

Article

Efficient Semi-Quantum Secure Multi-Party Summation Protocol Based on Cancelable Random Masks and Its Applications

Dan Wang ^{1,2}, Diedie Yang ³ and Haibin Wang ^{2,*} 

¹ School of Internet of Things and Artificial Intelligence, Wuxi Vocational College of Science and Technology, Wuxi 214028, China; wangdan@wxsc.edu.cn

² School of Computer Science, School of Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

³ School of Electronic and Information Engineering, Anhui Jianzhu University, Hefei 230601, China; diedieyang@stu.ahjzu.edu.cn

* Correspondence: whb9741705@nuist.edu.cn

Abstract

Quantum Secure Multi-party Summation (QSMS) is a fundamental primitive of Quantum Secure Multi-party Computation (QSMC), enabling multiple participants to jointly compute the sum of their private inputs without disclosing individual data. However, most existing QSMS protocols require all participants to possess full quantum capabilities and often rely on pre-shared keys, auxiliary mask transmission, or multiple trusted third parties, resulting in high communication overhead and limited practicality. To address these limitations, we propose an efficient Semi-Quantum Secure Multi-party Summation (SQSMS) protocol based on d -dimensional n -particle entangled states. By exploiting the global correlation properties of high-dimensional entangled states, the proposed protocol generates correlated random masks directly from quantum measurement outcomes. These masks cancel automatically during the aggregation process, eliminating the need for additional mask distribution and transmission. Compared with existing QSMS schemes, the proposed protocol reduces communication overhead, improves quantum efficiency, and avoids reliance on pre-shared keys or multiple trusted third parties. Moreover, only simple measurement operations are required from classical participants, making the protocol more practical for semi-quantum environments. We further provide formal correctness and security analyses of the proposed protocol and conduct quantum circuit simulations using the IBM Qiskit platform to demonstrate its feasibility. Moreover, based on the proposed summation protocol, we design several extended application protocols, including anonymous voting, anonymous auction, and anonymous ranking, which further illustrate the scalability and practical applicability of the proposed scheme.

Keywords: quantum secure multi-party summation; semi-quantum protocol; quantum Fourier transform; cancelable mask



Academic Editor: Rosario Lo Franco

Received: 8 May 2026

Revised: 11 June 2026

Accepted: 18 June 2026

Published: 23 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

With the rapid development of cloud computing, big data, and artificial intelligence, data have become a critical strategic resource for economic activities, social services, and technological innovation. However, the increasing value of data is accompanied by growing risks of privacy leakage and security threats in cross-institutional data collaboration. In practical scenarios such as financial risk control, collaborative medical diagnosis, joint statistical analysis, and government information sharing, multiple entities are often required

to jointly perform computational tasks without exposing their private data. This demand for “data usability without data disclosure” has driven the development of Secure Multi-party Computation (SMC). SMC enables multiple participants to jointly compute a target function without relying on a fully trusted third party, while ensuring that each participant’s private input remains confidential. Since Yao [1] introduced the classical “millionaire problem” and proposed the two-party secure computation framework, Goldreich et al. [2] further proved that any polynomial-time computable function can be securely realized in multi-party settings, thereby laying the theoretical foundation of SMC. After decades of development, SMC has evolved into several representative technical paradigms, including garbled circuits [3], secret sharing [4,5], oblivious transfer [6,7], and homomorphic encryption [8–10]. These techniques have demonstrated significant application value in privacy-preserving machine learning [11], anonymous voting [12,13], and secure statistical analysis [14].

Nevertheless, most classical SMC schemes rely on computational hardness assumptions, such as integer factorization and discrete logarithm problems. Their security fundamentally depends on the computational limitations of classical computers. With the rapid advancement of quantum computing, especially the emergence of Shor’s algorithm [15], which can solve integer factorization and discrete logarithm problems in polynomial time on ideal quantum computers, traditional public-key cryptosystems such as RSA face severe security threats. Consequently, constructing Secure Multi-party Computation mechanisms suitable for quantum environments has become an important research direction, leading to the development of QSMC. Benefiting from fundamental quantum mechanical properties, including the no-cloning theorem, quantum entanglement, and measurement disturbance, quantum cryptography provides a new framework for achieving information-theoretic security beyond classical computational assumptions. The BB84 quantum key distribution protocol proposed [16] demonstrated the intrinsic security advantages of quantum communication and established the theoretical foundation for subsequent quantum cryptographic protocols.

QSMS is an important branch of QSMC, aiming to securely compute the summation of private inputs without revealing participants’ confidential information. By exploiting quantum physical properties, QSMS can theoretically achieve information-theoretic security and has therefore attracted considerable attention in privacy-preserving computation research. However, existing QSMS protocols still face significant practical challenges. Most current schemes [17–25] assume that all participants possess full quantum capabilities, including quantum state preparation, unitary operations, and joint measurements. Given the high cost and limited accessibility of quantum hardware, such assumptions are difficult to satisfy in practical implementations. Furthermore, some protocols rely heavily on high-dimensional quantum systems or multi-particle entangled states [17,22,25] whose preparation, transmission, and error correction require substantial physical resources, resulting in increased communication overhead and system complexity. These limitations motivate the exploration of more practical quantum computation models that balance security and implementation feasibility.

To reduce the quantum capability requirements for ordinary users, Boyer et al. [26,27] proposed the concept of semi-quantum computation, where only a subset of participants possesses full quantum capabilities, while the remaining participants are restricted to simple operations such as reflecting qubits or measuring and resending qubits under fixed bases. Based on this idea, Semi-Quantum Secure Multi-party Computation (SQSMC) has gradually emerged as an important research direction in quantum privacy-preserving computation. In the field of SQSMS, Zhang et al. [28] first introduced the semi-quantum paradigm into multi-party summation in 2021 and proposed a three-party semi-quantum

summation protocol. Using single photons as information carriers, the protocol employs GHZ-basis measurements to verify the behavior of the trusted third party and achieve secure summation of private inputs. Subsequently, Ye et al. [29] proposed a two-party semi-quantum summation protocol based on logical qubits, which improves resistance against collective decoherence noise and enhances privacy protection. In 2024, Tian et al. [30] designed three semi-quantum summation protocols based on single-photon states. By optimizing the communication topology and protocol structure, their schemes further reduce the dependence of classical users on quantum measurement capabilities. Early SQSMS studies mainly focused on two-party or three-party modulo-2 summation scenarios. More recently, research has gradually extended to arbitrary multi-party and modulo- d computation settings. High-dimensional quantum systems have attracted increasing attention in quantum information processing because they can encode more information per carrier and thus provide higher channel capacity and transmission efficiency than qubit-based systems. These advantages have led to a variety of high-dimensional quantum computation and communication schemes [31,32]. In 2024, Ye et al. [33] proposed a multi-party modulo- d summation protocol combining high-dimensional entangled states with single-particle states, enabling secure summation among arbitrary numbers of participants. However, the protocol requires massive high-dimensional quantum resources, resulting in exponentially increasing overhead. Meanwhile, Lian et al. [34] proposed a hybrid semi-quantum summation protocol supporting comparison, multiplication, and summation functions. Although the scheme improves resource utilization efficiency, it relies on a dual-trusted-party architecture, where collusion or deviation between trusted entities may compromise overall security.

Overall, although semi-quantum models significantly reduce the quantum capability requirements compared with fully quantum schemes, existing SQSMS protocols still suffer from several limitations, including dependence on pre-shared keys, reliance on multiple trusted parties, and relatively low quantum efficiency. Therefore, improving quantum resource utilization, reducing trust assumptions, and enhancing scalability while maintaining strict security guarantees remain important and challenging research problems.

To address these challenges, this paper proposes an efficient Semi-Quantum Secure Multi-party Summation protocol based on d -dimensional n -particle entangled states. The main contributions of this paper are summarized as follows:

- We propose an efficient Semi-Quantum Secure Multi-party Summation protocol based on d -dimensional n -particle entangled states. By utilizing the global correlations of entangled states to construct mutually cancelable random masks, the protocol achieves secure aggregation of private inputs while reducing quantum communication overhead.
- We analyze the correctness, security, and efficiency of the proposed protocol, and implement the corresponding quantum circuit model on the IBM Qiskit platform. Our theoretical analysis and simulation results verify the correctness, security, and feasibility of the protocol.
- Based on the proposed protocol, we further construct semi-quantum anonymous voting, anonymous auction, and anonymous ranking protocols, demonstrating its scalability and applicability in privacy-preserving multi-party computation scenarios.

The remainder of this paper is organized as follows. Section 2 introduces the preliminary knowledge used in this work, including basic mathematical notations, measurement bases, and related properties. Section 3 presents the detailed implementation process of the proposed protocol. Section 4 analyzes the correctness, security, and quantum efficiency of the protocol and evaluates its feasibility through simulation experiments. Section 5 discusses the extended anonymous application protocols. Finally, Section 6 concludes the paper and outlines future research directions.

2. Preliminary

2.1. Definition of Notations

Table 1 lists the definition of notations that will be used in our paper.

Table 1. List of Symbols.

Symbol	Definition
n	Number of participants
d	Modulus for modular arithmetic or dimension of the Hilbert space
δ	Number of decoy particles used for eavesdropping detection
x_i	Private input of participant P_i
$ \Phi\rangle$	Original d -dimensional n -particle entangled state
$ \psi\rangle$	Entangled state after QFT
r_{ij}, r_{il}	Shared random mask or measurement result
c_i	Ciphertext
F	Quantum Fourier transform operator
S_i	A sequence sent from TP to P_i
S'_i	Sequence returned by P_i after operator REFLECT or MEASURE
f_j	Bitwise aggregated value computed by TP
R	The summation result
η	Quantum communication efficiency
W, w_l	Aggregated statistical vector and its elements

2.2. Two Measurement Bases

In high-dimensional quantum systems, the most commonly adopted measurement bases include the computational basis and the Fourier basis. Both play essential roles in quantum information processing and quantum communication protocols. In particular, for the construction and measurement analysis of high-dimensional entangled states, the transformation relationship between these two bases is generally established via the Quantum Fourier Transform (QFT).

For a d -dimensional quantum system, the computational basis is defined as

$$B_1 = \{|0\rangle, |1\rangle, \dots, |d-1\rangle\}, \quad (1)$$

which forms a set of standard orthonormal bases of the d -dimensional Hilbert space. When a quantum state is measured under the computational basis it collapses into one of the basis states and the measurement outcome corresponds to the label of the collapsed basis state.

Correspondingly, the Fourier basis can be derived by applying the QFT to the computational basis. Let F denote the d -dimensional Quantum Fourier Transform operator; the Fourier basis is then defined as

$$B_2 = \{F|0\rangle, F|1\rangle, \dots, F|d-1\rangle\}. \quad (2)$$

The action of QFT on an arbitrary computational basis state $|j\rangle$ is given by

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{\frac{2\pi i j k}{d}} |k\rangle. \quad (3)$$

Accordingly, each basis state in the Fourier basis is a uniform superposition of computational basis states with specific phase factors. A one-to-one correspondence between the computational basis and the Fourier basis is established via QFT and its inverse transform $\text{QFT}^\dagger$, making them a pair of mutually unbiased bases.

High-dimensional entangled states possess distinctive nonlocal correlation properties under different measurement bases. The mathematical expression of the d -dimensional n -particle GHZ entangled state is given by

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_1 |j\rangle_2 \cdots |j\rangle_n, \quad (4)$$

Such high-dimensional GHZ entangled states have remarkable particle-to-particle nonlocal correlations. This section introduces complementary correlation characteristics of the original state and its Fourier-transformed counterpart under two typical measurement bases. Note that the detailed derivations of all equations involved in the following properties are available in Refs. [35,36]. The relevant inherent properties are listed below.

Property 1. For $|\Phi\rangle$, if all particles are measured under the computational basis B_1 then the resulting measurement outcomes are perfectly correlated. Specifically, all participants obtain the same measurement result, namely

$$m_1 = m_2 = \cdots = m_n. \quad (5)$$

Property 2. For $|\Phi\rangle$, if all particles are measured under the Fourier basis B_2 then the measurement outcomes satisfy a modular summation constraint such that

$$m_1 + m_2 + \cdots + m_n \equiv 0 \pmod{d}. \quad (6)$$

Furthermore, by applying the Quantum Fourier Transform F to each particle of $|\Phi\rangle$, the following quantum state can be obtained:

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} F|j\rangle_1 \otimes F|j\rangle_2 \otimes \cdots \otimes F|j\rangle_n. \quad (7)$$

The transformed state $|\Psi\rangle$ can be regarded as the Fourier-domain representation of $|\Phi\rangle$, and it exhibits complementary correlation properties under the two measurement bases.

Property 3. For $|\Psi\rangle$, if all particles are measured under the computational basis B_1 then the measurement outcomes satisfy the following modular relation:

$$m_1 + m_2 + \cdots + m_n \equiv 0 \pmod{d}. \quad (8)$$

Property 4. For $|\Psi\rangle$, if all particles are measured under the Fourier basis B_2 then the resulting measurement outcomes are completely identical, i.e.,

$$m_1 = m_2 = \cdots = m_n. \quad (9)$$

3. Proposed Protocol

This protocol considers a computation model consisting of n mutually untrusted classical participants $P_1, P_2, \dots, P_n$ and one quantum participant TP. Each classical participant P_i holds a private input $x_i \in \{0, 1, \dots, d-1\}$, where d denotes the dimension of the quantum system and the public modulo parameter. The objective is to collaboratively compute the summation result $R = \sum_{i=1}^n x_i \pmod{d}$ without revealing any participant's private information. In the security model, all classical participants are mutually untrusted and may attempt to infer others' private inputs from the exchanged information, while still following the protocol honestly. As a remote quantum server, TP is assumed to be semi-honest, i.e., it

faithfully executes the protocol but may analyze the obtained information. Moreover, TP is not allowed to collude with any participant or tamper with the protocol execution.

Protocol 1. *Semi-Quantum Secure Multi-Party Summation Protocol (SQSMS).*

Input: Each classical participant P_i ($i = 1, 2, \dots, n$) holds a private input $x_i \in \{0, 1, \dots, d-1\}$.

Output: Compute the summation result $R = \sum_{i=1}^n x_i \pmod{d}$ without revealing any participant's private input.

(1) Initialization Phase

Step 1. Each classical participant P_i constructs a binary encoding sequence $X_i = \{x_{i0}, x_{i1}, \dots, x_{i(d-1)}\}$ of length d , where $x_{ij} \in \{0, 1\}$ for $j \in \{0, 1, \dots, d-1\}$. The encoding rule is defined as:

$$x_{ij} = \begin{cases} 1 & \text{if } j = x_i, \\ 0 & \text{if } j \neq x_i. \end{cases} \quad (10)$$

Step 2. TP prepares d sets of the d -dimensional n -particle GHZ entangled state defined previously, which takes the form

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (|j\rangle)^{\otimes n} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_1 |j\rangle_2 \cdots |j\rangle_n. \quad (11)$$

TP then applies the QFT to every particle of this state, and the resulting state is written as

$$|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (F|j\rangle)^{\otimes n} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} F|j\rangle_1 F|j\rangle_2 \cdots F|j\rangle_n, \quad (12)$$

where F denotes the d -dimensional QFT operator. TP subsequently partitions all entangled states according to particle positions. The i -th quantum sequence S_i consists of the i -th particle selected from all prepared states, forming the sequence set $S_1, S_2, \dots, S_n$.

Step 3. TP additionally prepares δ sets of identical original entangled states $|\Phi\rangle$ as decoy states. Half of these decoy state sets are chosen randomly, and the predefined operator F is applied to all particles to generate transformed decoy states $|\psi\rangle$. Following the same particle partitioning operation described in Step 2, TP divides all δ decoy state sets into n groups and randomly inserts each group into the corresponding quantum sequence S_i . The updated sequences are marked as $S'_1, S'_2, \dots, S'_n$, and TP records all insertion positions for subsequent eavesdropping detection.

(2) Interactive Phase

Step 4. After each classical participant P_i ($i = 1, 2, \dots, n$) receives the corresponding quantum sequence S'_i , TP publicly announces the positions of all decoy particles together with the corresponding measurement bases. According to the published information, each participant locates the decoy particles and performs measurements using the specified bases. The measurement results are then returned to TP for consistency verification.

To verify the security of the quantum channel, TP checks the consistency of all reported measurement results according to the preparation method of the decoy particles and the selected measurement bases. The corresponding criteria are listed in Table 2.

TP calculates the error rate according to the above criteria. If the error rate is below the preset threshold then the quantum channel is regarded as secure and the protocol continues. Otherwise, the protocol is terminated due to possible eavesdropping.

Table 2. Eavesdropping detection criteria.

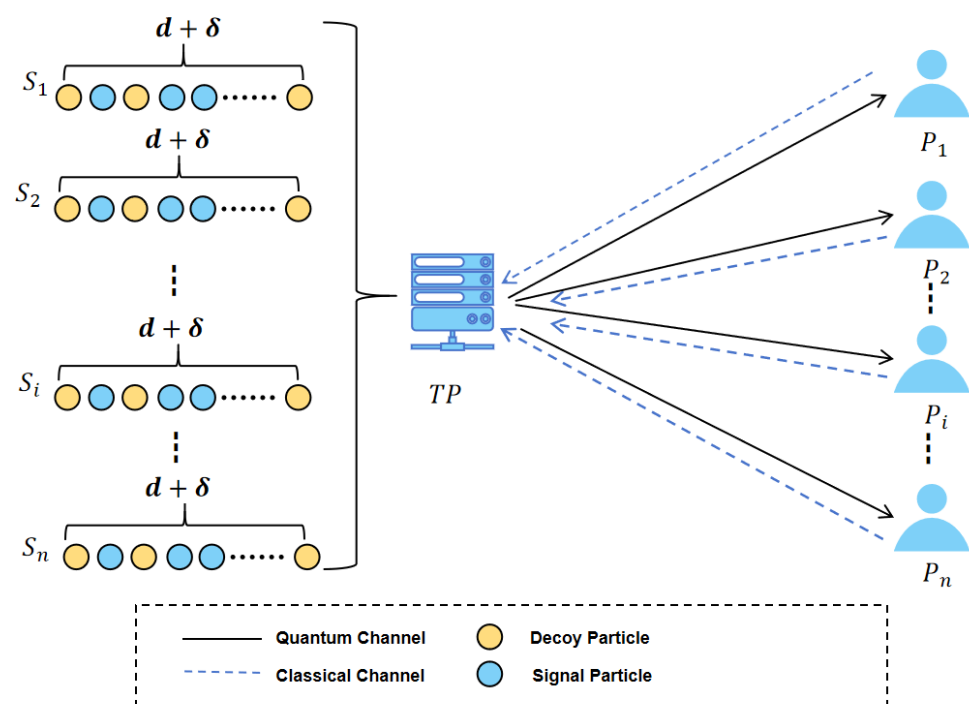
Case	QFT	Measurement Basis	Result
1	Yes	Computational basis	The sum of all measurement results modulo d equals 0
2	Yes	Fourier basis	All measurement results are identical
3	No	Computational basis	All measurement results are identical
4	No	Fourier basis	The sum of all measurement results modulo d equals 0

Step 5. After the eavesdropping detection is completed, each participant removes all decoy particles from the received sequence. Participant P_i then sequentially measures the remaining quantum particles and records the corresponding outcomes r_{ij} , where $j \in \{0, 1, \dots, d-1\}$ denotes the j -th entangled state.

Step 6. Each participant P_i encrypts the private sequence X_i using the measurement results r_{ij} . The encryption rule is defined as

$$c_{ij} = x_{ij} + r_{ij} \pmod{d}, \quad (13)$$

where $i \in \{1, \dots, n\}$, $j \in \{0, \dots, d-1\}$, and where x_{ij} represents the j -th element of X_i . Each participant constructs the encrypted sequence $X'_i = (c_{i0}, c_{i1}, \dots, c_{i(d-1)})$ and sends it to TP. The interaction process is illustrated in Figure 1.

**Figure 1.** Schematic diagram of interactive phase operation.

(3) Output Result Phase

Step 7. After receiving all the encrypted sequences, TP performs the following summation for each index j :

$$f_j = \sum_{i=1}^n c_{ij} = \sum_{i=1}^n (x_{ij} + r_{ij}) = \sum_{i=1}^n x_{ij}. \quad (14)$$

Finally, TP computes the output result by

$$R = \sum_{j=0}^{d-1} j \cdot f_j \pmod{d}. \quad (15)$$

4. Performance Analysis

This section presents a comprehensive performance evaluation of the SQSMS protocol, including its correctness, security, efficiency, and practical feasibility. The analysis is conducted through theoretical derivation, comparative assessment, and simulation verification to demonstrate the protocol's reliability and applicability in realistic scenarios.

4.1. Correctness

This section proves that the proposed SQSMS protocol can correctly compute the following result when all participants honestly execute the protocol:

$$R = \sum_{i=1}^n x_i \pmod{d}. \quad (16)$$

In the initialization phase, each participant P_i encodes its private input $x_i \in \{0, 1, \dots, d-1\}$ into a binary sequence $X_i = \{x_{i0}, x_{i1}, \dots, x_{i(d-1)}\}$ of length d , where

$$x_{ij} = \begin{cases} 1, & j = x_i, \\ 0, & j \neq x_i, \end{cases} \quad j \in \{0, 1, \dots, d-1\}. \quad (17)$$

Accordingly, each encoding sequence satisfies

$$\sum_{j=0}^{d-1} x_{ij} = 1. \quad (18)$$

Summing over all participants gives

$$\sum_{j=0}^{d-1} j \left(\sum_{i=1}^n x_{ij} \right) = \sum_{i=1}^n x_i. \quad (19)$$

In the SQSMS protocol, TP first prepares the original d -dimensional n -particle entangled states. It then applies the operator F to all particles of the entangled states before distributing them to each participant. As stated in Property 3 of the preliminary section, the transformed entangled states retain their inherent correlation constraints. Accordingly, the measurement results r_{ij} obtained by participants from the received quantum states satisfy

$$\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d}. \quad (20)$$

Each participant encrypts the private encoding sequence according to Equations (13) and (14). TP then computes the aggregation value at the j -th position:

$$f_j = \sum_{i=1}^n c_{ij} = \sum_{i=1}^n x_{ij} + \sum_{i=1}^n r_{ij} \equiv \sum_{i=1}^n x_{ij}. \quad (21)$$

Therefore, the masking terms are eliminated during aggregation and do not affect the correctness of the summation result.

In the output phase, TP reconstructs the final result according to Equations (13)–(15). Since $f_j = \sum_{i=1}^n x_{ij}$, we have

$$R = \sum_{j=0}^{d-1} j \cdot f_j \pmod{d} = \sum_{i=1}^n x_i \pmod{d}. \quad (22)$$

Therefore, the protocol can correctly compute the summation of all private inputs under honest conditions.

To further illustrate the correctness of the protocol, consider a simple example with $n = 3$ and $d = 5$. Suppose the private inputs are $x_1 = 1$, $x_2 = 3$, and $x_3 = 4$. According to the one-hot encoding rule, the corresponding encoding sequences are $(0, 1, 0, 0, 0)$, $(0, 0, 0, 1, 0)$, $(0, 0, 0, 0, 1)$.

Bitwise aggregation yields $f_0 = 0$, $f_1 = 1$, $f_2 = 0$, $f_3 = 1$, $f_4 = 1$.

During the quantum measurement phase, the entangled correlation guarantees that the masking terms satisfy

$$\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d}.$$

Hence,

$$f_j = \sum_{i=1}^3 x_{ij}.$$

Substituting the aggregation results into the reconstruction formula gives

$$R = 0 \times 0 + 1 \times 1 + 2 \times 0 + 3 \times 1 + 4 \times 1 = 8 \equiv 3 \pmod{5}. \quad (23)$$

The direct summation of the original private inputs is

$$1 + 3 + 4 = 8 \equiv 3 \pmod{5}.$$

The two results are identical, which verifies the correctness of the proposed protocol.

4.2. Security

This section analyzes the security of the proposed SQSMS protocol against six representative attack models, namely measurement attack, intercept–resend attack, entangled measurement attack, impersonation attack, collusion attack, and external attack. The security analysis is conducted under the semi-honest model, where all participants follow the protocol execution while potentially attempting to infer additional information from the accessible data.

Lemma 1. *Resistance to measurement attack. Any adversary performing unauthorized measurements on the transmitted quantum sequences can be detected during the eavesdropping detection process.*

Proof. Suppose an adversary intercepts a transmitted sequence and performs single-particle measurements before forwarding the particles.

According to Step 3, TP randomly inserts δ decoy entangled states into each transmitted sequence. Some decoy states remain in the original GHZ state $|\Phi\rangle$, while the others are transformed into $|\psi\rangle$ by applying QFT.

After receiving the particles, participants measure the decoy particles according to the measurement bases announced by TP.

For the original GHZ state $|\Phi\rangle$, Property 1 shows that all measurement outcomes must be identical in the computational basis, while Property 2 requires

$$\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d} \quad (24)$$

in the Fourier basis.

Similarly, for the transformed state $|\psi\rangle$ the two correlation conditions are exchanged.

Since the adversary does not know the positions of decoy particles or whether QFT has been applied, any unauthorized measurement collapses the corresponding quantum state and disturbs the original correlations.

Consequently, the reported measurement outcomes no longer satisfy the verification criteria listed in Table 2, leading to an abnormal error rate. Therefore, the attack is detected by TP during Step 4. $\square$

Lemma 2. *Resistance to intercept–resend attack. The proposed SQSMS protocol can resist intercept–resend attacks.*

Proof. Suppose an adversary intercepts a transmitted sequence, measures the intercepted particles, prepares new particles according to the measurement outcomes, and then resends them to the legitimate participant.

Because the adversary has no knowledge of the locations of the decoy particles and does not know whether a decoy state belongs to $|\Phi\rangle$ or $|\psi\rangle$ the reconstructed particles cannot preserve the original correlation structure.

Consequently, the forged particles fail to satisfy the correlation conditions required by Table 2. During the eavesdropping detection process, TP compares all reported measurement outcomes and computes the error rate.

Therefore, the intercept–resend attack inevitably introduces detectable inconsistencies and is discovered before the protocol proceeds to the summation stage. $\square$

Lemma 3. *Resistance to collusion attack. Assuming that TP does not collude with any participant, any subset of dishonest participants cannot recover the private inputs of honest participants.*

Proof. Suppose a coalition $C = \{P_1, P_2, \dots, P_k\}$ attempts to infer the private input of an honest participant P_t , where $k < n - 1$.

According to Step 6, participant P_t uploads

$$c_{ij} = x_{ij} + r_{ij} \pmod{d}. \quad (25)$$

The masking value r_{ij} originates from the measurement outcomes of the shared high-dimensional entangled state and satisfies

$$\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d}. \quad (26)$$

Although the colluding participants know their own measurement results they cannot obtain the measurement outcomes belonging to honest participants. Therefore, they cannot determine the exact value of r_{ij} .

Since r_{ij} remains unknown to the colluding set, the ciphertext c_{ij} reveals no useful information about x_{ij} . Consequently, the coalition cannot recover the private input of the honest participant. $\square$

Lemma 4. *Resistance to external attack. External adversaries cannot obtain valid information through either the quantum channel or the classical channel.*

Proof. For the quantum channel, an external adversary may perform measurement attacks, intercept–resend attacks, or entangled measurement attacks by introducing auxiliary particles and performing joint operations.

However, any operation on the transmitted particles disturbs the correlations of the original entangled states. As a result, the measurement outcomes of the decoy particles no longer satisfy the verification criteria in Table 2, and the attack is detected during Step 4.

For the classical channel, the transmitted information is

$$c_{ij} = x_{ij} + r_{ij} \pmod{d}. \quad (27)$$

Since the masking value r_{ij} is generated from the quantum measurement outcomes and is unavailable to external adversaries, the ciphertext sequence alone is insufficient to recover any participant's private input.

Therefore, external attacks cannot obtain useful information from either communication channel. $\square$

4.3. Efficiency Evaluation

For this section, we systematically evaluated the performance of the proposed SQSMS protocol. Several metrics were adopted for comparison with existing quantum summation protocols, including quantum resource consumption, summation type, quantum operation complexity, reliance on pre-shared keys, the number of TPs, and quantum efficiency. The detailed comparison results are presented in Table 3.

In a d -dimensional Hilbert space, quantum efficiency is widely used to evaluate the communication efficiency of a quantum protocol, which is defined as

$$\eta = \frac{c}{q + b}, \quad (28)$$

where c denotes the total length of encoded plaintext information involved in the computation, q represents the total number of consumed d -dimensional quantum particles (i.e., qudits), and b denotes the total number of classical bits exchanged for decoding.

Consider the SQSMS protocol with n participants, where each participant encodes one private input into a sequence of length d , and δ decoy particles are employed for channel security detection. During protocol execution, TP prepares d d -dimensional n -particle entangled states for information transmission and additional δ entangled states as decoy states. Therefore, the total number of consumed quantum particles is

$$q = n(d + \delta). \quad (29)$$

In Step 6, each participant sends an encrypted sequence $X'_i = (c_{i0}, c_{i1}, \dots, c_{i(d-1)})$ of length d to TP. According to the encoding procedure in Step 1, each private input x_i is first mapped into a binary sequence $X_i = (x_{i0}, x_{i1}, \dots, x_{i(d-1)})$ of length d . Since the subsequent encryption, transmission, and summation operations are all performed on these encoded elements, the total amount of plaintext information involved in the computation is nd . Therefore, the total length of plaintext messages is $c = nd$.

Accordingly, the quantum communication efficiency of the proposed SQSMS protocol is

$$\eta = \frac{nd}{n(d + \delta) + nd} = \frac{d}{2d + \delta}. \quad (30)$$

It can be observed that for a fixed number of participants and security parameter δ the quantum efficiency gradually approaches a constant as the encoding dimension d increases:

$$\lim_{d \rightarrow \infty} \eta = \frac{1}{2}. \quad (31)$$

Therefore, while guaranteeing channel security detection the proposed protocol achieves linear-scale resource consumption and maintains stable quantum communication efficiency for large-scale inputs.

As shown in Table 3, the proposed SQSMS protocol exhibits several advantages in key performance indicators. In terms of quantum resources, the protocol adopts d -dimensional n -particle entangled states as information carriers and completes the summation task using only measurement operations, without introducing complex quantum logic gates such as SUM gates or U_k gates. Therefore, the protocol has lower implementation complexity than the scheme in Ref. [25]. Although the protocol in Ref. [34] employs d -dimensional single-particle states it requires two TPs, resulting in higher system complexity. By contrast, the proposed protocol relies only on a single semi-honest TP and does not require pre-shared keys, thereby avoiding additional overhead caused by key distribution and management. In terms of functionality, the proposed protocol supports modulo- d summation, making it more suitable for high-dimensional data processing than modulo-2 summation schemes. Quantitatively, the protocol achieves quantum efficiency $\frac{d}{2d+\delta}$, which is higher than most existing modulo- d summation protocols.

Overall, the proposed SQSMS protocol achieves favorable performance in terms of quantum operation complexity, system structure simplicity, trust model rationality, and communication scalability, while maintaining satisfactory security guarantees.

Table 3. Performance evaluation of SQSMS protocols.

Protocol	Quantum Resources	Summation Type	Quantum Operations	Pre-Shared Key	Number of TPs	Quantum Efficiency
Lian [34]	d -dimensional single-particle states	Modulo d	Measurement	No	2	$\frac{1}{25n+1}$
Ye [33]	d -dimensional n -particle entangled states, single-particle states	Modulo d	Measurement	No	1	$\frac{1}{2^n+2+\delta}$
Yi [25]	d -dimensional n -particle entangled states	Modulo d	SUM gate, U_k gate, and measurement	No	1	$\frac{1}{n(L+1)}$
Tian [30]	n -qubit product states	Modulo 2	Measurement	Yes	1	$\frac{2L+\delta}{d}$
Our protocol	d -dimensional n -particle entangled states	Modulo d	Measurement	No	1	$\frac{d}{2d+\delta}$

d : Hilbert space dimension; L : length of private input encoding sequence; δ : number of decoy particles for eavesdropping detection; n : number of participants.

4.4. Simulation

Numerical simulations were conducted using the IBM Qiskit platform to verify the logical correctness and internal consistency of the proposed SQSMS protocol under ideal quantum circuit settings. In the considered model, the trusted third party (TP) prepares high-dimensional GHZ entangled states as quantum resources and distributes them to the participants. Each participant performs measurements in either the computational basis or the Fourier basis to generate correlated outcomes and to verify consistency relations required by the protocol. It is important to emphasize that the simulation was performed on an ideal noise-free quantum circuit model and was used solely to validate the theoretical measurement correlations and protocol functionality, rather than to evaluate physical implementation performance on near-term quantum hardware.

Without loss of generality, an 8-dimensional three-particle quantum system was considered for simulation. The TP prepared the following two groups of entangled states:

$$|\Phi\rangle = \frac{1}{\sqrt{8}} \sum_{j=0}^7 |j\rangle_1 |j\rangle_2 |j\rangle_3, \quad (32)$$

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{j=0}^7 F|j\rangle_1 F|j\rangle_2 F|j\rangle_3. \quad (33)$$

When measuring the original entangled state $|\Phi\rangle$ via the computational basis, three participants obtained identical measurement outcomes in each trial. The measured results were uniformly distributed over $\{000, 001, 010, 011, 100, 101, 110, 111\}$. The corresponding quantum circuit and measurement results are displayed in Figure 2.

When adopting the Fourier basis to measure $|\Phi\rangle$, the sum of three groups of measurement results was concentrated on 0, 8 and 16, which complied well with the theoretical modulo- d constraint. The relevant simulation results are illustrated in Figure 3.

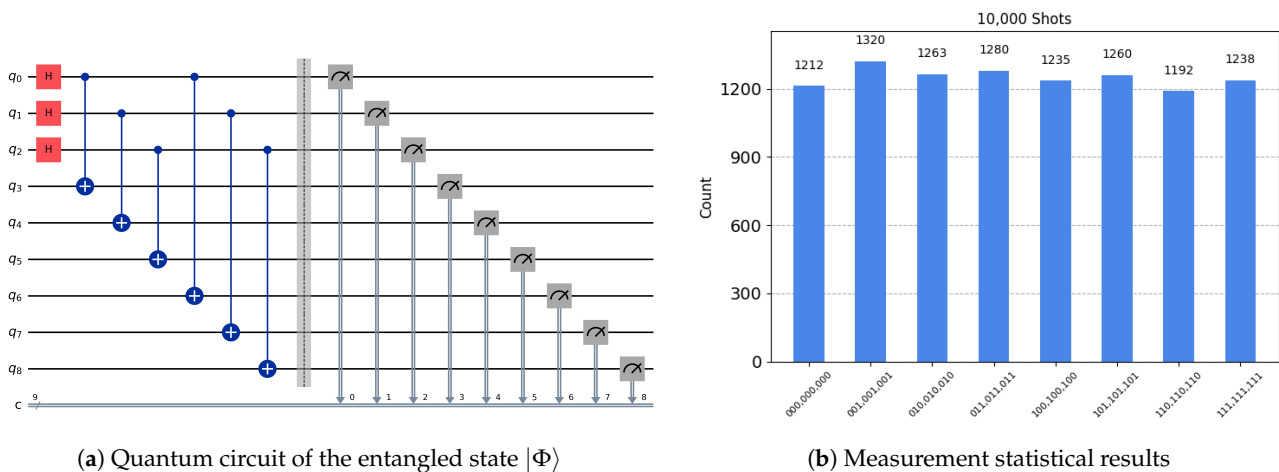


Figure 2. Quantum circuit and computational basis measurement results of the entangled state $|\Phi\rangle$.

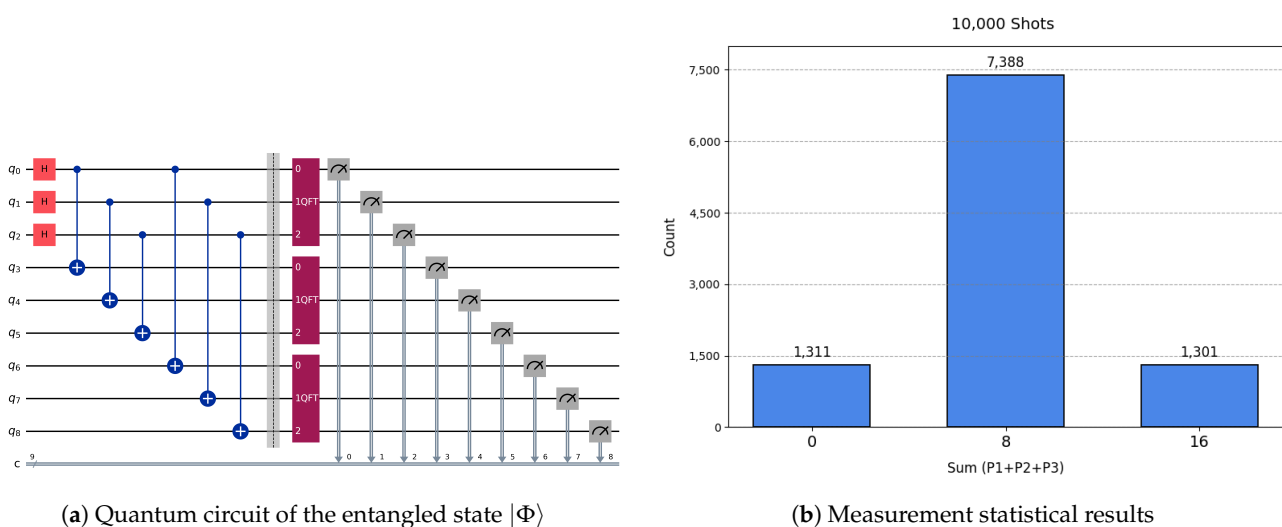


Figure 3. Quantum circuit and Fourier basis measurement results of the entangled state $|\Phi\rangle$.

For the Fourier-transformed entangled state $|\psi\rangle$, the computational basis measurement results satisfied the constraint $\sum \equiv 0 \pmod{d}$, and the summation values were concen-

trated on 0, 8 and 16. The corresponding quantum circuit and result distribution are shown in Figure 4.

By contrast, the Fourier basis measurements on $|\psi\rangle$ generated consistent outcomes among the three participants in each simulation. All the measurement results followed a uniform distribution across $\{000, 001, 010, 011, 100, 101, 110, 111\}$. The quantum circuit and statistical results are presented in Figure 5. Overall, the Qiskit simulations confirmed the expected entanglement correlations and measurement consistency of the proposed protocol under ideal quantum circuit assumptions.

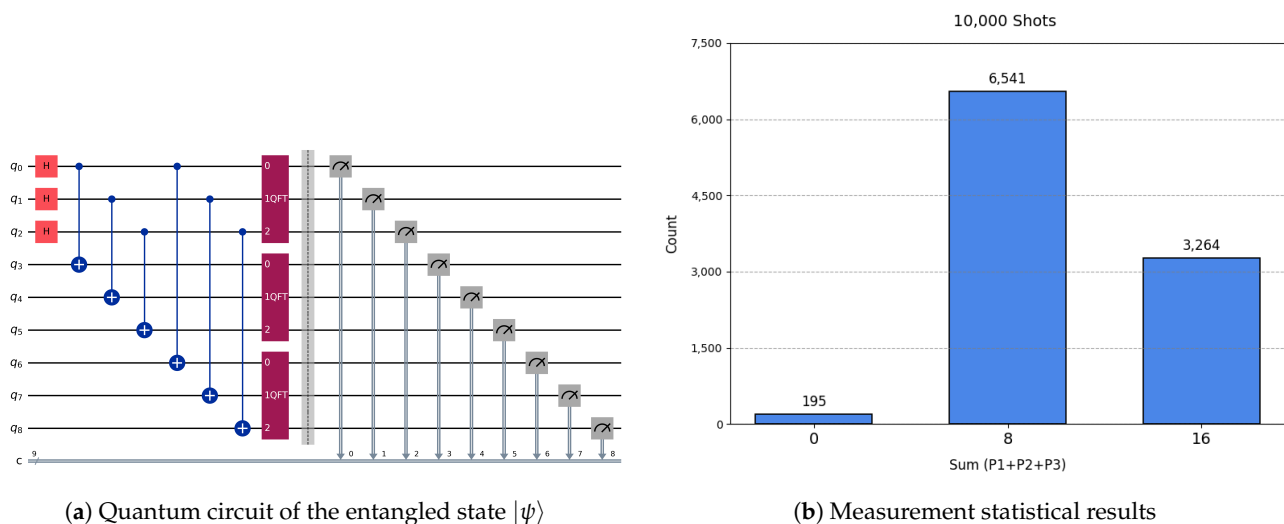


Figure 4. Quantum circuit and computational basis measurement results of the entangled state $|\psi\rangle$.

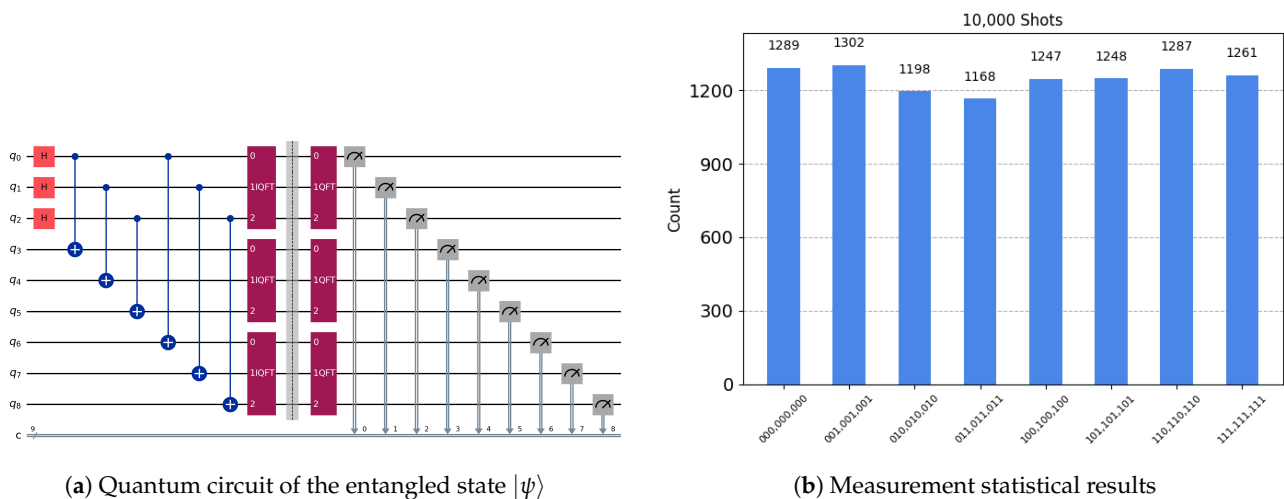


Figure 5. Quantum circuit and Fourier basis measurement results of the entangled state $|\psi\rangle$.

5. Applications

In this section, we further extend the proposed SQSMS protocol and design three types of semi-quantum multi-party computation protocols suitable for anonymous scenarios, namely anonymous voting, anonymous auction, and anonymous ranking. Since these three protocols are constructed based on the SQSMS framework, we do not repeat the specific implementation steps of the original protocol. Instead, we focus on analyzing how to adopt the SQSMS protocol to construct the anonymous voting, anonymous auction, and anonymous ranking protocols.

5.1. Semi-Quantum Anonymous Voting Protocol

Definition 1 (Semi-quantum anonymous voting). Suppose there exists a trusted quantum-assisted third party TP and n voters $\{P_1, P_2, \dots, P_n\}$. Each voter P_i holds a private vote $x_i \in [0, d - 1]$. The goal is to count the candidate with the highest number of votes while ensuring the anonymity of both voting contents and voter identities.

Protocol 2. Semi-quantum Secure Multi-party Anonymous Voting Protocol (SQSMAV)

Input: Each participant P_i inputs a private vote x_i .

Output: The TP announces the candidate number with the maximum number of votes.

Step 1. Parameter publication. The TP releases the candidate set $\{0, 1, \dots, d - 1\}$ and the maximum number of participants n .

Step 2. Voting vector generation. Each voter P_i determines its private vote $x_i \in [0, d - 1]$ and constructs a voting vector v_i of length d . The x_i -th entry is set to 1, and all other entries are set to 0.

$$R = (r_0, \dots, r_l, \dots, r_{d-1}) = \begin{pmatrix} r_{10} \\ \vdots \\ r_{i0} \\ \vdots \\ r_{n0} \end{pmatrix} \cdots \begin{pmatrix} r_{1l} \\ \vdots \\ r_{il} \\ \vdots \\ r_{nl} \end{pmatrix} \cdots \begin{pmatrix} r_{1d-1} \\ \vdots \\ r_{id-1} \\ \vdots \\ r_{nd-1} \end{pmatrix}. \quad (34)$$

Step 3. Mask generation. All voters generate shared masks r_i through the SQSMS protocol.

Step 4. Encryption and transmission. Each P_i encrypts its voting vector with the generated mask:

$$v_{il}^* = v_{il} + r_{il}, \quad l = 0, 1, \dots, d - 1. \quad (35)$$

Then each participant sends the encrypted vector to the TP.

Step 5. Vote counting and statistics. The TP initializes the vote vector $W = \{w_0, w_1, \dots, w_{d-1}\}$ and calculates

$$w_l = \sum_{i=1}^n (v_{il} + r_{il}) \bmod d, \quad l = 0, 1, \dots, d - 1. \quad (36)$$

Finally, the TP publishes the statistical result W to all voters and announces the candidate with the highest votes.

Example 1. To illustrate the execution of the SQSMAV protocol, a concrete instance is given as follows. Suppose there exists a trusted quantum-assisted third party TP with $n = 3$ voters $\{P_1, P_2, P_3\}$, and the number of candidates is $d = 3$ indexed by $\{0, 1, 2\}$.

First, the TP releases the candidate set and the maximum number of participants. Subsequently, the three voters cast their votes independently: P_1 and P_3 vote for Candidate 1, while P_2 votes for Candidate 2, i.e., $x_1 = 0, x_2 = 1, x_3 = 0$. According to the protocol, each voter constructs a voting vector of length 3: $v_1 = (1, 0, 0)$, $v_2 = (0, 1, 0)$, and $v_3 = (1, 0, 0)$.

Then, the three voters generate a shared random mask matrix $R = (r_{il})$ via the SQSMS protocol, satisfying

$$\sum_{i=1}^3 r_{il} \equiv 0 \pmod{10}. \quad (37)$$

Assume the generated mask matrix is

$$R = \begin{pmatrix} 2 & 4 & 3 \\ 5 & 1 & 6 \\ 3 & 5 & 1 \end{pmatrix}.$$

Each voter encrypts its voting vector by $v_{il}^* = (v_{il} + r_{il}) \bmod 10$, yielding the encrypted voting vectors $v_1^* = (3, 4, 3)$, $v_2^* = (5, 2, 6)$, and $v_3^* = (4, 5, 1)$, which are then transmitted to the TP.

After receiving all the encrypted vectors, the TP initializes the vote vector $W = (w_0, w_1, w_2)$, computes

$$w_l = \sum_{i=1}^3 (v_{il} + r_{il}) \bmod 10,$$

and obtains $W = (2, 1, 0)$. Since the column sum of masks is zero modulo d , the random masks cancel out automatically during aggregation, and the statistical result coincides with the real vote count. It follows that Candidate 0 obtains 2 votes, Candidate 1 obtains 1 vote, and Candidate 2 obtains 0 votes.

This example demonstrates that the TP only obtains encrypted data throughout the process and cannot infer the specific vote of any voter. The protocol achieves anonymity of voting content and voter identity while guaranteeing the correctness of statistical results.

Correctness. The correctness of the SQSMAV protocol can be directly derived from the correctness of the SQSMS protocol. Each voter encodes its vote into a unit vector, and all participants generate shared masks satisfying

$$\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d} \quad (38)$$

via the SQSMS protocol. When the TP performs bitwise aggregation, the random mask terms in the encrypted data cancel each other out modulo d , yielding the true statistical result

$$w_l = \sum_{i=1}^n v_{il}.$$

Accordingly, the TP can accurately count the votes of each candidate and correctly determine the winner with the highest votes. Therefore, the protocol guarantees the correctness of voting statistics under the honest execution of all participants.

Security. The SQSMAV protocol inherits the information-theoretic security of the SQSMS protocol. Since each mask r_{il} obeys a uniform distribution modulo d , the encrypted data is statistically independent of the original vote value. Thus, neither the TP nor external eavesdroppers can recover the private vote of any voter. Meanwhile, all voters submit their vectors anonymously; the TP only obtains the aggregated result and cannot establish the correspondence between voting content and voter identity, realizing identity anonymity. Under the semi-honest and non-full-collusion model, any subset of participants cannot eliminate the uncertainty introduced by unknown masks. Hence, the protocol can effectively resist collusion attacks and preserve voting privacy.

5.2. Semi-Quantum Anonymous Auction Protocol

Definition 2 (Semi-quantum anonymous auction). Suppose there exists a semi-honest auctioneer TP and n bidders $\{P_1, P_2, \dots, P_n\}$. Each bidder P_i holds a private bid $x_i \in [0, N - 1]$. The objective is to determine the unique highest bidder while preserving bid privacy and identity anonymity.

Protocol 3. Semi-Quantum Secure Multi-party Anonymous Auction Protocol (SQSMAA).

Input: Each bidder P_i submits its private bid x_i .

Output: The TP announces the unique winner without disclosing any bid values.

Step 1. Parameter negotiation. The TP and bidders agree on two public parameters: subinterval width Δ and the number of intervals $L = \lceil N/\Delta \rceil$. The whole range is divided into L consecutive subintervals: $[0, \Delta), [\Delta, 2\Delta), \dots, [N - \Delta, N)$. The modulus parameter satisfies $d > n$.

Step 2. Vector mapping. Each bidder P_i constructs an L -length vector v_i . If $x_i \in [l\Delta, (l+1)\Delta)$ then set $v_{il} = 1$ and 0 otherwise.

Step 3. Mask generation and encryption. All bidders execute the SQSMS protocol to generate the shared mask matrix R as shown in Equation (34). Each bidder encrypts its vector bitwise:

$$v_{il}^* = v_{il} + r_{il}, \quad l = 0, 1, \dots, L-1. \quad (39)$$

The encrypted vector v_i^* is sent to the TP via a classical channel.

Step 4. Preliminary judgment. The TP performs the following for $l = 0, 1, \dots, L-1$:

- If $\sum_{i=1}^n (v_{il} + r_{il}) \bmod d = 0$ then no bid in this interval: continue;
- If $\sum_{i=1}^n (v_{il} + r_{il}) \bmod d > 1$ then multiple bidders exist: go to Step 5;
- If $\sum_{i=1}^n (v_{il} + r_{il}) \bmod d = 1$ then unique bidder found: go to Step 6.

Step 5. Fine-grained iteration. If multiple bidders exist in the current interval, reduce Δ , repartition the range, and repeat Steps 1–4 until the unique highest bidder is found.

Step 6. Winner announcement. If only one bidder exists in the current interval then the TP announces the winner without revealing any bid values or private information.

Example 2. To illustrate the execution of the SQSMAA protocol we provide a concrete example. Consider a semi-honest auctioneer TP and $n = 3$ bidders $\{P_1, P_2, P_3\}$ with a bid range $[0, 15]$ ($N = 16$). Their private bids are $x_1 = 5$, $x_2 = 12$, and $x_3 = 9$.

First, the TP and bidders set $\Delta = 4$ and $L = \lceil 16/4 \rceil = 4$. The range is divided into $[0, 4), [4, 8), [8, 12), [12, 16)$. The bidders construct vectors: $v_1 = (0, 1, 0, 0)$, $v_2 = (0, 0, 0, 1)$, $v_3 = (0, 0, 1, 0)$.

They generate a shared mask matrix $R = (r_{il})$ via SQSMS, satisfying

$$\sum_{i=1}^3 r_{il} \equiv 0 \pmod{d}. \quad (40)$$

Let $d = 10$ and let the mask matrix be

$$R = \begin{pmatrix} 3 & 2 & 4 & 1 \\ 5 & 3 & 2 & 6 \\ 2 & 5 & 4 & 3 \end{pmatrix}.$$

Each bidder encrypts its vector by $v_{il}^* = (v_{il} + r_{il}) \bmod 10$, obtaining $v_1^* = (3, 3, 4, 1)$, $v_2^* = (5, 3, 2, 7)$, $v_3^* = (2, 5, 5, 3)$.

The TP calculates

$$\sum_{i=1}^3 (v_{il} + r_{il}) \bmod 10$$

and obtains $(0, 1, 1, 1)$. Since masks cancel out, the result reflects the real distribution. The TP checks from the highest interval and finds that the fourth interval has a count of 1, so P_2 is the winner. The bid values and identities remain anonymous.

Correctness. The correctness of SQSMAA follows directly from that of SQSMS. By mapping bids to interval vectors and encrypting with zero-sum masks the TP obtains

$$\sum_{i=1}^n (v_{il} + r_{il}) \equiv \sum_{i=1}^n v_{il} \pmod{d}, \quad l = 0, 1, \dots, L-1, \quad (41)$$

which accurately counts bidders in each interval. By checking from high to low and refining intervals the TP correctly identifies the unique highest bidder.

Security. All bid vectors are encrypted with uniformly random masks modulo d . The TP cannot recover any private bid and only obtains interval-level statistics. Only the winner's identity is disclosed, and no exact bids are leaked. Masks in different rounds are independent, preventing correlation attacks. Under the semi-honest model, the protocol resists eavesdropping and limited collusion, ensuring bid privacy and identity anonymity.

5.3. Semi-Quantum Anonymous Sorting Protocol

Definition 3 (Semi-quantum anonymous ranking). Suppose there are n participants $\{U_1, U_2, \dots, U_n\}$ and a trusted third party TP. Each participant U_i holds a private input $x_i \in [0, L-1]$. The protocol aims to anonymously compute the ascending or descending ranking position of each participant among all the data without disclosing any private input values and identity information. The modulus parameter satisfies $d > n$ to avoid ambiguity in aggregation statistics.

Protocol 4. Semi-Quantum Secure Multi-party Anonymous Ranking Protocol (SQSMAS).

Input: Private integer x_i of participant U_i .

Output: Each participant obtains its own ranking result, while it cannot infer the private inputs or rankings of others.

Step 1. Private value encoding. Each participant U_i maps its private input x_i into an L -dimensional vector v_i defined as

$$v_i = [v_{i0}, v_{i1}, \dots, v_{i(L-1)}], \quad v_{ij} = \begin{cases} 1, & x_i = j, \\ 0, & \text{otherwise.} \end{cases} \quad (42)$$

Step 2. Mask generation. All participants negotiate and generate the mask set R via the SQSMS protocol, as shown in Equation (34). Each participant U_i encrypts its vector bitwise with the generated mask:

$$v_{il}^* = (v_{il} + r_{il}) \pmod{d}, \quad l = 0, 1, \dots, L-1. \quad (43)$$

The encrypted vector is denoted as v_i^* and transmitted to the TP through the classical channel.

Step 3. Encrypted aggregation. The TP aggregates the vector data of all the participants bit by bit:

$$w_l = \sum_{i=1}^n (v_{il} + r_{il}) \pmod{d} = \left(\sum_{i=1}^n v_{il} \right) \pmod{d}, \quad l = 0, 1, \dots, L-1. \quad (44)$$

Since the sum of all the masks satisfies the zero-sum property modulo d , the correctness of the final statistical result is guaranteed.

Step 4. Anonymous ranking publication. The TP publishes the aggregated vector $W = [w_0, w_1, \dots, w_{L-1}]$ to all participants. Combined with its own private input x_i , each participant locally calculates its ascending and descending ranking:

Ascending ranking:

$$\text{Rank}_{\text{asc}}(x_i) = 1 + \sum_{l=0}^{x_i-1} w_l. \quad (45)$$

Descending ranking:

$$\text{Rank}_{\text{desc}}(x_i) = 1 + \sum_{l=x_i+1}^{L-1} w_l. \quad (46)$$

Example 3. To illustrate the execution of the SQSMAS protocol, a concrete example is presented. Consider a trusted third party TP and $n = 3$ participants $\{U_1, U_2, U_3\}$. The private input range is $[0, 4]$, i.e., $L = 5$. The private inputs of the three participants are $x_1 = 1$, $x_2 = 3$, and $x_3 = 2$.

Each participant constructs an encoded vector $\mathbf{v}_i = [v_{i0}, v_{i1}, \dots, v_{i4}]$ of length L , where $v_{ij} = 1$ if $j = x_i$ and $v_{ij} = 0$ otherwise. The corresponding vectors are $\mathbf{v}_1 = (0, 1, 0, 0, 0)$, $\mathbf{v}_2 = (0, 0, 0, 1, 0)$, and $\mathbf{v}_3 = (0, 0, 1, 0, 0)$.

All participants generate a shared random mask matrix $\mathbf{R} = (r_{il})$ via the SQSMS protocol, satisfying

$$\sum_{i=1}^3 r_{il} \equiv 0 \pmod{d}. \quad (47)$$

Set the modulus $d = 10$, and the mask matrix is

$$\mathbf{R} = \begin{pmatrix} 2 & 3 & 4 & 1 & 5 \\ 5 & 4 & 1 & 6 & 2 \\ 3 & 3 & 5 & 3 & 3 \end{pmatrix}.$$

Each participant encrypts its vector by $\mathbf{v}_{il}^* = (v_{il} + r_{il}) \bmod 10$, obtaining encrypted vectors $\mathbf{v}_1^* = (2, 4, 4, 1, 5)$, $\mathbf{v}_2^* = (5, 4, 1, 7, 2)$, and $\mathbf{v}_3^* = (3, 3, 6, 3, 3)$, which are sent to the TP.

After receiving all the encrypted vectors the TP performs bitwise aggregation:

$$w_l = \sum_{i=1}^3 (v_{il} + r_{il}) \bmod 10.$$

Since the column sum of masks is zero modulo d , the random masks cancel out automatically, and the true statistical result is $\mathbf{W} = (0, 1, 1, 1, 0)$, which indicates that each value 1, 2, and 3 appears once.

Subsequently, the TP publishes $\mathbf{W}$ to all participants, and each one calculates its ranking locally based on its private input. According to the ascending ranking formula $\text{Rank}_{\text{asc}} = 1 + \sum_{l=0}^{x_i-1} w_l$: Participant U_1 with $x_1 = 1$ obtains an ascending rank $1 + w_0 = 1$; Participant U_3 with $x_3 = 2$ obtains an ascending rank $1 + w_0 + w_1 = 2$; Participant U_2 with $x_2 = 3$ obtains an ascending rank $1 + w_0 + w_1 + w_2 = 3$.

According to the descending ranking formula $\text{Rank}_{\text{desc}} = 1 + \sum_{l=x_i+1}^{L-1} w_l$: U_2 gets the first rank, U_3 gets the second rank, and U_1 gets the third rank in descending order.

In the whole process, the TP only obtains encrypted data and publishes the aggregated statistical results. No participant can acquire the exact input value or identity information of others. The protocol preserves data privacy and identity anonymity while guaranteeing the correctness of the sorting results.

Correctness. The correctness of the SQSMAS protocol stems from the unbiased aggregation property of the SQSMS protocol. Each participant encodes its private input into a unit vector, encrypts the vector with shared masks, and sends it to the TP. Since the masks satisfy $\sum_{i=1}^n r_{ij} \equiv 0 \pmod{d}$, the aggregation result calculated by the TP is $w_l = \sum_{i=1}^n v_{il}$, which accurately counts the occurrence frequency of each value. Based on the statistical vector, each participant can locally compute its exact ascending or descending ranking without recovering the original raw data.

Security. The SQSMAS protocol inherits the privacy-preserving characteristics of the SQSMS protocol. All uploaded data are encrypted by random masks and statistically independent of the original inputs. Thus, neither the TP nor external adversaries can recover

the exact ownership of individual private inputs. Meanwhile, the TP only publishes the aggregated statistical vector rather than individual raw data. Each participant can only compute its own ranking with its private input and cannot deduce the specific values or identities of the other participants. Under the semi-honest and non-full-collusion model the uncertainty introduced by random masks guarantees the indistinguishability of private inputs and achieves a good balance between ranking availability and input privacy.

6. Conclusions

In this paper, we have proposed an efficient Semi-Quantum Secure Multi-party Summation protocol based on d -dimensional n -particle entangled states. Designed under the semi-quantum framework, the protocol generates cancelable random masks by exploiting the global correlation of entangled states to realize secure aggregation of private inputs. The entire computation relies only on quantum measurement operations, without requiring pre-shared keys or a multi-TP collaborative architecture. It improves communication efficiency and structural complexity while maintaining satisfactory security. Furthermore, we have conducted a formal analysis of the correctness and security of the protocol, and we constructed a corresponding quantum circuit model on the IBM Qiskit platform for simulation verification. Moreover, we extended the basic protocol to design application schemes for anonymous voting, auction and sorting, which demonstrate the good scalability and application potential of the proposed method.

Although the protocol achieves promising results in the research of Semi-Quantum Secure Multi-party Summation there still exists room for further improvement. First, the protocol exhibits relatively high dependence on the quantum capability of the trusted third party. In future work, adaptive mechanisms will be investigated to enable dynamic adaptation according to the available quantum resources of the TP, so as to reduce such dependence and enhance the flexibility and scalability of the protocol. In addition, the current scheme lacks global process simulation, making it difficult to comprehensively evaluate its practical performance. Future research could establish a global simulation model to analyze the protocol behavior under diverse scenarios, identify inefficient parts, and optimize the overall structure. In summary, subsequent research will focus on improving quantum resource utilization and conducting comprehensive scenario-based simulations so as to further refine the protocol and validate its computational performance and engineering feasibility.

Author Contributions: Conceptualization, D.W. and D.Y.; methodology, D.W. and D.Y.; validation, D.W.; formal analysis, D.Y.; writing—original draft preparation, D.W.; writing—review and editing, H.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Basic Research Program of Jiangsu grant number BK20231142.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Yao, A.C.C. Protocols for Secure Computations. In Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS), Chicago, IL, USA, 3–5 November 1982; pp. 160–164.
2. Goldreich, O.; Micali, S.; Wigderson, A. How to Play Any Mental Game or A Completeness Theorem for Protocols with Honest Majority. In Proceedings of the 19th Annual ACM Symposium on Theory of Computing (STOC), New York, NY, USA, 25–27 May 1987; pp. 218–229.

3. Yao, A.C.C. How to Generate and Exchange Secrets. In Proceedings of the 27th Annual Symposium on Foundations of Computer Science (FOCS), Toronto, ON, Canada, 27–29 October 1986; pp. 162–167.
4. Beaver, D. Efficient Multiparty Protocols Using Circuit Randomization. In *Proceedings of the Advances in Cryptology—CRYPTO'91*; Springer: Berlin/Heidelberg, Germany, 1991; pp. 420–432.
5. Zhang, H.; Zeng, K. Communication-Aware Secret Share Placement in Hierarchical Edge Computing. *IEEE Internet Things J.* **2022**, *9*, 3717–3728. [[CrossRef](#)]
6. Even, S.; Goldreich, O.; Lempel, A. A Randomized Protocol for Signing Contracts. *Commun. ACM* **1985**, *28*, 637–647. [[CrossRef](#)]
7. Peikert, C.; Vaikuntanathan, V.; Waters, B. A Framework for Efficient and Composable Oblivious Transfer. In *Proceedings of the Advances in Cryptology—CRYPTO 2008*; Springer: Berlin/Heidelberg, Germany, 2008; pp. 554–571.
8. Zhang, J.; Li, L.; Tang, Y.; Luo, S.; Yang, Y.; Xin, Y. Secure Two-Party Computation of Solid Triangle Area and Tetrahedral Volume Based on Cloud Platform. *PLoS ONE* **2019**, *14*, e0217067. [[CrossRef](#)] [[PubMed](#)]
9. Elgamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [[CrossRef](#)]
10. Paillier, P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. In *Proceedings of the Advances in Cryptology—EUROCRYPT 1999*; Springer: Berlin/Heidelberg, Germany, 1999.
11. Cao, X.-K.; Wang, C.-D.; Lai, J.-H.; Huang, Q.; Chen, C.L.P. Multiparty Secure Broad Learning System for Privacy Preserving. *IEEE Trans. Cybern.* **2023**, *53*, 6636–6648. [[CrossRef](#)] [[PubMed](#)]
12. Huang, J.; He, D.; Chen, Y.; Khan, M.K.; Luo, M. A Blockchain-Based Self-Tallying Voting Protocol with Maximum Voter Privacy. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3808–3820. [[CrossRef](#)]
13. Satizábal, C.; Páez, R.; Forné, J. Secure Internet Voting Protocol (SIVP): A Secure Option for Electoral Processes. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 3647–3660. [[CrossRef](#)]
14. Morohashi, G.; Chida, K.; Hirota, K.; Kikuchi, H. Secure Multiparty Computation for Comparator Networks. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2008**, *E91-A*, 2349–2355. [[CrossRef](#)]
15. Shor, P.W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS), Santa Fe, NM, USA, 20–22 November, 1994; pp. 124–134.
16. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
17. Zhang, Y.; Yao, Y.; Sun, H.; Zhang, K.; Song, T. A New Hybrid Protocol That Simultaneously Achieves Quantum Multiparty Summation and Ranking. *Adv. Quantum Technol.* **2024**, *7*, 2400078. [[CrossRef](#)]
18. Xu, X.T.; Shi, R.H.; Ke, W.Y. Decentralized Quantum Anonymous Veto Voting Scheme Based on Measurement-Device-Independent. *Phys. Scr.* **2023**, *98*, 095116. [[CrossRef](#)]
19. Ke, W.Y.; Shi, R.H.; Yu, H.; Xu, X. A Receipt-Free Quantum Voting Protocol Based on Quantum Public Key Encryption and Quantum Key Agreement. *Phys. Scr.* **2023**, *98*, 065112. [[CrossRef](#)]
20. Shi, R.H.; Liu, B.; Zhang, M.W. Measurement-Device-Independent Quantum Secure Multiparty Summation. *Quantum Inf. Process.* **2022**, *21*, 122. [[CrossRef](#)]
21. Shi, R.H.; Zhang, S. Quantum Solution to a Class of Two-Party Private Summation Problems. *Quantum Inf. Process.* **2017**, *16*, 225. [[CrossRef](#)]
22. Sutradhar, K.; Om, H. Hybrid Quantum Protocols for Secure Multiparty Summation and Multiplication. *Sci. Rep.* **2020**, *10*, 9097. [[CrossRef](#)] [[PubMed](#)]
23. Li, X.B.; Xiong, Y.Y.; Zhang, C. Secure Multiparty Quantum Computation for Summation and Data Sorting. *Quantum Inf. Process.* **2024**, *23*, 321. [[CrossRef](#)]
24. Wang, Y.L.; Hu, P.C.; Xu, Q.L. Quantum Secure Multi-Party Summation Based on Entanglement Swapping. *Quantum Inf. Process.* **2021**, *20*, 319. [[CrossRef](#)]
25. Yi, X.; Cao, C.; Fan, L.; Zhang, R. Quantum Secure Multi-Party Summation Protocol Based on Blind Matrix and Quantum Fourier Transform. *Quantum Inf. Process.* **2021**, *20*, 249. [[CrossRef](#)]
26. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Quantum Inf. Comput.* **2007**, *7*, 1463–1474.
27. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semi-Quantum Key Distribution. *Phys. Rev. A* **2009**, *79*, 032341. [[CrossRef](#)]
28. Zhang, C.; Huang, Q.; Long, Y.; Sun, Z. Secure Three-Party Semi-Quantum Summation Using Single Photons. *Int. J. Theor. Phys.* **2021**, *60*, 3478–3487. [[CrossRef](#)]
29. Ye, T.-Y.; Xu, T.-J.; Geng, M.-J.; Chen, Y. Two-Party Secure Semi-Quantum Summation Against the Collective-Dephasing Noise. *Quantum Inf. Process.* **2022**, *21*, 118. [[CrossRef](#)]
30. Tian, Y.; Zhang, N.; Ye, C.; Bian, G.; Li, J. Different Secure Semi-Quantum Summation Models Without Measurement. *EPJ Quantum Technol.* **2024**, *11*, 35. [[CrossRef](#)]
31. Lv, S.X.; Jiao, X.F.; Zhou, P. Multiparty Quantum Computation for Summation and Multiplication with Mutually Unbiased Bases. *Int. J. Theor. Phys.* **2019**, *58*, 2872–2882. [[CrossRef](#)]

32. Jing, R.H.; Huang, Y.B.; Yang, J.; Bi, A.A.; Zhang, J.Y.; Xia, K.B.; Zhou, P. Deterministic Bidirectional Hierarchical Teleportation of an Arbitrary High-Dimensional Multi-Particle State with a Partially Entangled Quantum Channel. *Eur. Phys. J. Plus* **2024**, *139*, 894. [[CrossRef](#)]
33. Ye, C.; Li, J.; Chen, X.; Dong, M.; Ota, K.; Khalique, A.; Durad, M.H. Semi-Quantum Secure Multiparty Summation and Its Applications to Anonymous Auction and Ranking. *Adv. Quantum Technol.* **2024**, *7*, 2300347. [[CrossRef](#)]
34. Lian, J.Y.; Ye, T.Y. Hybrid Protocols for Multi-Party Semiquantum Private Comparison, Multiplication and Summation Without a Pre-Shared Key Based on d-Dimensional Single-Particle States. *EPJ Quantum Technol.* **2024**, *11*, 17. [[CrossRef](#)]
35. Tang, W.; Yu, S.; Oh, C.H. Greenberger-Horne-Zeilinger Paradoxes from Qudit Graph States. *Phys. Rev. Lett.* **2013**, *110*, 100403. [[CrossRef](#)] [[PubMed](#)]
36. Designolle, S.; Augusiak, R.; Sacchi, M.F.; Cirac, J.I. Detecting the Dimensionality of Genuine Multiparticle Entanglement. *Sci. Adv.* **2024**, *10*, eadq4467. [[CrossRef](#)] [[PubMed](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.