entropy

MDPI

Article

A New Quantum Private Protocol for Set Intersection Cardinality Based on a Quantum Homomorphic Encryption Scheme for Toffoli Gate

Wen Liu [1,2,3,*,†], Yangzhi Li [2,†], Zhirao Wang [2,†] and Yugang Li [4]

[1] State Key Laboratory of Media Convergence and Communication, Communication University of China, Beijing 100024, China
[2] School of Computer and Cyber Sciences, Communication University of China, Beijing 100024, China
[3] Key Laboratory of Convergent Media and Intelligent Technology, Communication University of China, Ministry of Education, Beijing 100034, China
[4] Academy of Broadcasting Science, Beijing 100045, China
* Correspondence: lw_8206@163.com
† These authors contributed equally to this work.

Abstract: Set Intersection Cardinality (SI-CA) computes the intersection cardinality of two parties' sets, which has many important and practical applications such as data mining and data analysis. However, in the face of big data sets, it is difficult for two parties to execute the SI-CA protocol repeatedly. In order to reduce the execution pressure, a Private Set Intersection Cardinality (PSI-CA) protocol based on a quantum homomorphic encryption scheme for the Toffoli gate is proposed. Two parties encode their private sets into two quantum sequences and encrypt their sequences by way of a quantum homomorphic encryption scheme. After receiving the encrypted results, the semi-honest third party (TP) can determine the equality of two quantum sequences with the Toffoli gate and decrypted keys. The simulation of the quantum homomorphic encryption scheme for the Toffoli gate on two quantum bits is given by the IBM Quantum Experience platform. The simulation results show that the scheme can also realize the corresponding function on two quantum sequences.

Keywords: private set intersection cardinality; Pauli gates; Toffoli gate; quantum homomorphic encryption

Citation: Liu, W.; Li Y.; Wang, Z; Li Y. A New Quantum Private Protocol for Set Intersection Cardinality Based on a Quantum Homomorphic Encryption Scheme for Toffoli Gate. *Entropy* **2023**, *25*, 516. https://doi.org/10.3390/e25030516

Academic Editor: Guilu Long

Received: 20 February 2023
Revised: 4 March 2023
Accepted: 13 March 2023
Published: 16 March 2023

1. Introduction

Secure multiparty computation (SMC) [1–3] is a crucial cryptographic primitive which fits the following description: Assume that there is a function typically specified by a map $\mathcal{F}: (\{0,1\}^*)^n \to (\{0,1\}^*)^n$ and a set of n parties, $\mathcal{P} = \{P_1, ..., P_n\}$, who want to compute values of this function with respect to their private data. Each party P_i has its input $x_i \in \{0,1\}^*$ and output $y_i \in \{0,1\}^*$, following correspondence $y_i = \mathcal{F}(x_i)$. Our target is to ensure that all parties in a subset $\mathcal{C} \subset \mathcal{P}$ receive correct outputs from others while no information related to the input can be accessed. SMC has raised widespread concerns and has wide applications in electronic voting, cloud computing, online auction, etc.

A typical SMC [4] application is Private Set Intersection (PSI), which also known as Private Matching (PM). Specifically, PSI permits two parties, P_1 and P_2, who respectively have a private set x_1 and x_2. Without disclosing any information that does not belong to this intersection, they seek to find the intersection $x_1 \cap x_2$. There have been many applications of PSI, such as privacy-preserving data mining [5], data outsourcing on cloud [6], location-based privacy-preserving sharing [7], testing of fully-sequenced human genomes [8], proximity testing [9], and other online services [10].

Due to the extensive and important applications, there have been many suggestions for PSI protocols. In 2004, Freedman et al. [4] first gave the definition of PSI and presented

several PSI protocols by using homomorphic encryption and balanced hashing. Homomorphic encryption was first proposed by Rivest et al. in 1978 [11]. A new symmetric homomorphic functional encryption using modular multiplications over a hidden ring was proposed [12]. Then, some PSI protocols were proposed based on classical cryptography [13–16]. However, PSI reveals too much private information and it cannot meet the higher privacy requirements in some scenarios. In this case, Private Set Intersection Cardinality (PSI-CA) [17] was introduced, which can securely determine the size of set intersection and can be used to generate association rules. In [18], a PSI-CA protocol was the first to achieve security in the standard model under the Quadratic Residuosity QR assumption with linear complexities, which can hide the size of the client's private set. In [19], a PSI-CA protocol was proposed, which had linear computation and communication complexities and was the most efficient PSI-CA protocol in previously proposed PSI-CA protocols [18,19]. PSI-CA only outputs the intersection cardinality and does not reveal the specific content of the intersection. The security of classical PSI-CA protocols is based on the computational complexity assumptions, which are vulnerable to attack by the quantum algorithms [20–22].

On the other hand, scholars began to seek a quantum approach to solving the PSI-CA problem. In [23], Shi et al. presented two quantum protocols to solve the Oblivious Set-member Decision problem. These protocols can be used to privately compute multi-party set intersection and union in the quantum domain. In [24], Shi et al. informally gave a definition of PSI first. Then they presented a quantum scheme for PSI based on n encoded states, n quantum operators, and n von Neumann measurements. In [25], Arpita gave a two-party protocol for computing set intersection securely in the quantum domain in a rational setting, where the players are trying to maximize their utilities. However, PSI reveals too much private personal information in some scenarios. In order to prevent revealing the specific content, Shi et al. proposed some quantum protocols of PSI-CA [26–28]. PSI-CA and PSU-CA enable two parties, each with a private set, to jointly compute the cardinality of their intersection or union without disclosing any private information about their respective sets. These protocols are useful in social networks and for privacy-preserving data mining.

In this paper, following the idea in [26], we propose a PSI-CA protocol based on a quantum homomorphic encryption scheme for the Toffoli gate. With the help of a semi-honest TP, two parties can use this protocol to privately obtain the number of all their private sets' common elements. When the amount of data is large, two parties, which do not have strong quantum computing capabilities, only prepare and encrypt quantum single-particle states. The role of semi-honest TP is to execute the protocol loyally and record all the results of its intermediate computations. However, the TP cannot learn anything about the private information. In our protocol, the semi-honest third party (TP) can be used to perform Toffoli gate and decryption operations. It will keep a record of all its intermediate results and might try to infer the private inputs from the record. Our protocol is simpler and easier to implement.

This paper is organized as follows: we introduce some correlative preliminaries in Section 2; we propose a quantum PSI-CA protocol in Section 3; in Section 4, we analyze the correctness and security of our protocol and describe the implementation of our protocols on the IBM Quantum Experience platform. A brief discussion and the concluding summary are given in Section 5.

2. Preliminary

2.1. Pauli Gates

Some operators are introduced first. Four single-qubit operators I, X, Y, Z are shown as follows:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1. \end{bmatrix} \tag{1}$$

The circuit symbols for the four single-qubit gates I, X, Y, Z are shown in Figure 1.

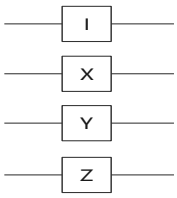

Figure 1. The circuit symbols for the four single-qubit gates, I, X, Y, Z.

2.2. Quantum Toffoli Gate

The quantum Toffoli gate (called the T gate) is seen as an important component in the theory of quantum computation. The unitary transform matrix of the T gate is as follows:

$$T = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{2}$$

The T gate has three input bits and three output bits. For a three-qubit quantum system, $|a\rangle|b\rangle|c\rangle$, the quantum T gate will act as:

$$T|a\rangle|b\rangle|c\rangle = |a\rangle|b\rangle|c \oplus (a \cdot b)\rangle. \tag{3}$$

The circuit symbol for the T gate is shown in Figure 2.

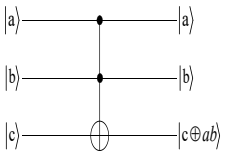

Figure 2. The circuit symbol for the T gate.

2.3. Information-Theoretic Security

In [23], the conception of mixed states is introduced and a quantum information-theoretic security criterion for a quantum protocol is given as follows:

The protocol is informationally secure for every input state φ_{in} if the output state φ_{out} is the totally mixed state. The relation of the input state φ_{in} and the output state φ_{out} is as follows:

$$\varphi_{out} = \sum_k \frac{1}{2^{2n}} U_k \varphi_{in} (U_k)^\dagger = \frac{1}{2^n} I_{2^n}, \tag{4}$$

where φ_{in} is the density operator of all possible n-qubit input states and U_k are the corresponding unitary operations applied on input state.

3. Quantum Private Computation Protocol for Set Intersection Cardinality

We use the definition of PSI-CA [19]. Suppose that there are two parties, Alice and Bob. They input a private set $S_A = \{a_1, a_2, ..., a_{n_1}\}$ and $S_B = \{b_1, b_2, ..., b_{n_2}\}$, respectively. S is a complete set $\{x_1, x_2, ..., x_n\}$ and $S_A, S_B \subset S$. After running the PSI-CA protocol with a help of the semi-honest third party, Calvin, Alice and Bob output the cardinality of the

intersection of their private sets, i.e., $|S_A \cap S_B|$, without leaking any information about their sets. The quantum scheme for PSI-CA is described as follows:

(1) Alice and Bob each prepare a $(n+n')$-photon sequence, denoted by $Sq_A = (|\psi_1^A\rangle, |\psi_2^A\rangle, ..., |\psi_{n+n'}^A\rangle), Sq_B = (|\psi_1^B\rangle|\psi_2^B\rangle, ..., |\psi_{n+n'}^B\rangle)$. The first n particles of Sq_A, Sq_B are prepared according to Alice's and Bob's private sets S_A, S_B:

$$\begin{cases} |\psi_i^A\rangle = |1\rangle, & if\ x_i \in S_A \\ |\psi_i^A\rangle = |0\rangle, & if\ x_i \notin S_A \end{cases} \qquad \begin{cases} |\psi_i^B\rangle = |1\rangle, & if\ x_i \in S_B \\ |\psi_i^B\rangle = |0\rangle, & if\ x_i \notin S_B \end{cases} \tag{5}$$

The last n' particles of Sq_A, Sq_B are dummy photons, which are randomly chosen from $\{|0\rangle, |1\rangle\}$.

(2) Alice and Bob work together to find the number of $|\psi_i^A\rangle = |\psi_i^B\rangle = |1\rangle (i = n+1, ..., n+n^{'})$, denoted by $N_{CA}^{'}$,which means how many bits are equal and equal to $|1\rangle$ in the last n' particles of Sq_A, Sq_B.

They also permutate Sq_A, Sq_B using the same permutation regulation π. The new sequences are denoted by $Sq_A^{'} = (|\psi_1^{A'}\rangle, |\psi_2^{A'}\rangle, ..., |\psi_{n+n'}^{A'}\rangle), Sq_B^{'} = (|\psi_1^{B'}\rangle, |\psi_2^{B'}\rangle, ..., |\psi_{n+n'}^{B'}\rangle)$.

Each of them chooses a sequence, $L_A = (l_1^A, l_2^A, l_3^A, l_4^A, ..., l_{2(n+n')-1}^A, l_{2(n+n')}^A)(L_B = (l_1^B, l_2^B, l_3^B, l_4^B, ..., l_{2(n+n')-1}^B, l_{2(n+n')}^B))$, where l_{2k-1}^B, l_{2k}^B are randomly chosen from $\{0, 1\}$. Then, she(he) uses the Quantum One-time Pad algorithm (QOTP) [25] to encrypt the kth particle of $Sq_A^{'}(Sq_B^{'})$ and get $Z^{l_{2k-1}^A} X^{l_{2k}^A} |\psi_k^A\rangle\ (Z^{l_{2k-1}^B} X^{l_{2k}^B} |\psi_k^B\rangle)$. The new particles sequence is denoted by $S_A^{''} = (Z^{l_1^A} X^{l_2^A} |\psi_1^{A'}\rangle, ..., Z^{l_{2(n+n')-1}^A} X^{l_{2(n+n')}^A} |\psi_{n+n'}^{A'}\rangle)(S_B^{''} = (Z^{l_1^B} X^{l_2^B} |\psi_1^{B'}\rangle, ..., Z^{l_{2(n+n')-1}^B} X^{l_{2(n+n')}^B} |\psi_{n+n'}^{B'}\rangle))$.

Alice (Bob) also inserts some checking particles, which are randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, into $S_A^{''}(S_B^{''})$ and sends the new sequence $S_A^{'''}(S_B^{'''})$ to the third party Calvin.

After that, Alice(Bob) transmits the insert positions $Po_A(Po_B)$ and $L_A(L_B)$ to Calvin using the quantum secure direct communication (QSDC) protocol. QSDC is one of the most important branches of quantum communication and it directly transmits secret messages.

(3) After receiving $S_A^{'''}, S_B^{'''}$, Alice, Bob, and Calvin perform the eavesdropping check using the insert positions Po_A, Po_B and the measuring bases of checking particles. If the error rate exceeds the threshold they preset, they abort the scheme. Otherwise, they discard the measured photons in $S_A^{'''}, S_B^{'''}$ and Calvin gets two sequences $S_A^{''} = (Z^{l_1^A} X^{l_2^A} |\psi_1^{A'}\rangle, ..., Z^{l_{2(n+n')-1}^A} X^{l_{2(n+n')}^A} |\psi_{(}n+n')^{A'}\rangle), S_B^{''} = (Z^{l_1^B} X^{l_2^B} |\psi_1^{B'}\rangle, ..., Z^{l_{2(n+n')-1}^B} X^{l_{2(n+n')}^B} |\psi_{(}n+n')^{B'}\rangle)$.

Calvin prepares a sequence $S_C = (|\psi_1^C\rangle, |\psi_2^C\rangle, ..., |\psi_{n+n'}^C\rangle)$, where $|\psi_i^C\rangle$ is randomly chosen from $\{|0\rangle, |1\rangle\}$.

(4) Calvin executes some operations on the ith quantum bits of $S_A^{''}, S_B^{''}, S_C$ and gets:

$$\begin{aligned} &|\psi_i^{A''}\rangle_1 |\psi_i^{B''}\rangle_2 |\psi_i^{C'}\rangle_3 \\ &= (CNOT_{1,3}^{l_{2i}^B} \otimes I_2)(I_1 \otimes CNOT_{2,3}^{l_{2i}^A})(Z^{l_{2i-1}^A} X^{l_{2i}^A} \otimes Z^{l_{2i-1}^B} X^{l_{2i}^B} \otimes X^{l_{2i}^A l_{2i}^B}) T (Z^{l_{2i-1}^A} X^{l_{2i}^A} \otimes Z^{l_{2i-1}^B} X^{l_{2i}^B} \otimes I) |\psi_i^{A'}\rangle_1 |\psi_i^{B'}\rangle_2 |\psi_i^C\rangle_3 \\ &= |\psi_i^{A'}\rangle_1 |\psi_i^{B'}\rangle_2 |\psi_i^C \oplus \psi_i^{A'} \psi_i^{B'}\rangle_3. \end{aligned} \tag{6}$$

Calvin measures $|\psi_i^{C'}\rangle$ using the X basis and compares the measurement result with $|\psi_i^C\rangle$. He also counts how many quantum bits $|\psi_i^{C'}\rangle, |\psi_i^C\rangle$ are different and the number is denoted by $N_{CA''}$. It is obvious that the intersection cardinality of S_A, S_B is equal to $N_{CA''} - N_{CA'}$.

We have to point out that if Alice and Bob apply a NOT gate on each particle of Sq_A, Sq_B in step(1), the private set union cardinality of S_A, S_B is equal to $|S| - (N_{CA''} - N_{CA'})$ using the PSI-CA quantum protocol.

4. Analysis and Comparison

4.1. Correctness Analysis

In this section, we illustrate the correctness of our protocol. Figure 3 describes the circuit U used to privately apply the T gate on $|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle$, where $l_{2i-1}^A, l_{2i}^A, l_{2i-1}^B, l_{2i}^B \in \{0,1\}$. For $i = 1, 2, ..., n+n'$, Alice, Bob and Calvin can use the circuit U to privately calculate $T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle$. If $|\psi_i^C\rangle$ is reversed, they can determine $|\psi_k^A\rangle = |\psi_k^B\rangle = |1\rangle$.

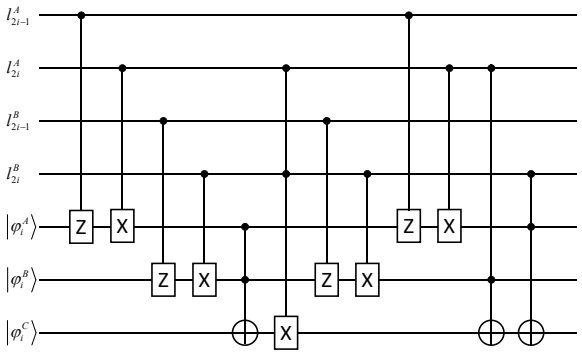

Figure 3. The circuit U used to privately calculate $T|\psi_k^A\rangle|\psi_k^B\rangle|\psi_k^C\rangle$.

According to the circuit U, it can be verified that

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^0X^0 \otimes Z^0X^0 \otimes X^0)T(Z^0X^0 \otimes Z^0X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle. \tag{7}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^0X^0 \otimes Z^1X^0 \otimes X^0)T(Z^0X^0 \otimes Z^1X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle. \tag{8}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^1X^0 \otimes Z^0X^0 \otimes X^0)T(Z^1X^0 \otimes Z^0X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{9}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^1X^0 \otimes Z^1X^0 \otimes X^0)T(Z^1X^0 \otimes Z^1X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle. \tag{10}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^1)(Z^0X^1 \otimes Z^0X^0 \otimes X^0)T(Z^0X^1 \otimes Z^0X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle\left|\psi_i^{B'}\right\rangle|\psi_i^C\rangle \tag{11}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^1)(Z^0X^1 \otimes Z^1X^0 \otimes X^0)T(Z^0X^1 \otimes Z^1X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{12}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^1)(Z^1X^1 \otimes Z^0X^0 \otimes X^0)T(Z^1X^1 \otimes Z^0X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{13}$$

$$(CNOT_{1,3}^0 \otimes I_2)(I_1 \otimes CNOT_{2,3}^1)(Z^1X^1 \otimes Z^1X^0 \otimes X^0)T(Z^1X^1 \otimes Z^1X^0 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{14}$$

$$(CNOT_{1,3}^1 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^0X^0 \otimes Z^0X^1 \otimes X^0)T(Z^0X^0 \otimes Z^0X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{15}$$

$$(CNOT_{1,3}^1 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^0X^0 \otimes Z^1X^1 \otimes X^0)T(Z^0X^0 \otimes Z^1X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{16}$$

$$(CNOT_{1,3}^1 \otimes I_2)(I_1 \otimes CNOT_{2,3}^0)(Z^1X^0 \otimes Z^0X^1 \otimes X^0)T(Z^1X^0 \otimes Z^0X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \tag{17}$$

$$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^0_{2,3})(Z^1X^0 \otimes Z^1X^1 \otimes X^0)T(Z^1X^0 \otimes Z^1X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \quad (18)$$

$$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^0X^1 \otimes Z^0X^1 \otimes X^1)T(Z^0X^1 \otimes Z^0X^1 \otimes I)|\psi_i^A\rangle\left|\psi_i^{B'}\right\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \quad (19)$$

$$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^0X^1 \otimes Z^1X^1 \otimes X^1)T(Z^0X^1 \otimes Z^1X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \quad (20)$$

$$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^1X^1 \otimes Z^0X^1 \otimes X^1)T(Z^1X^1 \otimes Z^0X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = -T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \quad (21)$$

$$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^1X^1 \otimes Z^1X^1 \otimes X^1)T(Z^1X^1 \otimes Z^1X^1 \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle = T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle. \quad (22)$$

According to Equations (7)–(22), we can obtain

$$\begin{aligned}&(CNOT^{I^B_{2i}}_{1,3} \otimes I_2)(I_1 \otimes CNOT^{I^A_{2i}}_{2,3})(Z^{I^A_{2i-1}}X^{I^A_{2i}} \otimes Z^{I^B_{2i-1}}X^{I^B_{2i}} \otimes X^{I^A_{2i}I^B_{2i}})T(Z^{I^A_{2i-1}}X^{I^A_{2i}} \otimes Z^{I^B_{2i-1}}X^{I^B_{2i}} \otimes I)|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \\ &= T|\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C\rangle \\ &= |\psi_i^A\rangle|\psi_i^B\rangle|\psi_i^C \oplus (\psi_i^A \cdot \psi_i^B)\rangle.\end{aligned} \quad (23)$$

Calvin measures $\left|\psi_i^C \oplus \left(\psi_i^{A'} \cdot \psi_i^{B'}\right)\right\rangle$. If $\left|\psi_i^C \oplus \left(\psi_i^{A'} \cdot \psi_i^{B'}\right)\right\rangle$ is different from $|\psi_i^C\rangle$, we can know $\left|\psi_i^{A'}\right\rangle = \left|\psi_i^{B'}\right\rangle = |1\rangle$. Alice and Bob have a common element in S_A, S_B.

Suppose that the private set of Alice is $S_A = \{2,4\}$ and the private set of Bob is $S_B = \{3,4\}$ where a complete set is $S = \{2,3,4\}$. The photon sequence of Alice is $S_{q_A} = \{|1\rangle, |0\rangle, |1\rangle\}$ and the photon sequence of Bob is $S_{q_B} = \{|0\rangle, |1\rangle, |1\rangle\}$. Calvin prepares a sequence $S_{q_C} = \{|1\rangle, |0\rangle, |0\rangle\}$. Alice chooses a sequence $L_A = (0,1,1,1,1,0)$ and Bob chooses a sequence $L_B = (0,0,1,1,0,1)$. Alice, Bob and Calvin perform some operations on $\{|1\rangle, |0\rangle, |1\rangle\}, \{|0\rangle, |1\rangle, |1\rangle\}, \{|1\rangle, |0\rangle, |0\rangle\}$ using L_A, L_B and get $(CNOT^0_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^0X^1 \otimes Z^0X^0 \otimes X^0)T(Z^0X^1 \otimes Z^0X^0 \otimes I)|1\rangle|0\rangle|1\rangle$, $(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^1_{2,3})(Z^1X^1 \otimes Z^1X^1 \otimes X^1)T(Z^1X^1 \otimes Z^1X^1 \otimes I)|0\rangle|1\rangle|0\rangle$,$(CNOT^1_{1,3} \otimes I_2)(I_1 \otimes CNOT^0_{2,3})(Z^1X^0 \otimes Z^0X^1 \otimes X^0)T(Z^1X^0 \otimes Z^0X^1 \otimes I)|1\rangle|1\rangle|0\rangle$. Then they can get $T(|1\rangle|0\rangle|1\rangle), T(|0\rangle|1\rangle|0\rangle), T(|1\rangle|1\rangle|0\rangle)$ and the new photon sequence of Calvin is $|1 \oplus (1 \cdot 0)\rangle|0 \oplus (0 \cdot 1)\rangle|0 \oplus (1 \cdot 1)\rangle$. Only the third photon in Calvin's new sequence $|0 \oplus (1 \cdot 1)\rangle = |1\rangle\}$ is different from the third photon of his original sequence $|0\rangle\}$. So we can get that Alice and Bob have only one common element in S_A, S_B.

4.2. Implementation of Quantum PSI-CA Protocols on IBM Quantum Experience Platform

Now, we move forward through a similar approach to experimentally realize our PSI-CA protocol on the IBM Quantum Experience platform. Let us say the two parties, Alice and Bob, have a private set S_A and S_B, respectively, where S is a complete set and $S_A, S_B \in S$. For the encoding procedure, S_A and S_B are encoded into two $(n+n')$-particle sequences. Alice, Bob, and Calvin can privately apply the T gate on their corresponding position particles using the IBM Quantum Experience platform. The measuring results of Calvin's particle are related to the PSI-CA of S_A, S_B.

The circuit on the IBM Quantum Experience platform for privately computing for eight cases of $T|\psi_{A0}\rangle|\psi_{B0}\rangle|\psi_{C0}\rangle$ and the experiment results with 1024 shots for eight cases on the quantum circuit are shown in Figures 4–11. In the experiment results' figures, the x-axis represents 16 measurement results, and each of them includes the $T|\psi_{A0}\rangle|\psi_{B0}\rangle|\psi_{C0}\rangle$ and the information of $l_{A0}, l_{A1}, l_{B0}, l_{B1}$.The y-axis represents the frequency of each measurement result. The first three binary bits in the x-axis correspond to the output of $T|\psi_{A0}\rangle|\psi_{B0}\rangle|\psi_{C0}\rangle$ and the following four binary bits in the x-axis are $l_{A0}, l_{A1}, l_{B0}, l_{B2}$.

In Figure 4, $|\psi_{A0}\rangle = |1\rangle, |\psi_{B0}\rangle = |1\rangle, |\psi_{C0}\rangle = |1\rangle$. Take the measurement results "1101010", for example, in Figure 4, the last four bits 1010 represent the measurement results of $l_{A0}, l_{A1}, l_{B0}, l_{B1}$, which are used to control the gates in the quantum circuit. The first three bits 110 represent the new measurement result of $|\psi_{A0}\rangle, |\psi_{B0}\rangle, |\psi_{C0}\rangle$ after operating the gates in the quantum circuit. From the frequency of each measurement result in Figure 4, it can be verified that no matter what the $l_{A0}, l_{A1}, l_{B0}, l_{B1}$ is, the circuit will act as a T gate on $|\psi_{A0}\rangle = |1\rangle, |\psi_{B0}\rangle = |1\rangle, |\psi_{C0}\rangle = |1\rangle$. Using the same analysis method, we can reach the same conclusion from the frequency of each measurement result in Figures 5–11.

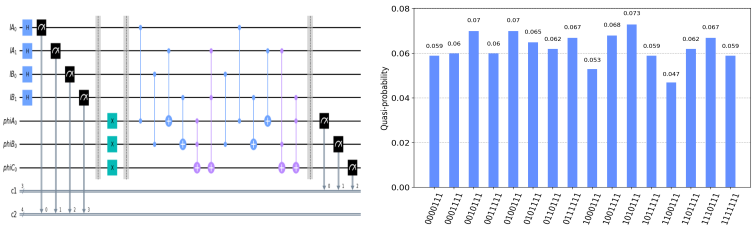

Figure 4. The circuit used to privately calculate $T|1\rangle|1\rangle|1\rangle$ and the experiment results.

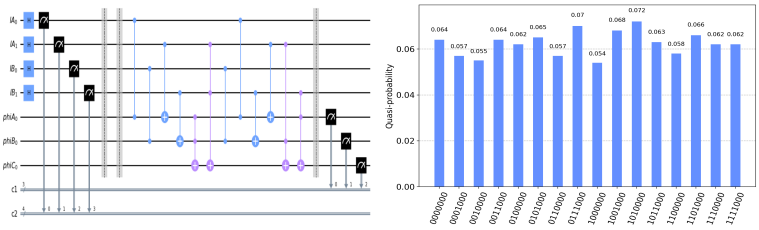

Figure 5. The circuit used to privately calculate $T|0\rangle|0\rangle|0\rangle$ and the experiment results.

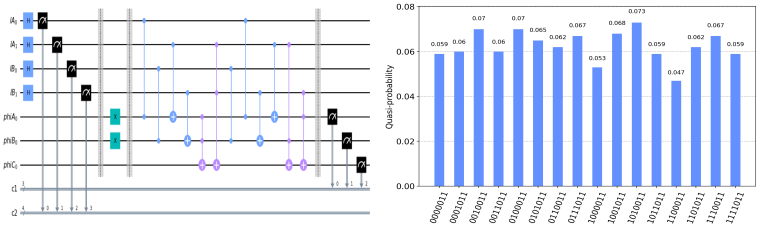

Figure 6. The circuit used to privately calculate $T|1\rangle|1\rangle|0\rangle$ and the experiment results.

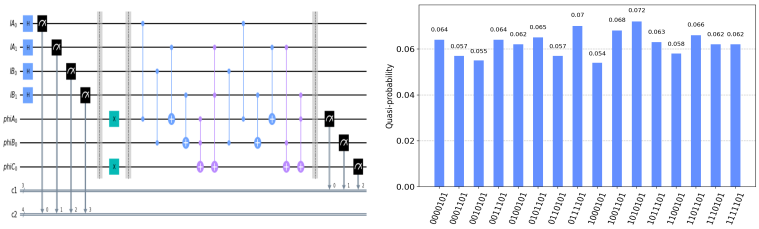

Figure 7. The circuit used to privately calculate $T|1\rangle|0\rangle|1\rangle$ and the experiment results.

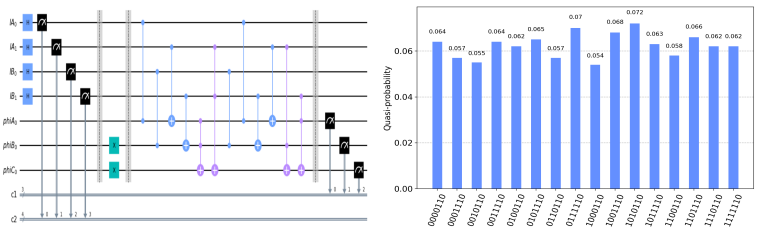

Figure 8. The circuit used to privately calculate $T|0\rangle|1\rangle|1\rangle$ and the experiment results.

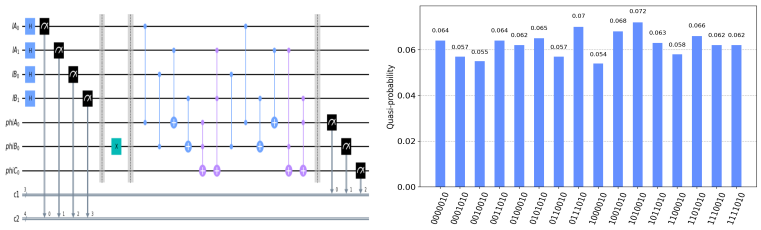

Figure 9. The circuit used to privately calculate $T|0\rangle|1\rangle|0\rangle$ and the experiment results.

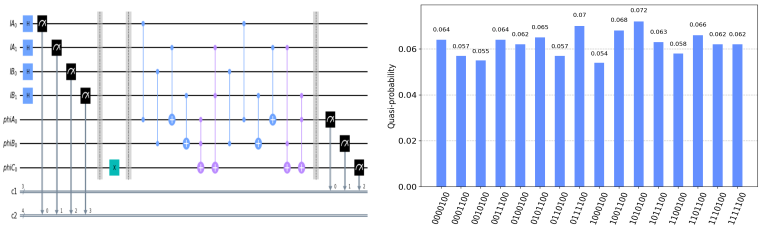

Figure 10. The circuit used to privately calculate $T|0\rangle|0\rangle|1\rangle$ and the experiment results.

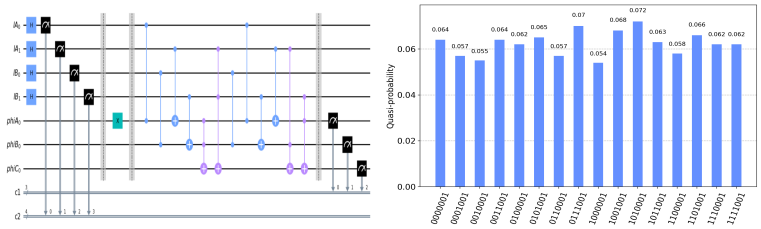

Figure 11. The circuit used to privately calculate $T|1\rangle|0\rangle|0\rangle$ and the experiment results.

4.3. Security Analysis

In this section, we verify the security of our quantum PSI-CA scheme by analyzing an external outside attack and a participant attack, respectively.

4.3.1. Outside Attacks

In terms of outside attacks, this protocol allows for outside eavesdroppers to attack the quantum channel and obtain Alice and Bob's particle sequences in step (2). Checking particles are introduced to to defend against it. With several checking particles inserted, the security checking procedure in Step (3) can detect the intercept–resend attack, the measurement–resend attack, the entanglement–measure attack, and the denial-of-service (DOS) attack with a nonzero probability.

In addition to this naive attack, there are some special forms of attack such as the delay photon Trojan horse attack, the invisible photon eavesdropping (IPE) Trojan horse attack, and the photon-number-splitting (PNS) attack, which are also available to outside eavesdroppers. In response to these attacks, we use several defenses. To defeat the delay-photon Trojan horse attack, we can use a photon-number splitter. To defeat the IPE attack, we can insert filters in front of their devices to filter out the photon signal with an illegitimate wavelength. To defeat the PNS attack, we can use the technology of beam splitters to split the sampling signals and judge whether these received photons are single photons or multiple photons. Therefore, the outside attacks are invalid to our protocol.

4.3.2. Participant Attack

Gao et al. proposed the term "participant attack" in Ref. [29], which has attracted much attention in the cryptanalysis of quantum cryptography. It underlines that malicious user attacks are typically more potent and should be given more consideration. We analyze the possibility that Alice, Bob, and Calvin could use participant attacks to learn knowledge

about the private binary strings in our protocol. Since both Alice and Bob's sequences are sent to Calvin after processing, it is most critical to consider Calvin's behavior.

In our protocol, Calvin only gets two-particle sequences $S_A^{''}, S_B^{''}$. Calvin applies the T gate on each sequence in step (3).

According to the definition of information-theoretic security given in Section 2.3, we can know that the output state of step (2) in our protocol can be described as follows:

$$\begin{aligned}
&\frac{1}{2^2}\sum_{l_{2i-1}^A, l_{2i}^A \in \{0,1\}} Z^{l_{2i-1}^A} X^{l_{2i}^A} |\psi_i^A\rangle (Z^{l_{2i-1}^A} X^{l_{2i}^A})^\dagger \\
&= \tfrac{1}{4} Z^0 X^0 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^0 X^0)^\dagger + \tfrac{1}{4} Z^0 X^1 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^0 X^1)^\dagger \\
&\quad + \tfrac{1}{4} Z^1 X^0 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^1 X^0)^\dagger + \tfrac{1}{4} Z^1 X^1 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^1 X^1)^\dagger \\
&= \tfrac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}
\end{aligned} \tag{24}$$

$$\begin{aligned}
&\frac{1}{2^2}\sum_{l_{2i-1}^B, l_{2i}^B \in \{0,1\}} Z^{l_{2i-1}^B} X^{l_{2i}^B} |\psi_i^B\rangle (Z^{l_{2i-1}^B} X^{l_{2i}^B})^\dagger \\
&= \tfrac{1}{4} Z^0 X^0 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^0 X^0)^\dagger + \tfrac{1}{4} Z^0 X^1 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^0 X^1)^\dagger \\
&\quad + \tfrac{1}{4} Z^1 X^0 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^1 X^0)^\dagger + \tfrac{1}{4} Z^1 X^1 (\tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|)(Z^1 X^1)^\dagger \\
&= \tfrac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1. \end{bmatrix}
\end{aligned} \tag{25}$$

These calculations indicate that all the states obtained by Calvin are just totally mixed states. So Calvin cannot learn Alice's and Bob's private binary strings from the particle sequences he obtained.

4.4. Comparison

The related quantum PSI-CA protocols in [27,28] required entangled states, other complicated oracle operators and measurements in high dimensional Hilbert space, hence it is more feasible with the current technologies than those proposed with entangled states. Compared with some recently proposed protocols [27,28], our proposed quantum PSI-CA protocol has the following advantages. First, it only needs to take single photons as quantum resources and to apply single operators and measurements. Obviously, it is more feasible to prepare these resources and implement these operators and measurements. Second, our new protocol is more robust and can easily use the fault tolerant technologies due to single photons. Therefore, our new quantum protocol for PSI-CA is more practical and feasible compared with the existing protocols.

5. Discussion and Conclusions

In summary, we give a novel quantum solution for PSI-CA. With the help of the quantum operators X, Z, and T, Calvin can help Alice and Bob obtain the PSI-CA results of their private sets after performing. Moreover, we provide a theoretical correctness study and use the Qiskit package to verify the scheme on the IBM Quantum Experience platform by way of a simulation experiment. In the end, we provide a security analysis of our protocol, which demonstrates that our protocol can resist various outside attacks, such as the disturbance attack, the Trojan horse attack, the intercept–resend attack, the entanglement-and-measure attack, and the man-in-the-middle attack. Additionally, it can also overcome the problem of information leakage with acceptable efficiency. Furthermore, we hope to extend our protocol for a generic case such as an n-qubit Toffoli gate and we also hope that our methods can provide some new ideas to solve more secure multi-party computations in the future.

Author Contributions: Investigation, Y.L. (Yangzhi Li) and Z.W.; methodology, W.L. and Y.L. (Yugang Li); software, Z.W.; validation, Y.L. (Yangzhi Li) and W.L.; formal analysis, W.L. and Y.L. (Yangzhi Li); writing—original draft preparation, Y.L. (Yangzhi Li) and Z.W.; writing—review and editing, W.L. and Y.L. (Yugang Li); visualization, Y.L. (Yangzhi Li); supervision, W.L. and Y.L. (Yangzhi Li); project administration, W.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Key Research and Development Program in China(2022YFC3302103-01),the Strategic Research Program of Science and Technology Commission of the Ministry of Education of China(JYB2022-01), and the Fundamental Research Funds for the Central Universities.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the author.

Acknowledgments: We would like to thank the editors and the anyonemous reviewers for their insightful comments and constructive suggestions.

Conflicts of Interest: The authors declare no conflict of interest.

Sample Availability: Samples of the compounds are available from the authors.

References

1. Gordon, S.D.; Hazay, C.; Katz, J.; Lindell, Y. Complete fairness in secure two-party computation. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing(STOC), Victoria, Canada, 17–20 May 2008; pp. 413–422; ACM Press: New York, NY, USA, 2008.
2. Asharov, G.; Canetti, R.; Hazay, C. Towards a game theoretic viewof secure computation. In *Advances in Cryptology-EUROCRYPT 2011*; Springer: Berlin/Heidelberg, Germany, 2011; Volume 6632, pp. 426-445.
3. Groce, A.; Katz, J. Fair computation with rational players. In *Advances in Cryptology- EUROCRYPT 2012*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 81–98.
4. Freedman, M.J.; Nissim, K.; Pinkas, B. Efficient Private Matching and Set Intersection. In Proceedings of the Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–19.
5. Chun, J.Y.; Hong, D.; Jeong, I.R.; Lee, D.H. Privacy-preserving disjunctive normal form operations on distributed sets. *Inform. Sci.* **2013**, *231*, 113–122.
6. Pervez, Z.; Awan, A.A.; Khattak, A.M.; Lee, S.; Huh, E.N. Privacy-aware searching with oblivious term matching for cloud storage. *J. Supercomput.* **2013**, *63*, 538–560.
7. Schlegel, R.; Chow, C.Y.; Huang, Q.; Wong, D.S. Privacy-preserving location sharing services for social networks. *IEEE Transactions on Services Computing*, **2016**, *10*, 811–825.
8. Baldi, P.; Baronio, R.; De Cristofaro, E.; Gasti, P.; Tsudik., G. Countering GATTACA: efficient and secure testing of fully-sequenced human genomes. In Proceedings of the 18th ACM Conference on Computer and Communications Security, Chicago, IL, USA, 17–21 October 2011; pp. 691–702.
9. Narayanan, A.; Thiagarajan, N.; Lakhani, M.; Hamburg, M.; Boneh, D. Location privacy via private proximity testing. In Proceedings of the Network and Distributed System Security Symposium (NDSS 2011), San Diego, CA, USA, 6–9 February 2011.
10. Bursztein, E.; Hamburg, M.; Lagarenne, J.; Boneh, D. Openconflict: preventing real time map hacks in online games. In *2011 IEEE Symposium on Security and Privacy*; IEEE: Manhattan, NY, USA, 2011; pp. 506–520.
11. Rivest R.L.; Adleman L.; Dertouzos M.L. On data banks and privacy homomorphisms. *Found. Secur. Comput.* **1978**, *4*, 169–180.
12. Kuang R.; Perepechaenko M.; Toth R. A New Symmetric Homomorphic Functional Encryption over a Hidden Ring for Polynomial Public Key Encapsulations. *arXiv* **2023**, arXiv:2301.11995.
13. Wu, M.E.; Chang, S.Y.; Lu, C.J.; Sun, H.M. A communication-efficient private matching scheme in client-server model. *Inform. Sci.* **2014**, *275*, 348–359.
14. Shao, Z.Y.; Yan, B. Private set intersection via public key encryption with keywords search. *Secur. Commun. Netw.* **2015**, *8*, 396–402.
15. Hazay, C.; Nissim, K. Efficient set operations in the presence of malicious adversaries. *J. Cryptol.* **2012**, *25*, 383–433.
16. Hazay, C. Oblivious polynomial evaluation and secure set intersection from algebraic PRFs. *J. Cryptol.* **2018**, *31*, 537–586.
17. Vaidya, J.; Clifton, C. Secure set intersection cardinality with application to association rule mining. *J. Comput. Secur.* **2005**, *13*, 593–622.
18. Debnath, S.K.; Dutta, R. Secure and efficient private set intersection cardinality using bloom filter. In *Information Security (Lecture Notes in Computer Science)*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9290, pp. 209–226.
19. Cristofaro, E.D.; Gasti, P.; Tsudik, G. Fast and private computation of cardinality of set intersection and union. In *Cryptology and Network Security (CANC 2010)*; LNCS 7712; Springer: Berlin/Heidelberg, Germany, 2012; pp. 218–231.

20. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Siam Rev.* **1999**, *41*, 303–332.
21. Grover, L.K. A fast quantum mechanical algorithm for database search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; pp. 212–219.
22. Li, Z.; Cai, B.; Sun, H.; Liu, H.; Wan, L.; Qin, S.; Wen, Q.; Gao, F. Novel quantum circuit implementation of AES with low costs. *Sci. China Phys. Mech. Astron.* **2022**, *65*, 290311
23. Shi, R.H.; Mu, Y.; Zhong, H.; Zhang, S. Quantum oblivious set-member decision protocol. *Phys. Rev. A* **2015**, *92*, 022309.
24. Shi, R.H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. An efficient quantum scheme for Private Set Intersection. *Quantum Inf. Process.* **2016**, *15*, 363–371.
25. Maitra, A. Quantum secure two-party computation for set intersection with rational players. *Quantum Inf. Process.* **2018**, *17*, 1–21. https://doi.org/10.1007/s11128-018-1968-9
26. Shi, R.H. Quantum private computation of cardinality of set intersection and union. *Eur. Phys. J.* **2018**, *12*, 1–6.
27. Shi, R.H.; Mu, Y.; Zhong, H.; Zhang, S.; Cui, J. Quantum private set intersection cardinality and its application to anonymous authentication. *Inform. Sci.* **2016**, *370–371*, 147–158.
28. Shi, R.H. Efficient quantum protocol for private set intersection cardinality. *IEEE Access* **2018**, *6*, 73102–73109.
29. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.C. A simple participant attack on the Bradler–Dusek protocol. *Quantum Inf. Comput.* **2007**, *7*, 329.