-1} \Big\{\frac{1}{M} \sum_{y=0}^{M-1} e^{i2\pi y[(1-\omega)-\frac{x}{M}]}\Big\} \mid x\rangle. \qquad (24)$$

If making a measurement on $\mid \tilde{x}_+\rangle$ in the computational basis $\{\mid 0\rangle, \mid 1\rangle, \ldots, \mid M-1\rangle\}$, it will get $\mid x\rangle$ with the probability of $|\frac{1}{M}\sum_{y=0}^{M-1} e^{i2\pi y(\omega-\frac{x}{M})}|^2$, where $P(|\frac{x}{M}-\omega| \leq \frac{1}{M}) > \frac{8}{\pi^2}$ (see Refs. [15], [33]). That is, if we make a measurement on $\mid \tilde{x}_+\rangle$, the probability of getting either $\lfloor M\omega \rfloor$ or $\lceil M\omega \rceil$ is at least $\frac{8}{\pi^2}$, which can provide an estimation for ω within the error $\frac{1}{M}$. Similarly, if we make a measurement on $\mid \tilde{x}_-\rangle$, the probability of getting either $\lfloor M(1-\omega) \rfloor$ or $\lceil M(1-\omega) \rceil$ is at least $\frac{8}{\pi^2}$, which can provide an estimation for $(1-\omega)$ within the error $\frac{1}{M}$.

Since $\theta = \pi\omega$, $t_j = Nsin^2\pi\omega$. Accordingly, for the first case (i.e., $\mid \tilde{x}_+\rangle$), $\omega \approx \frac{\tilde{x}_j}{M}$, so $t_j \approx Nsin^2(\pi\frac{\tilde{x}_j}{M})$, where $\tilde{x}_j$ is the final measurement result of the first $logM$ qubits of the state $\mid R_2\rangle$ in Step 4; for the second case (i.e., $\mid \tilde{x}_-\rangle$), $\omega \approx 1 - \frac{\tilde{x}_j}{M}$, so $t_j \approx Nsin^2(\pi - \pi\frac{\tilde{x}_j}{M}) = Nsin^2(\pi\frac{\tilde{x}_j}{M})$. In both cases, it gives the same estimation of t_j (i.e., $\sum_{i=0}^{N-1} x_{j,i} \cdot y_i$). That is, the single estimation of $\sum_{i=0}^{N-1} x_{j,i} \cdot y_i$ for any j is correct.

To sum up, the proposed quantum PSI-CA protocol ensures the correctness.

B. SECURITY

In the whole protocol proposed above, the server does not send out any quantum or classical message. Clearly, the client cannot get any private information about the server's set. That is, Server Privacy is unconditionally secure. In the following section, we focus on Client Privacy.

In the proposed protocol, the client only sends out m quantum states: $\mid \psi_1\rangle, \mid \psi_2\rangle, \ldots, \mid \psi_m\rangle$, without any classical message, where $\mid \psi_j\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_{j,i}\rangle$ for $j = 1$ to m. Although all classical information about his private vectors is embedded into these states, no one can extract all this information by the physical principles of quantum mechanics. For a dishonest server, he can extract the client's partial private information from these received states by the following possible attacks.

The first attack is to directly make a projective measurement on the state $\mid \psi_j\rangle$ (i.e., $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_{j,i}\rangle$). Accordingly, he will get $\mid x_{j,i}\rangle$ for any i with the probability of $\frac{1}{N}$. If $x_{j,i} = 0$, he cannot get any privacy information of the client because he cannot determine whether x_i is equal to 0, where $x_i = \sum_{i=0}^{m} x_{j,i}$. If $x_{j,i} = 1$, he can deduce that $i \in C$ (i.e., he knows a component of the client's private set). Furthermore, by the encoding and hiding methods, it is clearly shown that the probability of the result of $x_{j,i} = 1$ is $\frac{|C|}{mN}$. Here m is a secure parameter, which can be determined by the client in advance, such that $\frac{|C|}{mN}$ is small enough. It implies that if the server wants to learn a component of the client's private set from one of his received quantum states, the successful probability is very low (i.e., $\frac{|C|}{mN}$) Even if he measures all received quantum states: $\mid \psi_1\rangle, \mid \psi_2\rangle, \ldots, \mid \psi_m\rangle$, the probability of rightly getting r components of the client's set is just $(\frac{|C|}{mN})^r(1-\frac{|C|}{mN})^{(m-r)}$, where $r \leq m$. In fact, the client always can determine a secure parameter m by the size of his private set and the public parameter N, such that the amount of information leakage is small enough. In addition, if the server performs this attack, he will lose the chance to further compute the final result of $|C \cap S|$, due to No-cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state.

The second attack is to count the number of $\mid x_{j,i}\rangle$ satisfying $x_{j,i} = 1$ or 0 in each quantum state $\mid \psi_j\rangle$ by using quantum counting algorithm. Furthermore, the server can get an estimator of $|C|$ in theory. But he cannot get any privacy information about the contents of the client's set C. Similarly, if he performs this attack, he will also lose the opportunity to finally get the intersection cardinality.

In addition, the dishonest server still can perform a more complicated attack that he tries to compute the summation of all received quantum states by the help of a powerful oracle operator, since he knows that the client uses the classical secret splitting technology to hide his private encoded vector. Suppose that there is an oracle operator O, which is defined by,

$$\begin{aligned}
O :& \mid i_1\rangle \otimes \mid i_2\rangle \otimes \cdots \otimes \mid i_m\rangle \otimes \mid 0\rangle \\
&\rightarrow \mid i_1\rangle \otimes \mid i_2\rangle \otimes \cdots \otimes \mid i_m\rangle \otimes \mid i_1 + i_2 + \cdots + i_m\rangle, \qquad (25)
\end{aligned}$$

for any $i_j \in \{0, 1\}$. Then, after applying the oracle operator O on all received quantum states, the dishonest server will get,

$$\begin{aligned}
&O\Big[\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_{1,i}\rangle \otimes \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_{2,i}\rangle \\
&\quad \otimes \cdots \otimes \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1} \mid i\rangle \mid x_{m,i}\rangle \otimes \mid 0\rangle\Big] \\
&= \frac{1}{\sqrt{N^m}} \sum\nolimits_{i_1,i_2,\ldots,i_m} \mid i_1\rangle \mid i_2\rangle \cdots \mid i_m\rangle \mid x_{1,i_1}\rangle \mid x_{2,i_2}\rangle \\
&\quad \cdots \mid x_{m,i_m}\rangle \mid x_{1,i_1} + x_{2,i_2} + \cdots + x_{m,i_m}\rangle. \qquad (26)
\end{aligned}$$

In Eq.26, if $i_1 = i_2 = \cdots = i_m = i$, then $x_{1,i_1} + x_{2,i_2} + \cdots + x_{m,i_m} = x_i$. However, due to the randomness

TABLE 1. The comparison of different protocols.

Protocols	Computation costs	Communication costs	Security		Assumptions
The most efficient classical PSI-CA protocol [9]	$O(\lvert C\rvert + \lvert S\rvert)$	$O(\lvert C\rvert + \lvert S\rvert)$	Server Privacy	***CS***	The difficulty assumption of the discrete logarithm problem
			Client Privacy	***CS***	
			Classical channel	***CS***	
Our recently proposed quantum PSI-CA protocol [4]	$O(1)$	$O(1)$	Server Privacy	***US***	Two additional assumptions: (1) $\lvert C\rvert + \lvert S\rvert < \frac{N}{2}$; (2) $\lvert C\rvert$ and $\lvert S\rvert$ are public.
			Client Privacy	***US***	
			Quantum channel	***US***	
Our new proposed quantum PSI-CA protocol	$O(m)$	$O(m)$	Server Privacy	***US***	**No**
			Client Privacy	***SS***	
			Quantum channel	***US***	

Note. ***CS***, ***US*** and ***SS*** denote computationally secure, unconditionally secure and statistically secure, respectively.

of the measurement, the probability of extracting a private component of the client's encoded vector (i.e., x_i) from the final quantum state in Eq.26 is only $\frac{1}{N^{m-1}}$, which is negligible. Therefore, our proposed protocol can resist this attack. And if the server performs this attack, he will also lose the chance to finally get the intersection cardinality.

We have analyzed the security of proposed protocols in ideal settings. That is, our proposed quantum PSI-CA protocol achieves the unconditional security of Server Privacy and the statistical security of Client Privacy. However, in practical settings, there may be some faults (e.g., noise and error) in the quantum channel and measurement. In order to ensure its security in practical settings, we can use the fault tolerant technologies, such as decoherence-free states and error-correcting code, which were introduced in [33] and [34]. In addition, we can also use the decoy-particle technology [4] to ensure the security of the quantum channel.

C. PERFORMANCE AND COMPARISON

In the proposed protocol, it only requires to transmit m quantum states from the client to the server, and it mainly runs m quantum counting algorithms. Therefore, the computation complexity and the communication complexity are $O(m)$, which is independent of the size of the sets.

On the one hand, the bigger the secure parameter m is, the higher the security of the protocol is. On the other hand, the bigger the parameter m is, the higher the communication costs are. However, $\frac{|C|}{mN} < \frac{1}{m}$, so m is usually a small integer, e.g., $m = 4$ in our above example. Especially, for some applications with small $|C|$, we can let $m = 2$. In general, the size of the server's set is bigger than that of the client's set in many practical applications, e.g., anonymous authentication [4]. Accordingly, we can make $m = 2$ in these applications. Of cause, the client can choose an appropriate parameter m against information leakage by practical requirements. No matter what, m is usually a very small integer, e.g., $m = 2, 3, 4, 5$.

Furthermore, we give a comparison of our new protocol and other related protocols in Table 1. Compared with the most efficient classical PSI-CA protocol with the linear complexity (i.e., $O(|C| + |S|)$), Obviously, our protocol requires lower communication and computation costs, especially in applications with big data sets. In addition, our protocol obtains higher security, because it can resist the attacks of the quantum computer or the adversary with quantum computing power.

Compared with our recently proposed protocol [4], the biggest advantage of our new proposed protocol is to discard two additional assumptions about the cardinalities of two sets, which limits its wider applications. That is, our new protocol does not have any limitation, so it is suitable for any application in theory, including any large size of the sets. Of cause, our new protocol enhances the performance with slightly lower computation and communication complexity.

In addition, we can easily see that the necessary quantum resource, the most complex quantum operator and the most complex quantum measurement in our new proposed quantum PSI-CA protocol are $2n$-qubit entangled state prepared by the client in Step 3, the Grover operator G and the von Neumann measurement in N-dimensional Hilbert space performed by the server in Step 4, respectively. Currently, it is difficult to implement some complicated quantum operators and measurements in high-dimensional Hilbert space. However, there are also lots of great implementation achievements in quantum information processing by the newest reports [35]–[42]. Especially, it can successfully implement the preparing and transmitting multi-qubit entangled states [35], [40], [41]. Therefore, at present, although our protocol only provides a theoretical approach to the PSI-CA problem, we believe that it is possible to implement it in the near future.

V. CONCLUSION

In this paper, we present a stronger quantum PSI-CA protocol without any assumption and limitation. The proposed quantum PSI-CA protocol makes the best of quantum parallelism of quantum encoding and the randomness of quantum measurement, and subtly introduces the classical secret splitting technology, and accordingly it achieves better performances, i.e., the constant computation and communication complexities, the perfect security of Server Privacy and the statistical security of Client Privacy. Furthermore, we hope that our methods can provide some new ideas to solve more secure multi-party computations in future.

REFERENCES

[1] X.-B. Chen, Y. Su, G. Xu, Y. Sun, and Y.-X. Yang, "Quantum state secure transmission in network communications," *Inf. Sci.*, vol. 276, pp. 363–376, Aug. 2014.

[2] S. Li, C. Wu, D. Wang, and Y. Dai, "Secure multiparty computation of solid geometric problems and their applications," *Inf. Sci.*, vol. 282, pp. 401–413, Oct. 2014.

[3] A. C. Yao, "Protocols for secure computations," in *Proc. 23th Annu. Symp. Found. Comput. Sci. (FOCS)*, Nov. 1982, pp. 160–164.

[4] R.-H. Shi, Y. Mu, H. Zhong, S. Zhang, and J. Cui, "Quantum private set intersection cardinality and its application to anonymous authentication," *Inf. Sci.*, vols. 370–371, pp. 147–158, Nov. 2016.

[5] M.-E. Wu, S.-Y. Chang, C.-J. Lu, and H.-M. Sun, "A communication-efficient private matching scheme in Client–Server model," *Inf. Sci.*, vol. 275, pp. 348–359, Aug. 2014.

[6] F. Buccafurri, L. Fotia, G. Lax, and V. Saraswat, "Analysis-preserving protection of user privacy against information leakage of social-network likes," *Inf. Sci.*, vol. 328, pp. 340–358, Jan. 2016.

[7] M. Kantarcioglu, R. Nix, and J. Vaidya, "An efficient approximate protocol for privacy-preserving association rule mining," in *Proc. Adv. Knowl. Discovery Data Mining* (Lecture Notes in Computer Science), vol. 5476. Springer, 2009, pp. 515–524.

[8] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, and D. Boneh, "Location privacy via private proximity testing," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2011. [Online]. Available: https://crypto.stanford.edu/~dabo/pubs/papers/locpriv.pdf

[9] E. De Cristofaro, P. Gasti, and G. Tsudik, "Fast and private computation of cardinality of set intersection and union," in *Cryptology and Network Security—CANC* (Lecture Notes in Computer Science), vol. 7712. Springer, 2012, pp. 218–231.

[10] M. J. Freedman, K. Nissim, and B. Pinkas, "Efficient private matching and set intersection," in *Proc. EUROCRYPT*, in Lecture Notes in Computer Science, vol. 3027. Springer, 2004, pp. 1–19.

[11] J. Camenisch and G. M. Zaverucha, "Private intersection of certified sets," in *Financial Cryptography and Data Security—FC* (Lecture Notes in Computer Science), vol. 5628. Springer, 2009, pp. 108–127.

[12] S. K. Debnath and R. Dutta, "Secure and efficient private set intersection cardinality using Bloom filter," in *Proc. Inf. Secur. (ISC)* in Lecture Notes in Computer Science, vol. 9290. Springer, 2015, pp. 209–226.

[13] S. Hohenberger and S. A. Weis, "Honest-verifier private disjointness testing without random oracles," in *Privacy Enhancing Technology—PET* (Lecture Notes in Computer Science), vol. 4258, Springer, 2006, pp. 277–294.

[14] L. Kissner and D. Song, "Privacy-preserving set operations," in *Advances in Cryptology—CRYPTO* (Lecture Notes in Computer Science), vol. 3621. Springer, 2005, pp. 241–257.

[15] J. Vaidya and C. Clifton, "Secure set intersection cardinality with application to association rule mining," *J. Comput. Secur.*, vol. 13, no. 4, pp. 593–622, 2005.

[16] S. Zander, L. L. H. Andrew, and G. Armitage. (2013). *Scalable Private Set Intersection Cardinality for Capture-Recapture With Multiple Private Datasets*. [Online]. Available: http://caia.swin.edu.au/reports/130930A/CAIA-TR-130930A. pdf

[17] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.

[18] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Nov. 1994, pp. 124–134.

[19] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst., Signal Process.*, Dec. 1984, pp. 175–179.

[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, pp. 1895–1899, 1993.

[21] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 3, p. 1829, 1999.

[22] C. Wang, F.-G. Deng, Y.-S. Li, X.-S. Liu, and G. L. Long, "Quantum secure direct communication with high-dimension quantum superdense coding," *Phys. Rev. A, Gen. Phys.*, vol. 71, no. 4, p. 044305, 2005.

[23] R. J. Collins *et al.*, "Realization of quantum digital signatures without the requirement of quantum memory," *Phys. Rev. Lett.*, vol. 113, no. 4, p. 040502, 2014.

[24] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, "Secure multiparty quantum computation with (only) a strict honest majority," in *Proc. 47th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2006, pp. 249–260.

[25] C. Crépeau, D. Gottesman, and A. Smith, "Secure multi-party quantum computation," in *Proc. 34th Annu. ACM Symp. Theory Comput. (STOC)*, 2002, pp. 643–652.

[26] D. Unruh, "Universally composable quantum multi-party computation," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 6110. Springer, 2010, pp. 486–505.

[27] H.-K. Lo, "Insecurity of quantum secure computations," *Phys. Rev. A, Gen. Phys.*, vol. 56, pp. 1154–1162, 1997.

[28] R. Colbeck, "Impossibility of secure two-party classical computation," *Phys. Rev. A, Gen. Phys.*, vol. 76, no. 6, p. 062308, 2007.

[29] H. Buhrman, M. Christandl, and C. Schaffner, "Complete insecurity of quantum protocols for classical two-party computation," *Phys. Rev. Lett.*, vol. 109, no. 16, p. 160501, 2012.

[30] L. Hardy and A. Kent, "Cheat sensitive quantum bit commitment," *Phys. Rev. Lett.*, vol. 92, no. 15, p. 157901, 2004.

[31] Z. Diao, C. Huang, and K. Wang, "Quantum counting: Algorithm and error distribution," *Acta Appl. Math.*, vol. 118, pp. 147–159, 2012.

[32] G. Brassard, P. Høyer, and A. Tapp, "Quantum counting," in *Proc. 25th ICALP*, in Lecture Notes in Computer Science, vol. 1443. Springer, 1998, pp. 820–831.

[33] Y.-B. Li, S.-J. Qin, Z. Yuan, W. Huang, and Y. Sun, "Quantum private comparison against decoherence noise," *Quantum Inf. Process.*, vol. 12, no. 6, pp. 2191–2205, 2013.

[34] Y.B. Li, T.Y. Wang, H.Y, Chen, M.D. Li, Y.T. Yang, "Fault-tolerate quantum private comparison based on GHZ states and ECC," *Int. J. Theor. Phys.*, vol. 52, no. 8, pp. 2818–2825, 2013.

[35] Y.-H. Chen, Y. Xia, Q.-Q. Chen, and J. Song, "Fast and noise-resistant implementation of quantum phase gates and creation of quantum entangled states," *Phys. Rev. A, Gen. Phys.*, vol. 91, no. 1, p. 012325, 2015.

[36] S. Dogra, A. Dorai, and K. Dorai, "Implementation of the quantum Fourier transform on a hybrid qubit–qutrit NMR quantum emulator," *Int. J. Quantum Inf.*, vol. 13, no. 7, p. 1550059, 2015.

[37] D. Dong, Y.-L. Zhang, C.-L. Zou, X.-B. Zou, and G.-C. Guo, "Scheme for purifying a general mixed entangled state and its linear optical implementation," *Chin. Phys. B*, vol. 24, no. 10, p. 100306, 2015.

[38] W.-A. Li and L.-F. Wei, "One-step implementation of quantum controlled-phase gate via quantum zeno dynamics," *Quantum Inf. Compt.*, vol. 14, nos. 1–2, pp. 137–143, 2014.

[39] Y.-L. Li, J.-S. Huang, and Z.-H. Xu, "Implementation of a remote three-qubit controlled-Z gate via quantum zeno dynamics," *Int. J. Theor. Phys.*, vol. 54, no. 5, pp. 1680–1688, 2015.

[40] H.-W. Liu, F. Wang, H.-R. Li, Y. Deng, and M.-X. Luo, "Optimal bipartite entanglement transfer and photonic implementations," *Opt. Commun.*, vol. 334, pp. 273–279, Jan. 2015.

[41] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, "Experimental quantum multiparty communication protocols," *NPJ Quantum Inf.*, vol. 2, Jun. 2016, Art. no. 16010.

[42] S. Weimann *et al.*, "Implementation of quantum and classical discrete fractional Fourier transforms," *Nature Commun.*, vol. 7, Mar. 2016, Art. no. 11027.

RUN-HUA SHI received the Ph.D. degree from the University of Science and Technology of China in 2011. He is currently a Professor with North China Electric Power University. His current research interests include classical and quantum cryptography, in particular, privacy-preserving multi-party computation.