Lian and Ye *EPJ Quantum Technology* (2024) 11:17
https://doi.org/10.1140/epjqt/s40507-024-00228-y

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Hybrid protocols for multi-party semiquantum private comparison, multiplication and summation without a pre-shared key based on d-dimensional single-particle states

Jiang-Yuan Lian[1] and Tian-Yu Ye[1*]

*Correspondence:
happyyty@aliyun.com
[1]College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R. China

Abstract

In this paper, by utilizing d-dimensional single-particle states, three semiquantum cryptography protocols, i.e., the multi-party semiquantum private comparison (MSQPC) protocol, the multi-party semiquantum multiplication (MSQM) protocol and the multi-party semiquantum summation (MSQS) protocol, can be achieved simultaneously under the assistance of two semi-honest quantum third parties (TPs). Here, the proposed MSQPC scheme is the only protocol which is devoted to judging the size relationship of secret integers from more than two semiquantum participants without a pre-shared key. And the proposed MSQM protocol absorbs the innovative concept of semiquantumness into quantum multiplication for the first time, which can calculate the modulo d multiplication of private inputs from more than two semiquantum users. As for the proposed MSQS protocol, it is the only semiquantum summation protocol which aims to accomplish the modulo d addition of more than three semiquantum users' private integers. Neither quantum entanglement swapping nor unitary operations are necessary in the three proposed protocols. The security analysis verifies in detail that both the external attacks and the internal attacks can be resisted in the three proposed protocols.

Keywords: Multi-party semiquantum private comparison; Multi-party semiquantum multiplication; Multi-party semiquantum summation; d-dimensional single-particle states

1 Introduction

In the year of 1984, the pioneer protocol of quantum cryptography, which became known as BB84 protocol hereafter, was proposed by Bennett and Brassard [1]. As a quantum key distribution (QKD) protocol, BB84 protocol successfully integrated quantum mechanics into classical cryptography by employing the polarization of single photons. Since then, plenty of quantum cryptography protocols [1–39] have been born in turn, which can be categorized into quantum secret sharing (QSS) [2–10], quantum private compar-

Springer

ison (QPC) [11–19], quantum multiplication (QM) [20–25], quantum summation (QS) [20–22, 26–36], quantum blockchain [37, 38], quantum secure multiparty computation [39] and so on. The application of quantum cryptography into practical circumstances, for example, applying quantum cryptographic protocol into vehicular communication [40], has also been explored. Different from classical cryptography, quantum cryptography provides the unconditional security theoretically based on the laws of quantum mechanics. Nevertheless, not everyone has ability to afford the expensive quantum devices.

Thereupon, a novel concept of semiquantumness was put forward by Boyer *et al.* [41, 42] in the year of 2007, which means the birth of semiquantum cryptography. Unlike quantum cryptography schemes, semiquantum cryptography schemes [41–44] don't require semiquantum participants to prepare or measure quantum superposition states and quantum entangled states, which greatly saves experiment costs. In other words, the quantum users need to equip complete quantum capabilities, while the semiquantum participants are restricted to own limited abilities. In semiquantum cryptography, the first semiquantum private comparison (SQPC) protocol was proposed by Chou *et al.* [45] based on entanglement swapping of Bell states in the year of 2016, the first semiquantum summation (SQS) protocol was put forward by Zhang *et al.* [46] based on single photons in the year of 2021, and the semiquantum multiplication (SQM) protocol hasn't been designed until now.

Speaking of SQPC, it can be divided into two kinds: SQPC of equality [45, 47–50] and SQPC of size relationship [51–56]. Compared with the former kind, the latter kind has more functions on determining the relationship of semiquantum participants' private inputs. In the year of 2021, by adopting d-dimensional Bell states, Zhou *et al.* [51] designed a SQPC scheme of size relationship with a pre-shared key; and by using d-dimensional GHZ states, Wang *et al.* [52] proposed a SQPC protocol of size relationship with a pre-shared key. In the year of 2022, by employing d-dimensional single-particle states, Li *et al.* [53] put forward two SQPC protocols of size relationship, each of which requires a pre-shared key, where the first protocol and the second protocol use the distribution model and the circle model to transmit particles, respectively; by utilizing d-dimensional Bell states, Luo *et al.* [54] designed a SQPC scheme of size relationship which requires a pre-shared key; and by employing d-dimensional single-particle states, Geng *et al.* [55] put forward a SQPC protocol of size relationship with a pre-shared key, where TP has no knowledge about the final comparison results; and in the year of 2023, Ye and Lian [56] put forward the first multi-party semiquantum private comparison (MSQPC) protocol of size relationship with d-dimensional single-particle states. Compared to SQPC schemes, SQS protocols [46, 57, 58] have been few up to now. More seriously, there is no SQS scheme which can implement the modulo d addition of secret integers from more than three semiquantum participants within one round implementation.

According to the foregoing discussion, in this paper, we utilize d-dimensional single-particle states to design three semiquantum cryptography protocols, i.e., the MSQPC protocol, the multi-party semiquantum multiplication (MSQM) protocol and the multi-party semiquantum summation (MSQS) protocol. Note that only under the assistance of two semi-honest quantum third parties (TPs) can the goals of the three proposed protocols be achieved, where the semi-honest TPs are permitted to try their best to eavesdrop secret integers of semiquantum participants but cannot collude with anyone else. The proposed MSQPC protocol is the only MSQPC protocol which can implement the com-

parison of size relationship of more than two semiquantum participants' private inputs within one execution of protocol, with no requirement of a pre-shared key. The proposed MSQM protocol is the first scheme absorbing the innovative concept of semiquantumness into quantum multiplication, which is devoted to computing the modulo d multiplication of secret integers from more than two semiquantum users within one round implementation. Note that within a d-dimensional quantum system, semiquantum users are typically constrained to the following operations: (a) measuring the qudits in the Z basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$; (b) preparing the fresh qudits in the Z basis; (c) transmitting or reflecting the qudits without disturbance; and (d) recordering the qudits via various delay lines. As for the proposed MSQS protocol, it is also the pioneer scheme of SQS, aiming to compute the modulo d addition of private integers from more than three semiquantum users within one execution of protocol. Neither quantum entanglement swapping nor unitary operations are required in the three proposed protocols. Besides, the usage of quantum resources for the three proposed schemes is identical, as the only section where quantum resources are utilized is in Sect. 2.1 during the key-sharing process.

2 Description of protocols

In a d-dimensional Hilbert space, two common conjugate bases can be described as

$$T_1 = \left\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\right\} \tag{1}$$

and

$$T_2 = \left\{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\right\}. \tag{2}$$

Here, F is the d-dimensional discrete quantum Fourier transform, $F|t\rangle = \frac{1}{\sqrt{d}} \times \sum_{\delta=0}^{d-1} e^{\frac{2\pi i \delta t}{d}} |\delta\rangle$ and $t = 0, 1, \ldots, d-1$.

There are N semiquantum users, $P_1, P_2, \ldots, P_N$, and two quantum TPs, TP_1 and TP_2, where the TPs are required to have complete quantum capabilities, while $P_1, P_2, \ldots, P_N$ are merely asked to possess restricted quantum abilities. It is worth noting that both TP_1 and TP_2 are semi-honest, which means that they can launch all possible attacks to steal private inputs of N semiquantum users except colluding with anyone else. Assume that P_n possesses a L-length secret integer string $p_n = \{p_n^1, p_n^2, \ldots, p_n^L\}$, where P_n denotes the nth semiquantum participant, p_n^i denotes the ith private integer of nth semiquantum participant, $p_n^i \in \{0, 1, \ldots, d-1\}$, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. The quantum channels are assumed to be ideal, and the classical channels are assumed to be authenticated.

This paper proposes a hybrid protocol which initially designs a semiquantum key distribution (SQKD) scheme based on d-dimensional single particles in Sect. 2.1, followed by the use of traditional mathematical methods to achieve multi-party private comparison, multiplication, and summation in Sect. 2.2, Sect. 2.3 and Sect. 2.4, respectively. The term "hybrid" means that the proposed multi-party semiquantum private comparison scheme, the proposed multi-party semiquantum multiplication scheme and the proposed multi-party semiquantum summation scheme share the SQKD scheme based on d-dimensional single-particle states together. The SQKD scheme based on d-dimensional single particles aims to create a semiquantum private key between P_n and TP_1 and a semiquantum private key between P_n and TP_2 by using d-dimensional single particles.

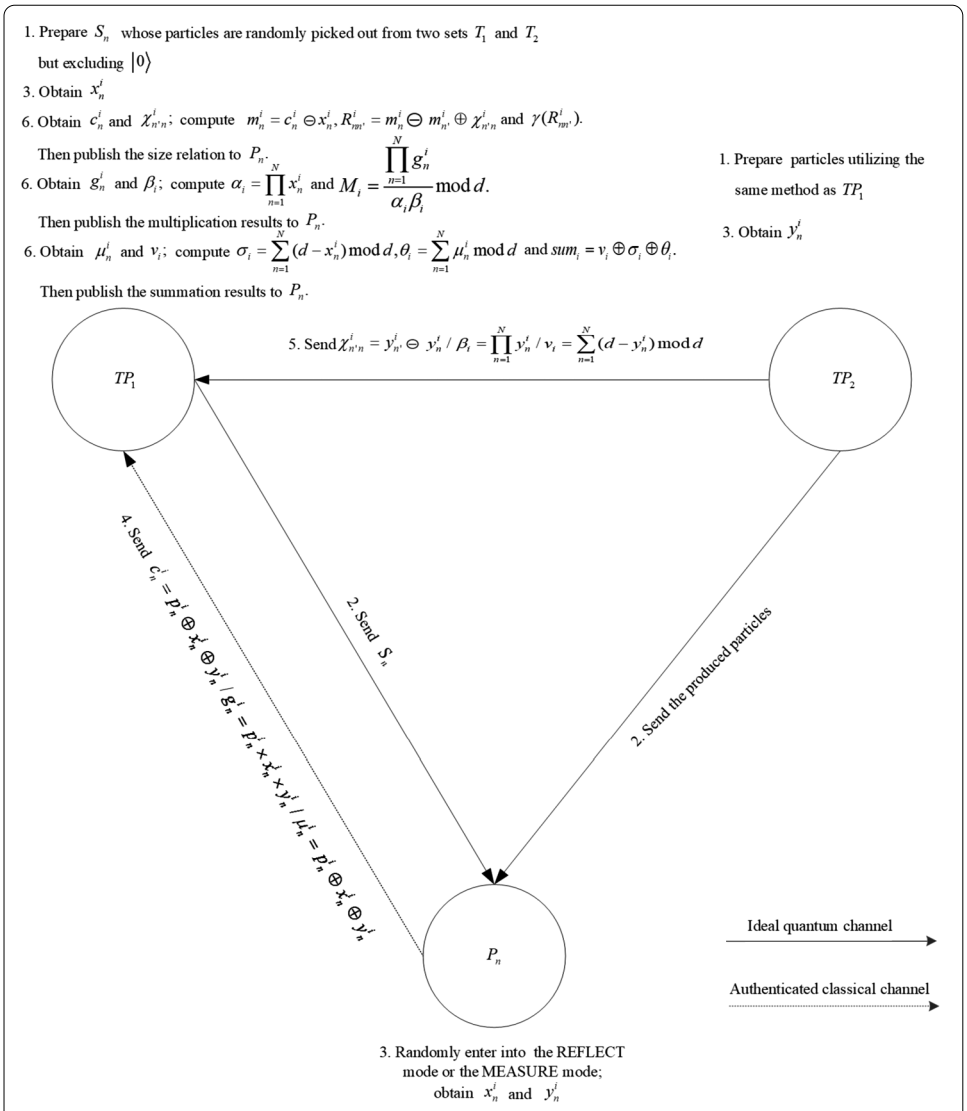

Figure 1 The flow chart for the proposed hybrid protocols

To make it much easier to understand the process of the proposed hybrid protocols, we create a concise flowchart, depicted in Fig. 1.

2.1 Common procedures of protocols

Step 1: TP_1 prepares N d-dimensional single-particle state sequences $S_1, S_2, \ldots, S_N$ whose particles are randomly picked out from two sets T_1 and T_2 but excluding $|0\rangle$. Note that for the successful implementation of the three proposed protocols, the minimum number of particles in S_n should be $8L$. Here, let $S_n = \{S_n^1, S_n^2, \ldots, S_n^{8L}\}$ for $n = 1, 2, \ldots, N$, where S_n^l denotes the lth particle of S_n and $l = 1, 2, \ldots, 8L$. Furthermore, TP_1 sends S_n to P_n through a quantum channel. Note that except the first particle, TP_1 sends out the next particle of S_n to P_n only after receiving the previous one from P_n.

Step 2: P_n randomly enters into the REFLECT mode or the MEASURE mode after gaining the lth particle from TP_1. Here, the REFLECT mode means to reflect the received particle back without any disturbance, while the MEASURE mode implies to measure the

Table 1 TP_1's operations under different Cases

Case	The preparation basis of TP_1	The mode of P_n	The operations of TP_1
Case 1	The T_1 basis	The REFLECT mode	Measuring $S_n^{l'}$ with the T_1 basis
Case 2	The T_2 basis	The REFLECT mode	Measuring $S_n^{l'}$ with the T_2 basis
Case 3	The T_2 basis	The MEASURE mode	Ignoring $S_n^{l'}$
Case 4	The T_1 basis	The MEASURE mode	Measuring $S_n^{l'}$ with the T_1 basis

received particle with the T_1 basis, record the measurement result, prepare the fresh quantum state as found and return the fresh particle back to the sender. The new sequence after P_n performs her operations on S_n is represented by S'_n.

Step 3: After receiving all particles of S'_n from P_n, TP_1 announces P_n the positions where the particles were produced within the T_1 basis, and P_n publishes TP_1 her specific operation modes on the particles of S_n. Based on the announced information, TP_1 implements the corresponding operations as shown in Table 1.

Case 1: P_n has applied the REFLECT mode to the received particle prepared within the T_1 basis. After measuring $S_n^{l'}$ with the T_1 basis, TP_1 compares her measurement result with the corresponding initially prepared state to determine whether there is an eavesdropper or not, where $l \in \{1, 2, \ldots, 8L\}$. If there is no eavesdropper, this protocol will be proceeded;

Case 2: P_n has applied the REFLECT mode to the received particle prepared within the T_2 basis. After measuring $S_n^{l'}$ with the T_2 basis, TP_1 compares her measurement result with the corresponding initially prepared state to judge whether there is a stealer or not, where $l \in \{1, 2, \ldots, 8L\}$. If there is no stealer, this protocol will be proceeded;

Case 3: P_n has applied the MEASURE mode to the received particle prepared within the T_2 basis and TP_1 takes no action. It is noteworthy that this Case is ignored;

Case 4: P_n has applied the MEASURE mode to the received particle prepared within the T_1 basis. TP_1 measures $S_n^{l'}$ with the T_1 basis. TP_1 randomly picks out half particles belonging to this Case in her hand. Then, TP_1 announces P_n the selected positions, and then P_n publishes TP_1 her measurement results on the corresponding positions. Afterward, TP_1 can know whether there is an eavesdropping behavior or not by comparing her measurement results, the corresponding initially prepared states and the measurement results published by P_n. If there is no eavesdropping behavior, this protocol will be proceeded.

Step 4: TP_1 counts the number of remaining particles in Case 4. If this quantity is less than L, the communication will be suspended and restarted from Step 1. Then, P_n and TP_1 select the first L particles from the remaining particles in Case 4 and record the corresponding measurement results as $x_n = \{x_n^1, x_n^2, \ldots, x_n^L\}$, where $x_n^i \in \{1, 2, \ldots, d-1\}$, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$.

Step 5: TP_2 executes the same procedures as TP_1 in Steps (1)–(4), in order to make TP_2 and P_n also share a L-length secret sequence represented by $y_n = \{y_n^1, y_n^2, \ldots, y_n^L\}$, where $y_n^i \in \{1, 2, \ldots, d-1\}$, $i = 1, 2, \ldots, L$ and $n = 1, 2, \ldots, N$.

Additionally, it is important to clarify why the minimum particle number in S_n should be $8L$. In Case 4, the number of particles used for privacy comparison should be L, consequently requiring the number of particles for eavesdropping detection greater than or equal to L. This suggests that the particle number in Case 4 should be greater than or equal to $2L$. Given that the particles in S_n are distributed in the four Cases with equal probabilities, the quantity of particles in S_n should be greater than or equal to $8L$.

2.2 Protocol for multi-party semiquantum private comparison

It is necessary to highlight that the value range of p_n^i needs to be reset, i.e., $p_n^i \in \{0, 1, \ldots, h\}$, where $h = \lfloor \frac{d-1}{2} \rfloor$ and the symbol $\lfloor \rfloor$ denotes the floor operation. For instance, if $d = 12$, then $h = \lfloor \frac{12-1}{2} \rfloor = \lfloor 5.5 \rfloor = 5$.

Step 6′: After performing Steps (1)–(5) of Sect. 2.1, P_n calculates

$$c_n^i = p_n^i \oplus x_n^i \oplus y_n^i, \tag{3}$$

where the symbol $\oplus$ represents the modulo d addition, $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. Then, P_n sends c_n^i to TP_1 through an authenticated classical channel. Furthermore, TP_2 computes

$$\chi_{n'n}^i = y_{n'}^i \ominus y_n^i \tag{4}$$

and sends $\chi_{n'n}^i$ to TP_1 through an authenticated classical channel, where the symbol $\ominus$ denotes the modulo d subtraction, $i = 1, 2, \ldots, L$, $n = 1, 2, \ldots, N$, $n' = 2, 3, \ldots, N$ and $n' > n$.

Step 7′: After obtaining $\chi_{n'n}^i$ from TP_2, TP_1 calculates

$$m_n^i = c_n^i \ominus x_n^i \tag{5}$$

and

$$R_{nn'}^i = m_n^i \ominus m_{n'}^i \oplus \chi_{n'n}^i, \tag{6}$$

where $i = 1, 2, \ldots, L$, $n = 1, 2, \ldots, N$, $n' = 2, 3, \ldots, N$ and $n < n'$.

Furthermore, TP_1 makes

$$\gamma\left(R_{nn'}^i\right) = \begin{cases} -1, & \text{if } h < R_{nn'}^i \leq d-1; \\ 0, & \text{if } R_{nn'}^i = 0; \\ 1, & \text{if } 0 < R_{nn'}^i \leq h. \end{cases} . \tag{7}$$

Here, $\gamma(R_{nn'}^i) = -1$ means $p_n^i < p_{n'}^i$; $\gamma(R_{nn'}^i) = 1$ means $p_n^i > p_{n'}^i$; and $\gamma(R_{nn'}^i) = 0$ means $p_n^i = p_{n'}^i$. Finally, TP_1 publishes the comparison results to $P_1, P_2, \ldots, P_N$.

2.3 Protocol for multi-party semiquantum multiplication

Step 6″: After executing Steps (1)–(5) of Sect. 2.1, P_n calculates

$$g_n^i = p_n^i \times x_n^i \times y_n^i, \tag{8}$$

where $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. Then, P_n sends $g_n = \{g_n^1, g_n^2, \ldots, g_n^L\}$ to TP_1 via an authenticated classical channel. Furthermore, TP_2 calculates

$$\beta_i = \prod_{n=1}^{N} y_n^i \tag{9}$$

for $i = 1, 2, \ldots, L$ and sends the sequence $\beta = \{\beta_1, \beta_2, \ldots, \beta_L\}$ to TP_1 through an authenticated classical channel.

Step 7″: After obtaining g_n for $n = 1, 2, \ldots, N$ and the sequence β, TP_1 calculates

$$\alpha_i = \prod_{n=1}^{N} x_n^i \tag{10}$$

and

$$M_i = \frac{\prod_{n=1}^{N} g_n^i}{\alpha_i \beta_i} \bmod d \tag{11}$$

for $i = 1, 2, \ldots, L$. Finally, TP_1 announces $P_1, P_2, \ldots, P_N$ the multiplication result sequence $M = \{M_1, M_2, \ldots M_L\}$, where M_i denotes the modulo d multiplication of $p_1^i, p_2^i, \ldots, p_N^i$.

2.4 Protocol for multi-party semiquantum summation

Step 6‴: After implementing Steps (1)–(5) of Sect. 2.1, P_n calculates

$$\mu_n^i = p_n^i \oplus x_n^i \oplus y_n^i, \tag{12}$$

where $n = 1, 2, \ldots, N$ and $i = 1, 2, \ldots, L$. Then, P_n sends $\mu_n = \{\mu_n^1, \mu_n^2, \ldots, \mu_n^L\}$ to TP_1 via an authenticated classical channel. Moreover, TP_2 computes

$$\nu_i = \sum_{n=1}^{N} \left(d - y_n^i\right) \bmod d \tag{13}$$

for $i = 1, 2, \ldots, L$ and sends the sequence $\nu = \{\nu_1, \nu_2, \ldots, \nu_L\}$ to TP_1 through an authenticated classical channel.

Step 7‴: After obtaining μ_n for $n = 1, 2, \ldots, N$ and the sequence ν, TP_1 calculates

$$\sigma_i = \sum_{n=1}^{N} \left(d - x_n^i\right) \bmod d \tag{14}$$

and

$$\theta_i = \sum_{n=1}^{N} \mu_n^i \bmod d \tag{15}$$

for $i = 1, 2, \ldots, L$. Finally, TP_1 calculates

$$sum_i = \nu_i \oplus \sigma_i \oplus \theta_i \tag{16}$$

for $i = 1, 2, \ldots, L$ and publishes the final summation result sequence $sum = \{sum_1, sum_2, \ldots, sum_L\}$ to $P_1, P_2, \ldots, P_n$, where sum_i represents the modulo d addition of $p_1^i, p_2^i, \ldots, p_N^i$.

3 Correctness analysis

3.1 Correctness analysis of the proposed MSQPC protocol

3.1.1 Output correctness

By combining Eq. (3) with Eq. (5), we infer that

$$m_n^i \ominus m_{n'}^i = \left(c_n^i \ominus x_n^i\right) \ominus \left(c_{n'}^i \ominus x_{n'}^i\right)$$

$$= \left(p_n^i \oplus y_n^i\right) \ominus \left(p_{n'}^i \oplus y_{n'}^i\right)$$
$$= \left(p_n^i \ominus p_{n'}^i\right) \oplus \left(y_n^i \ominus y_{n'}^i\right). \tag{17}$$

After inserting Eq. (17) and Eq. (4) into Eq. (6), we acquire that

$$\begin{aligned} R_{nn'}^i &= m_n^i \ominus m_{n'}^i \oplus \chi_{n'n}^i \\ &= \left(p_n^i \ominus p_{n'}^i\right) \oplus \left(y_n^i \ominus y_{n'}^i\right) \oplus \left(y_{n'}^i \ominus y_n^i\right) \\ &= p_n^i \ominus p_{n'}^i. \end{aligned} \tag{18}$$

In the light of Eq. (18) and Eq. (7), it can be concluded that when $h < p_n^i \ominus p_{n'}^i \leq 2h$, i.e., $\gamma(R_{nn'}^i) = -1$, we get $p_n^i < p_{n'}^i$; when $p_n^i \ominus p_{n'}^i = 0$, i.e., $\gamma(R_{nn'}^i) = 0$, we have $p_n^i = p_{n'}^i$; when $0 < p_n^i \ominus p_{n'}^i \leq h$, i.e., $\gamma(R_{nn'}^i) = 1$, we acquire $p_n^i > p_{n'}^i$. Here, $i = 1, 2, \ldots, L$, $n = 1, 2, \ldots, N$, $n' = 2, 3, \ldots, N$ and $n < n'$. Thus, it can be concluded that the accuracy of comparison results of the proposed MSQPC protocol can be ensured.

3.1.2 Example

For the sake of further supporting the foregoing analysis of output correctness of the presented MSQPC protocol, a specific example is given in detail. Suppose that P_1, P_2, P_3, P_4 are four semiquantum participants whose first private inputs are $p_1^1 = 0$, $p_2^1 = 6$, $p_3^1 = 4$, $p_4^1 = 8$, respectively in a 17-dimensional quantum system; after measuring the qudits prepared by TP_1, P_1, P_2, P_3, P_4 obtain $x_1^1 = 2$, $x_2^1 = 14$, $x_3^1 = 1$, $x_4^1 = 16$, respectively; and after measuring the qudits prepared by TP_2, P_1, P_2, P_3, P_4 acquire $y_1^1 = 6$, $y_2^1 = 4$, $y_3^1 = 12$, $y_4^1 = 1$,respectively. By virtue of Eq. (3), P_1, P_2, P_3, P_4 compute $c_1^1 = 0 \oplus 2 \oplus 6 = 8$, $c_2^1 = 6 \oplus 14 \oplus 4 = 7$, $c_3^1 = 4 \oplus 1 \oplus 12 = 0$ and $c_4^1 = 8 \oplus 16 \oplus 1 = 8$, respectively. Furthermore, TP_2 gets $\chi_{21}^1 = 4 \ominus 6 = 15$, $\chi_{31}^1 = 12 \ominus 6 = 6$, $\chi_{41}^1 = 1 \ominus 6 = 12$, $\chi_{32}^1 = 12 \ominus 4 = 8$, $\chi_{42}^1 = 1 \ominus 4 = 14$ and $\chi_{43}^1 = 1 \ominus 12 = 6$ in accordance with Eq. (4).

After receiving the classical information sent out by P_1, P_2, P_3, P_4 and TP_2, TP_1 gets $m_1^1 = 8 \ominus 2 = 6$, $m_2^1 = 7 \ominus 14 = 10$, $m_3^1 = 0 \ominus 1 = 16$ and $m_4^1 = 8 \ominus 16 = 9$ based on Eq. (5). Then, TP_1 calculates $R_{12}^1 = 6 \ominus 10 \oplus 15 = 11$, $R_{13}^1 = 6 \ominus 16 \oplus 6 = 13$, $R_{14}^1 = 6 \ominus 9 \oplus 12 = 9$, $R_{23}^1 = 10 \ominus 16 \oplus 8 = 2$, $R_{24}^1 = 10 \ominus 9 \oplus 14 = 15$ and $R_{34}^1 = 16 \ominus 9 \oplus 6 = 13$ by virtue of Eq. (6). Furthermore, according to Eq. (7), TP_1 makes $\gamma(R_{12}^1) = -1$, $\gamma(R_{13}^1) = -1$, $\gamma(R_{14}^1) = -1$, $\gamma(R_{23}^1) = 1$, $\gamma(R_{24}^1) = -1$ and $\gamma(R_{34}^1) = -1$. In other words, TP_1 obtains $p_1^1 < p_2^1$, $p_1^1 < p_3^1$, $p_1^1 < p_4^1$, $p_2^1 > p_3^1$, $p_2^1 < p_4^1$ and $p_3^1 < p_4^1$, which means $p_1^1 < p_3^1 < p_2^1 < p_4^1$. Therefore, we can conclude that the comparison results of the proposed MSQPC protocol are right.

3.2 Correctness analysis of the proposed MSQM protocol

3.2.1 Output correctness

In the light of Eqs. (8)–(10), it can be deduced that

$$\prod_{n=1}^{N} g_n^i = \prod_{n=1}^{N} \left(p_n^i \times x_n^i \times y_n^i\right) = \left(\prod_{n=1}^{N} p_n^i\right)\left(\prod_{n=1}^{N} x_n^i\right)\left(\prod_{n=1}^{N} y_n^i\right) = \alpha_i \beta_i \prod_{n=1}^{N} p_n^i. \tag{19}$$

After inserting Eq. (19) into Eq. (11), it has

$$M_i = \frac{\prod_{n=1}^{N} g_n^i}{\alpha_i \beta_i} \bmod d = \frac{\alpha_i \beta_i \prod_{n=1}^{N} p_n^i}{\alpha_i \beta_i} \bmod d = \prod_{n=1}^{N} p_n^i \bmod d \tag{20}$$

for $i = 1, 2, \ldots, L$, which validates that the output correctness of multiplication results in the proposed MSQM protocol.

3.2.2 Example

Here, a numerical example is given to further demonstrate that the output of the proposed MSQM is accurate. Assume that the first private integer of four semiquantum users P_1, P_2, P_3, P_4 are $p_1^1 = 3$, $p_2^1 = 7$, $p_3^1 = 1$ and $p_4^1 = 6$,respectively in a 10-dimensional quantum system; and by measuring the corresponding single photons prepared by TP_1 and TP_2, P_1 obtains $x_1^1 = 2$, $y_1^1 = 9$, P_2 gets $x_2^1 = 5$, $y_2^1 = 4$, P_3 acquires $x_3^1 = 7$, $y_3^1 = 1$ and P_4 gains $x_4^1 = 3$, $y_4^1 = 2$. Then, according to Eq. (8), P_1, P_2, P_3, P_4 calculate $g_1^1 = 3 \times 2 \times 9 = 54$, $g_2^1 = 7 \times 5 \times 4 = 140$, $g_3^1 = 1 \times 7 \times 1 = 7$ and $g_4^1 = 6 \times 3 \times 2 = 36$,respectively, and sends them to TP_1. Furthermore, in accordance with Eq. (9), TP_2 calculates $\beta_1 = 9 \times 4 \times 1 \times 2 = 72$ and sends it to TP_1.

Afterward, TP_1 computes $\alpha_1 = 2 \times 5 \times 7 \times 3 = 210$ according to Eq. (10) and figures up $M_1 = \frac{54 \times 140 \times 7 \times 36}{210 \times 72} \bmod 10 = 6$ by virtue of Eq. (11), which represents that the output accuracy of the proposed MSQM protocol can be assured.

3.3 Correctness analysis of the proposed MSQS protocol

3.3.1 Output correctness

By substituting Eq. (12) into Eq. (15), it can be shown that

$$\theta_i = \sum_{n=1}^{N} \mu_n^i \bmod d = \left(\sum_{n=1}^{N} p_n^i \bmod d\right) \oplus \left(\sum_{n=1}^{N} x_n^i \bmod d\right) \oplus \left(\sum_{n=1}^{N} y_n^i \bmod d\right). \tag{21}$$

Furthermore, inserting Eq. (21), Eq. (13) and Eq. (14) into Eq. (16) generates

$$\begin{aligned} sum_i &= \nu_i \oplus \sigma_i \oplus \theta_i \\ &= \left[\sum_{n=1}^{N} (d - y_n^i) \bmod d\right] \oplus \left[\sum_{n=1}^{N} (d - x_n^i) \bmod d\right] \oplus \left(\sum_{n=1}^{N} p_n^i \bmod d\right) \\ &\quad \oplus \left(\sum_{n=1}^{N} x_n^i \bmod d\right) \oplus \left(\sum_{n=1}^{N} y_n^i \bmod d\right) \\ &= \sum_{n=1}^{N} p_n^i \bmod d \end{aligned} \tag{22}$$

for $i = 1, 2, \ldots, L$, which means that the summation results of the proposed MSQS protocol are reliable.

3.3.2 Example

In this section, we give a specific example to further prove that the summation result of the proposed MSQS protocol is correct. It is assumed that semiquantum subscribers P_1, P_2, P_3, P_4 possess their own private inputs $p_1^1 = 0$, $p_2^1 = 11$, $p_3^1 = 3$ and $p_4^1 = 6$, respectively in a 12-dimensional quantum system. After P_1, P_2, P_3, P_4 measure the single photons produced by TP_1 and TP_2, respectively, it can be obtained that $x_1^1 = 8$, $y_1^1 = 2$, $x_2^1 = 4$, $y_2^1 = 1$, $x_3^1 = 7$, $y_3^1 = 11$, $x_4^1 = 1$ and $y_4^1 = 6$. Then, in accordance with Eq. (12), P_1, P_2, P_3, P_4 compute $\mu_1^1 =$

$0 \oplus 8 \oplus 2 = 10$, $\mu_2^1 = 11 \oplus 4 \oplus 1 = 4$, $\mu_3^1 = 3 \oplus 7 \oplus 11 = 9$ and $\mu_4^1 = 6 \oplus 1 \oplus 6 = 1$, respectively. Furthermore, TP_2 transmits $\nu_1 = (12-2) \oplus (12-1) \oplus (12-11) \oplus (12-6) = 4$ to TP_1 in accordance with Eq. (13).

After receiving μ_1^1, μ_2^1, μ_3^1, μ_4^1 and ν_1, by virtue of Eq. (14) and Eq. (15), TP_1 calculates $\sigma_1 = (12-8) \oplus (12-4) \oplus (12-7) \oplus (12-1) = 4$ and $\theta_1 = 10 \oplus 4 \oplus 9 \oplus 1 = 0$. As a result, based on Eq. (16), TP_1 acquires $sum_1 = 4 \oplus 4 \oplus 0 = 8$, which confirms that the output correctness of the proposed MSQS protocol.

4 Simulation based on IBM's Qiskit

To further demonstrate the output correctness of three proposed protocols, we conduct the simulation experiment by utilizing IBM's Qiskit without considering the eavesdropping check processes. The three proposed protocols only utilize d-dimensional single-particle states as quantum resources and perform d-dimensional single-particle measurements, which suggests that only when the quantum measurement results on single photons are accurate can the output correctness of protocols be guaranteed. It is easy to construct the quantum measurement circuit for single photon. In the following, we will simulate out the measurement outcomes of four single photons, considering a quantum system with a level of 8. The simulated quantum measurement circuits for $|6\rangle, |7\rangle, F|6\rangle$ and $F|7\rangle$ are shown in Figs. 2-5, respectively. Here, $F|6\rangle = \frac{1}{\sqrt{8}} \sum_{\delta=0}^{7} e^{\frac{3\pi\delta i}{2}} |\delta\rangle$ and $F|7\rangle = \frac{1}{\sqrt{8}} \sum_{\delta=0}^{7} e^{\frac{7\pi\delta i}{4}} |\delta\rangle$. Obviously, for any $\delta = 0, 1, \ldots, 7$, we have $\left| e^{\frac{3\pi\delta i}{2}} \right|^2 = \left| e^{\frac{7\pi\delta i}{4}} \right|^2 = 1$. Therefore, for simplicity, we disregard the specific phase values $e^{i \times \frac{3\pi\delta}{2}}$ and $e^{i \times \frac{7\pi\delta}{4}}$ in Figs. 4(a) and Figs. 5(a), respectively, as they have no impact on the corresponding measurement results. Note that 100,000 simulation experiments are conducted for each single photon.

Based on Figs. 2-5, it can be concluded that the measurement outcomes on single photons are entirely accurate. This implies that the output correctness of three proposed protocols can be guaranteed, as they only necessitate the d-dimensional single-particle measurements.

5 Security analysis

5.1 Outside attacks

To steal the confidential integer sequence p_n, an outside eavesdropper, Eve, may launch seven types of attacks during Steps (1)–(5), i.e., the intercept-resend attack, the measure-resend attack, the entangle-measure attack, the double controlled-not (CNOT) attacks, the Trojan horse attacks, the collective attack and the coherent attack. Note that either

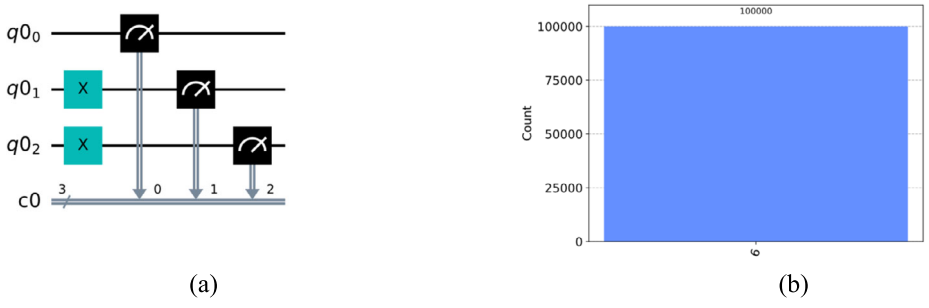

Figure 2 (a) Quantum circuit of the single-particle state $|6\rangle$ (b) The simulation results of (a)

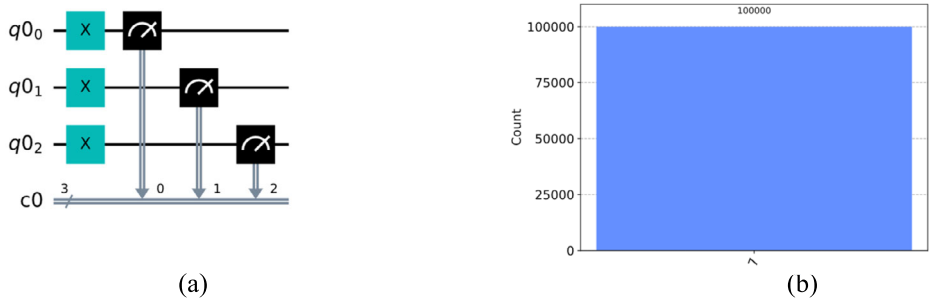

Figure 3 (a) Quantum circuit of the single-particle state $|7\rangle$ (b) The simulation results of (a)

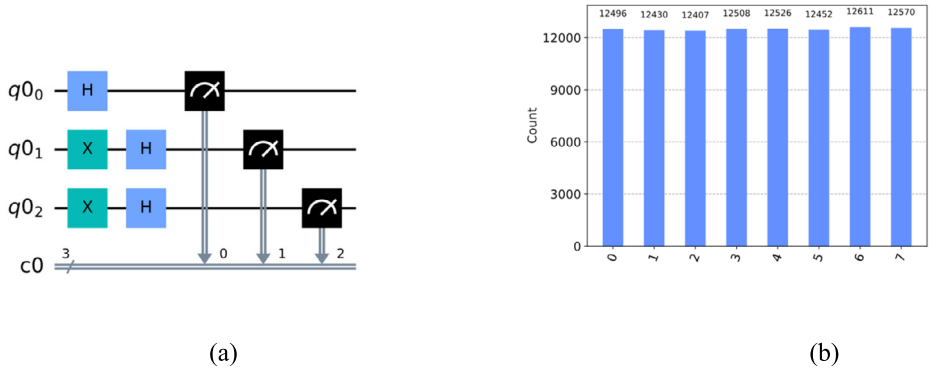

Figure 4 (a) Quantum circuit of the single-particle state $F|6\rangle$ (b) The simulation results of (a)

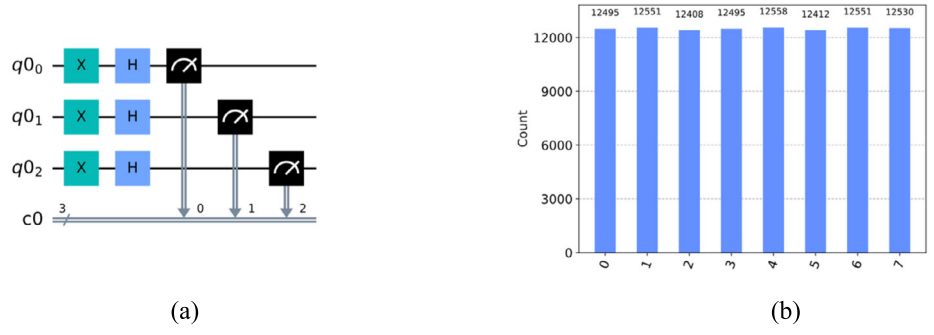

Figure 5 (a) Quantum circuit of the single-particle state $F|7\rangle$ (b) The simulation results of (a)

in the quantum channel between TP_1 and P_n or between TP_2 and P_n, Eve always acts equally. Consequently, we only discuss the security of the quantum channel between TP_1 and P_n.

(1) The intercept-resend attack

Eve intercepts the particle of S_n from TP_1 to P_n and sends P_n the fake one she has already produced in the T_1 basis in Step 1; after P_n implements her operation on the fake particle, Eve intercepts the corresponding particle of S_n' from P_n to TP_1 and transmits TP_1 the intercepted genuine one of S_n in Step 2. When the intercepted genuine particle is prepared in the T_2 basis, no matter what mode P_n has entered into, the existence of Eve cannot be

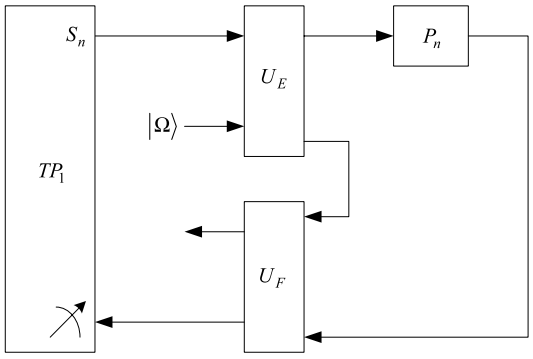

Figure 6 Eve's entangle-measure attack with U_E and U_F

discovered either in Case 2 or Case 3 of Step 3. Considering that the intercepted genuine particle is produced in the T_1 basis, if P_n has entered into the REFLECT mode, the eavesdropping behavior of Eve cannot be detected in Case 1 of Step 3; if P_n has entered into the MEASURE mode, the probability that the intercepted particle is chosen for eavesdropping detection is $\frac{1}{2}$, and the probability that P_n's measurement result on the fake particle is not same to the corresponding initial prepared state and TP_1's measurement result on the intercepted genuine particle of S_n is $\frac{d-2}{d-1}$, so the existence of Eve can be discovered with the probability of $\frac{d-2}{2d-2}$ in Case 4 of Step 3, which validates that Eve's eavesdropping behavior on one of the particles transmitted between TP_1 and P_n cannot be detected with the probability of $\frac{d}{2d-2}$. Consequently, the probability that Eve's this intercept-resend attack on the $8L$ particles of S_n can be discovered is $1-(\frac{d}{2d-2})^{8L}$, which will approach to 1 if L is large enough.

(2) The measure-resend attack

In Step 1, Eve intercepts the particle of S_n from TP_1 to P_n, utilizes the T_1 basis to measure it and transmits the resulted state to P_n. When the intercepted particle is in the T_1 basis, the presence of Eve cannot be detected either in Case 1 or Case 4 of Step 3, no matter what mode P_n has entered into. Considering that the intercepted particle is in the T_2 basis, when P_n has entered into the MEASURE mode, the eavesdropping behavior of Eve cannot be discovered in Case 3 of Step 3, as the intercepted particle is not chosen for security check; when P_n has entered into the REFLECT mode, the presence of Eve will be detected undoubtedly in Case 2 of Step 3, as Eve's measurement destroys the quantum superposition state of the intercepted particle.

(3) The entangle-measure attack

As shown in Fig. 6, Eve launches her entangle-measure attack on the transmitted particle by employing two unitary operations U_E and U_F, where U_E is imposed on the particle of S_n from TP_1 to P_n in Step 1 and U_F is performed on the particle of S'_n from P_n to TP_1 in Step 2. As illustrated in Refs.[41, 42], U_E and U_F share a common probe space with the auxiliary state $|\Omega\rangle$, where Eve is permitted by the shared probe to launch the attack on the particle of S'_n on the basis of the knowledge gained from U_E.

Theorem 1 *Suppose that Eve implements U_E on the qudit from TP_1 to P_n in Step* 1 *and imposes U_F on the qudit from P_n to TP_1 in Step* 2*. For introducing no error in Step* 3*, the final state of Eve's probe should be independent of not only the operations of P_n and TP_1, but also their measurement results. Consequently, Eve fails to acquire knowledge about x_n.*

Proof For convenience, we utilize $|t\rangle$ and $|G_t\rangle$ to denote the T_1 basis and the T_2 basis, respectively, where $|G_t\rangle = F|t\rangle = \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}|\delta\rangle$ and $t = 0, 1, \ldots, d-1$.

(i) Consider the situation that the particle attacked by Eve in Step 1 is prepared in the T_1 basis.

In the light of Ref.[55], the effect of U_E on the particle and Eve's probe can be described as

$$U_E\big(|t\rangle|\Omega\rangle\big) = \sum_{t'=0}^{d-1} \lambda_{tt'}|t'\rangle|\omega_{tt'}\rangle, \tag{23}$$

where the probe $|\omega_{tt'}\rangle$ are decided by U_E, $\sum_{t'=0}^{d-1}|\lambda_{tt'}|^2 = 1$ and $t = 0, 1, \ldots, d-1$.

When P_n intends to enter into the MEASURE mode, in order to get rid of the eavesdropping check in Case 4, Eve should make P_n's measurement result on the attacked particle be the same to the corresponding initial prepared state. Hence, it can be deduced that

$$\lambda_{tt'}|t'\rangle|\omega_{tt'}\rangle = 0 \tag{24}$$

for $t \neq t'$. After P_n performed the MEASURE mode, the global state of composite system was collapsed into $\lambda_{tt}|t\rangle|\omega_{tt}\rangle$ in accordance with Eq. (23) and Eq. (24). In order to escape the security check in Case 4, Eve should make P_n's measurement result on the attacked particle of S_n be the same to TP_1's measurement result on the corresponding particle of S'_n. Thus, the whole quantum system after being applied with U_F should be

$$U_F\big(\lambda_{tt}|t\rangle|\omega_{tt}\rangle\big) = \lambda_{tt}|t\rangle|F_{tt}\rangle, \tag{25}$$

which means that U_F is not allowed to alter the quantum state of S'_n.

When P_n has chosen the REFLECT mode, by virtue of Eqs. (23)–(25), the whole quantum system after being applied with U_F should be

$$U_F\big[U_E\big(|t\rangle|\Omega\rangle\big)\big] = U_F\left(\sum_{t'=0}^{d-1}\lambda_{tt'}|t'\rangle|\omega_{tt'}\rangle\right) = U_F\big(\lambda_{tt}|t\rangle|\omega_{tt}\rangle\big) = \lambda_{tt}|t\rangle|F_{tt}\rangle, \tag{26}$$

which means that TP_1's measurement result on the particle of S'_n is naturally same to the corresponding initial prepared state. As a result, as long as Eqs. (24), (25) are established, the eavesdropping behavior of Eve cannot be discovered in Case 1 of Step 3.

(ii) Consider the situation that the attacked particle is prepared in the T_2 basis. Combining Eq. (23) and Eq. (24), we obtain

$$U_E\big(|t\rangle|\Omega\rangle\big) = \sum_{t'=0}^{d-1}\lambda_{tt'}|t'\rangle|\omega_{tt'}\rangle = \lambda_{tt}|t\rangle|\omega_{tt}\rangle. \tag{27}$$

When U_E is implemented on the particle prepared in the T_2 basis and Eve's probe, the global composite system should be

$$\begin{aligned} U_E\big(|G_t\rangle|\Omega\rangle\big) &= U_E\left[\left(\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}|\delta\rangle\right)|\Omega\rangle\right] \\ &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}} U_E\big(|\delta\rangle|\Omega\rangle\big). \end{aligned} \tag{28}$$

On the basis of Eq. (27) and Eq. (28), it can be derived that

$$U_E\big(|G_t\rangle|\Omega\rangle\big) = \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}\lambda_{\delta\delta}|\delta\rangle|\omega_{\delta\delta}\rangle. \tag{29}$$

When P_n has chosen the MEASURE mode, the trace of Eve will never be discovered in Case 3 of Step 3, as there is no eavesdropping detection in this Case. When P_n has chosen the REFLECT mode, based on Eq. (25) and Eq. (29), the whole quantum system after being applied with U_F should be

$$\begin{aligned} U_F\big[U_E\big(|G_t\rangle|\Omega\rangle\big)\big] &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}} U_F\big(\lambda_{\delta\delta}|\delta\rangle|\omega_{\delta\delta}\rangle\big) \\ &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}\lambda_{\delta\delta}|\delta\rangle|F_{\delta\delta}\rangle. \end{aligned} \tag{30}$$

In the light of the inverse quantum Fourier transform, it can be deduced that

$$|\delta\rangle = \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{-\frac{2\pi ij\delta}{d}}|G_j\rangle, \tag{31}$$

where $\delta = 0, 1, \ldots, d-1$. Inserting Eq. (31) into Eq. (30) generates

$$\begin{aligned} U_F\big[U_E\big(|G_t\rangle|\Omega\rangle\big)\big] &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}\lambda_{\delta\delta}\left(\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1} e^{-\frac{2\pi ij\delta}{d}}|G_j\rangle\right)|F_{\delta\delta}\rangle \\ &= \frac{1}{d}\sum_{\delta=0}^{d-1}\sum_{j=0}^{d-1} e^{\frac{2\pi i\delta(t-j)}{d}}\lambda_{\delta\delta}|G_j\rangle|F_{\delta\delta}\rangle \\ &= \frac{1}{d}\left(|G_0\rangle\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta(t-0)}{d}}\lambda_{\delta\delta}|F_{\delta\delta}\rangle + |G_1\rangle\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta(t-1)}{d}}\lambda_{\delta\delta}|F_{\delta\delta}\rangle + \cdots\right. \\ &\quad \left. + |G_{d-1}\rangle\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta[t-(d-1)]}{d}}\lambda_{\delta\delta}|F_{\delta\delta}\rangle\right). \end{aligned} \tag{32}$$

In order to escape the security check in Case 2 of Step 3, Eve should make TP_1's measurement result on the particle of S'_n be the same to the corresponding initial prepared

state. Hence, in accordance with Eq. (32), it can be deduced that

$$\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta(t-j)}{d}} \lambda_{\delta\delta}|F_{\delta\delta}\rangle = 0 \tag{33}$$

for $t \neq j$, where $t,j = 0,1,\ldots,d-1$. Obviously, for any $t \neq j$, we obtain

$$\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta(t-j)}{d}} = 0. \tag{34}$$

Combining Eq. (33) and Eq. (34), it can be derived that

$$\lambda_{00}|F_{11}\rangle = \lambda_{11}|F_{11}\rangle = \cdots = \lambda_{(d-1)(d-1)}|F_{(d-1)(d-1)}\rangle = \lambda|F\rangle. \tag{35}$$

(iii) Inserting Eq. (35) into Eq. (25) produces

$$U_F\big(\lambda_{tt}|t\rangle|\omega_{tt}\rangle\big) = |t\rangle\big(\lambda|F\rangle\big), \tag{36}$$

which means that Eve cannot extract any knowledge about x_n^i, under the condition that the attacked particle is prepared in the T_1 basis and P_n enters into the MEASURE mode. Then, inserting Eq. (35) into Eq. (26) produces

$$U_F\left(\sum_{t'=0}^{d-1} \lambda_{tt'}|t'\rangle|\omega_{tt'}\rangle\right) = U_F\big(\lambda_{tt}|t\rangle|\omega_{tt}\rangle\big) = \lambda_{tt}|t\rangle|F_{tt}\rangle = |t\rangle\big(\lambda|F\rangle\big), \tag{37}$$

which means that Eve cannot obtain x_n^i, under the condition that the attacked particle is prepared in the T_1 basis and P_n enters into the REFLECT mode. Furthermore, inserting Eq. (35) into Eq. (32) produces

$$U_F\big[U_E\big(|G_t\rangle|\Omega\rangle\big)\big] = |G_j\rangle\big(\lambda|F\rangle\big), \tag{38}$$

which means that Eve has no knowledge about x_n^i, under the condition that the attacked particle is prepared in the T_2 basis and P_n enters into the REFLECT mode.

By virtue of Eqs. (36)–(38), it can be concluded that when Eve implements U_E on the qudit from TP_1 to P_n in Step 1 and imposes U_F on the qudit from P_n to TP_1 in Step 2. For introducing no error in Step 3, the final state of Eve's probe should be independent of not only the operations of P_n and TP_1, but also their measurement results. Consequently, Eve fails to acquire knowledge about x_n. □

(4) The double CNOT attacks

In accordance with Ref. [49], Eve initiates the first CNOT attack in Step 1, employing the particle of S_n and her ancillary particle as the control qudit and the target qudit, respectively. Subsequently, Eve proceeds with the second CNOT operation on the particle of S'_n as the control qudit and her auxiliary particle as the target qudit in Step 2, with the aim of extracting the information about P_n's operation from her auxiliary particle. For convenience, we adopt $|t\rangle$ and $|G_t\rangle$ to represent the T_1 basis and the T_2 basis, respectively,

where $|G_t\rangle = F|t\rangle = \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1} e^{\frac{2\pi i\delta t}{d}}|\delta\rangle$ and $t = 0, 1, \ldots, d-1$. In a d-level quantum system, the CNOT operation can be described as

$$U_{CT(d)} = \sum_{j=0}^{d-1}\sum_{k=0}^{d-1}|j, k\oplus j\rangle\langle j, k|, \tag{39}$$

where the symbol $\oplus$ denotes the modulo d addition.

(i) Consider the scenario where the initial particle of S_n is prepared in the T_1 basis. After Eve performs the first CNOT attack $U_{CT(d)}$ on the single photon $|t\rangle_S$ and her ancillary qudit $|\varepsilon\rangle_E$ in Step 1, the global state of the composite system is evolved into

$$U_{CT(d)}\left(|t\rangle_S|\varepsilon\rangle_E\right) = |t\rangle_S|t\oplus\varepsilon\rangle_E \tag{40}$$

for $t = 0, 1, \ldots, d-1$, where ε is a constant that can take any value from 0 to $d-1$. Afterward, P_n executes the REFLECT mode or the MEASURE mode on the received particle. It is worth noting that regardless of the mode P_n has chosen, the new quantum system after undergoing the second CNOT attack launched by Eve in Step 2 will collapse into

$$U_{CT(d)}\left(|t\rangle_S|t\oplus\varepsilon\rangle_E\right) = |t\rangle_S|t\oplus t\oplus\varepsilon\rangle_E. \tag{41}$$

Based on Eq. (40) and Eq. (41), it can be understood that TP_1's measurement result on the particle of S_n' is automatically identical to P_n's measurement result on the particle of S_n and the initial prepared state of S_n, which implies that Eve can evade the security check in both Case 1 and Case 4 of Step 3.

(ii) Consider the scenario where the initial prepared state of S_n is in the T_2 basis. When the single particle $|G_t\rangle_S$ and the auxiliary qudit $|\varepsilon\rangle_E$ generated by Eve are subjected to the first CNOT operation $U_{CT(d)}$ in Step 1, the composite system global state is evolved into

$$\begin{aligned} U_{CT(d)}\left(|G_t\rangle_S|\varepsilon\rangle_E\right) &= \left(\sum_{j=0}^{d-1}\sum_{k=0}^{d-1}|j, k+j\rangle\langle j, k|\right)\left[\left(\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}e^{\frac{2\pi i\delta t}{d}}|\delta\rangle_S\right)|\varepsilon\rangle_E\right] \\ &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}e^{\frac{2\pi i\delta t}{d}}|\delta\rangle_S|\delta\oplus\varepsilon\rangle_E \end{aligned} \tag{42}$$

for $t = 0, 1, \ldots, d-1$, where ε is a constant that can take any value from 0 to $d-1$. After P_n has applied the REFLECT mode to the received particle, Eve launches the second CNOT operation in Step 2, which can be depicted as

$$\begin{aligned} &U_{CT(d)}\left(\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}e^{\frac{2\pi i\delta t}{d}}|\delta\rangle_S|\delta\oplus\varepsilon\rangle_E\right) \\ &= \left(\sum_{j=0}^{d-1}\sum_{k=0}^{d-1}|j, k\oplus j\rangle\langle j, k|\right)\left(\frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}e^{\frac{2\pi i\delta t}{d}}|\delta\rangle_S|\delta\oplus\varepsilon\rangle_E\right) \\ &= \frac{1}{\sqrt{d}}\sum_{\delta=0}^{d-1}e^{\frac{2\pi i\delta t}{d}}|\delta\rangle_S|\delta\oplus\delta\oplus\varepsilon\rangle_E, \end{aligned} \tag{43}$$

in accordance with Eq. (39) and Eq. (42). In order to escape the eavesdropping detection in Case 2 of Step 3, Eve should make TP_1's measurement result on the particle of S'_n be same to the initial produced particle state of S_n, which means that the values of $\delta \oplus \delta$ should consistently be a constant for $\delta = 0, 1, \ldots, d-1$ according to Eq. (43).

(iii) By consolidating the foregoing discussions, we can draw the following two judgements.

Firstly, considering that d is equal to 2. Then, regardless of whether $t = 0$ or $t = 1$, we can consistently deduce that the value of $t \oplus t$ is equal to 0. Hence, Eq. (41) and Eq. (43) will transform into

$$U_{CT(2)}\left(|t\rangle_S|t \oplus \varepsilon\rangle_E\right) = |t\rangle_S|\varepsilon\rangle_E, \tag{44}$$

and

$$U_{CT(2)}\left(\frac{1}{\sqrt{2}}\sum_{\delta=0}^{1} e^{\pi i\delta t}|\delta\rangle_S|\delta \oplus \varepsilon\rangle_E\right) = \frac{1}{\sqrt{2}}\sum_{\delta=0}^{1} e^{\pi i\delta t}|\delta\rangle_S|\varepsilon\rangle_E, \tag{45}$$

respectively. On the basis of Eq. (44) and Eq. (45), we can infer that Eve's attacks cannot be discovered in Step 3. Nevertheless, Eve still has no way to obtain the information about P_n's operation, due to that her auxiliary particle $|\varepsilon\rangle_E$ consistently stays unchanged. It can be concluded that if d is equal to 2, Eve will acquire nothing by performing the double CNOT operations on the particles transmitted in the quantum channel between TP_1 and P_n in Step 1 and Step 2.

Secondly, considering that d is greater than 2. When δ takes all values from 0 to $d-1$, the corresponding d values of $\delta \oplus \delta$ must not be a constant. Therefore, according to Eq. (43), TP_1's measurement result on S'_n must not be same to the initial produced state, which implies that if d is greater than 2, Eve's double CNOT attacks will inevitably be detected in Case 2 of Step 3.

(iv) Overall, by initiating the double CNOT attacks on the qudits transmitted between TP_1 and P_n in Step 1 and Step 2, Eve fails to eavesdrop the information about P_n's operation without being detected, not to mention the knowledge about x_n.

(5) The Trojan horse attacks

As the particles of S_n travel from TP_1 to P_n and back from P_n to TP_1, we need to address two kinds of Trojan horse attacks launched by Eve: the delay-photon Trojan horse attack [59, 60] and the invisible photon eavesdropping attack [61]. Both these attacks involve stealing the information about P_n's operation by inserting a tail-made photon produced by Eve into the one transmitted between TP_1 and P_n. To guarantee the security of the proposed protocols, P_n employs a photon beam splitter (PBS: 50/50) to divide each sample signal into two pieces and measure them, which can effectively resist the former type of attack. [60, 62] As for the latter type of attack, P_n utilizes a wavelength filter to process each signal before executing the operation. [60, 62]

(6) The collective and coherent attacks

The collective attack represents a class of attacks that exploit the vulnerabilities within a quantum communication system. The coherent attack denotes a type of attack that takes advantage of the coherence of quantum systems. According to Ref. [22], Eve generates an autonomous ancillary particle to communicate with each qudit and jointly performs the

measurement operation on all the ancillary qudits, which can be seen as the collective attack. In the coherent attack, Eve produces an individual ancillary particle, intercepts the participant's particle and conducts the measurement process within the computational basis $\{|1\rangle, |2\rangle, \ldots, |d-1\rangle\}$. Unfortunately, Eve's trace will undoubtedly be discovered based on the deduction of Eqs. (23)–(45), indicating that she has no way to acquire p_n.

5.2 Participant attacks

(1) The participant attack from one dishonest user

In the three proposed protocols, the semiquantum subscribers $P_1, P_2, \ldots, P_N$ play the equal roles all the time. Without losing generality, it is assumed that P_1 is the dishonest user who tries her best to steal the secret integers of the remaining $N-1$ participants.

Firstly, in Steps (1)–(5), to acquire $x_a = \{x_a^1, x_a^2, \ldots, x_a^L\}$ or $y_a = \{y_a^1, y_a^2, \ldots, y_a^L\}$, P_1 may launch her attacks on the qudits between TP_1 and P_a or between TP_2 and P_a, where $a = 2, 3, \ldots, N$. Nevertheless, P_1 is independent from P_a, TP_1 and TP_2, which makes her play the role of an outside eavesdropper. Consequently, in the three proposed protocols, P_1 has no information about x_a and y_a in accordance with Sect. 5.1.

Secondly, in Step 6′, P_1 may hear of c_a^i sent out from P_a and $\chi_{n'n}^i$ sent out from TP_2, but she cannot acquire p_a^i according to Eq. (3) and Eq. (4), due to that she is unable to obtain x_a^i and y_a^i simultaneously. Then, in Step 7′, although P_1 may hear of the final comparison results from TP_1, she still cannot obtain p_a^i.

Thirdly, in Step 6″, P_1 may hear of g_a^i sent out from P_a and β_i sent out from TP_2, but she has no way to infer out p_a^i in accordance with Eq. (8) and Eq. (9), because of being short of both x_a^i and y_a^i. Besides, in Step 7″, P_1 may hear of the final multiplication results from TP_1, but she still has no chance to get p_a^i.

Fourthly, in Step 6‴, P_1 may hear of μ_a^i sent out from P_a and ν_i sent out from TP_2, but she is unable to acquire p_a^i based on Eq. (12) and Eq. (13), due to lack of both x_a^i and y_a^i. Furthermore, in Step 7‴, P_1 may hear of the final summation results from TP_1, but she still has no idea about p_a^i.

In short, one dishonest user cannot acquire the private inputs of remaining $N-1$ users in the three proposed protocols.

(2) The participant attack from two or more dishonest users

Consider the worst situation that $N-1$ participants, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$, conspire to steal the secret inputs of P_b, where $b \in \{2, 3, \ldots, N-1\}$.

Firstly, in Steps (1)–(5), to acquire $x_b = \{x_b^1, x_b^2, \ldots, x_b^L\}$ or $y_b = \{y_b^1, y_b^2, \ldots, y_b^L\}$, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may launch their attacks on the qudits between TP_1 and P_b or between TP_2 and P_b. Obviously, the union of $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ is independent from P_b, TP_1 and TP_2, making the union of $N-1$ participants play the role of an external attacker. As a result, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ has no way to get the knowledge about x_b or y_b according to Sect. 5.1.

Secondly, in Step 6′, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may steal c_b^i sent out from P_b and $\chi_{n'n}^i$ sent out from TP_2, which means that y_b^i can be decoded out in the light of Eq. (4). Nevertheless, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ still cannot obtain p_b^i based on y_b^i and c_b^i, because of being short of x_b^i, according to Eq. (3). Then, in Step 7′, although $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may hear of the final comparison results from TP_1, they still has no way to extract p_b^i.

Thirdly, in Step 6″, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may steal g_b^i sent out from P_b and β_i sent out from TP_2, in which y_b^i can be derived out based on β_i and $y_1^i, y_2^i, \ldots, y_{b-1}^i, y_{b+1}^i, \ldots, y_N^i$,

according to Eq. (9). Unfortunately, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ has no chance to obtain p_b^i which is encrypted by x_b^i and y_b^i, in accordance with Eq. (8). Furthermore, in Step 7″, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may hear of the final multiplication results from TP_1, but they are still helpless in getting p_b^i.

Fourthly, in Step 6‴, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may hear of μ_b^i sent out from P_b and v_i sent out from TP_2, so they can infer out y_b^i according to Eq. (13). However, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ has no chance to obtain p_b^i based on Eq. (12), due to lack of x_b^i. Besides, in Step 7‴, $P_1, P_2, \ldots, P_{b-1}, P_{b+1}, \ldots, P_N$ may hear of the final summation results from TP_1, but they still cannot acquire p_b^i.

In conclusion, two or more users has no chance to acquire the secret integers of remaining users in the three proposed protocols.

(3) The participant attack from semi-honest TP_1

It is assumed that TP_1 cannot be allowed to conspire with anyone else. On the one hand, TP_1 may launch her attacks on the qudits between TP_2 and P_n to steal y_n^i; nevertheless, her eavesdropping behaviors are definitely detected according to Sect. 5.1. On the other hand, TP_1 receives $c_n^i/g_n^i/\mu_n^i$ and $\chi_{n'n}^i/\beta_i/v_i$ from P_n and TP_2, respectively; however, she cannot infer out p_n^i, due to lack of y_n^i, according to Eq. (3)/Eq. (8)/Eq. (12). In addition, the final comparison/multiplication/summation results cannot work in getting p_n^i either.

(4) The participant attack from semi-honest TP_2

It is assumed that TP_2 cannot be permitted to collude with anyone else. On the one hand, TP_2 may launch her attacks on the particles between TP_1 and P_n to get x_n^i, but she is undoubtedly discovered based on Sect. 5.1. On the other hand, TP_2 may hear of $c_n^i/g_n^i/\mu_n^i$ from P_n to TP_1 in Step 6′/ Step 6″/ Step 6‴; nevertheless, she has no chance to acquire p_n^i, because of being short of x_n^i, in accordance with Eq. (3)/Eq. (8)/Eq. (12). In addition, TP_2 may hear of the final comparison/multiplication/summation results from TP_1, but is still helpless for her to get p_n^i.

6 Discussions and conclusions

The proposed hybrid protocol can achieve the multi-party semiquantum private comparison scheme, the multi-party semiquantum multiplication scheme and the multi-party semiquantum summation scheme simultaneously under the help of two TPs. Here, TP_1 and TP_2 mutually supervise each other. The function of TP_1 is to create a semiquantum private key x_n with P_n; in the meanwhile, TP_2 creates a semiquantum private key y_n with P_n. Some existing semiquantum private comparison [55] and summation protocols [46] only need one TP. However, in practical applications, these protocols can only be applied to the scenario with a single authority center. However, a protocol with two TPs, such as our hybrid protocol, can be applied to the situation with two mutually supervising authority centers. In addition, our hybrid protocol can be applied into many scenarios, such as voting, ranking, bidding, and so on.

As illustrated in Ref. [55], the qudit efficiency is utilized to calculate the communication efficiency of a quantum protocol suitable for the d-dimensional Hilbert space, which is defined as

$$\eta = \frac{\kappa}{\tau + \xi}. \tag{46}$$

Here, κ, τ and ξ are the length of private inputs established, the number of qudits consumed and the number of classical bits expended, respectively. Note that we neglect the classical resources expended during the eavesdropping detection processes.

In the proposed MSQPC protocol, the length of p_n is L, so we gain $\kappa = L$. TP_1/TP_2 prepares N groups of $8L$ d-dimensional single-particle states and transmits them to the semiquantum participants; after getting the qudits from TP_1/TP_2, when P_n enters into the MEASURE mode, she is asked to produce $4L$ fresh qudits based on the found states within the T_1 basis; so we obtain $\tau = (8L \times N + 4L \times N) \times 2 = 24NL$. Then, P_n and TP_2 send c_n^i and $\chi_{n'n}^i$ to TP_1, respectively, where $n = 1, 2, \ldots, N$, $n' = 2, 3, \ldots, N$, $n' > n$ and $i = 1, 2, \ldots, L$. Hence, we have $\xi = L \times N + \frac{N(N-1)}{2} \times L = NL + \frac{NL(N-1)}{2}$. As a result, the proposed MSQPC protocol's qudit efficiency is $\eta = \frac{L}{24NL+NL+\frac{NL(N-1)}{2}} = \frac{2}{N^2+49N}$.

Whether in the proposed MSQM protocol or MSQS protocol, by adopting the same analysis method as foregoing discussion, we can obtain $\kappa = L$ and $\tau = 24NL$. Furthermore, P_n and TP_2 send g_n^i/μ_n^i and β_i/ν_i to TP_1, respectively, where $i = 1, 2, \ldots, L$. Therefore, it can be deduced that $\xi = L \times N + L = (N + 1)L$. Consequently, the qudit efficiency of the proposed MSQM protocol or MSQS protocol is $\eta = \frac{L}{24NL+(N+1)L} = \frac{1}{25N+1}$.

In the SQPC protocol of Ref. [55], the length of Alice's or Bob's secrets is n, so we get $\kappa = n$. The minimum number of d-dimensional single-particle states generated by TP should be $16n$; then, TP sends $8n$ particles to Alice and $8n$ particles Bob; when Alice and Bob enter into the MEASURE mode, they send the freshly prepared qudits to TP. Furthermore, this protocol adopts the SQKD protocol [63] to produce the pre-shared keys among Alice and Bob, consuming $24n$ qudits. Hence, we obtain $\tau = 16n + 4n + 4n + 24n = 48n$. In addition, Alice sends R_A^i to TP while Bob sends R_B^i to TP. TP needs to announce r_i to Alice and Bob. As a result, we obtain $\xi = 3n$. It can be concluded that the qudit efficiency of the protocol in Ref. [55] is $\eta = \frac{n}{48n+3n} = \frac{1}{51}$.

Using the same method, we obtain that the qudit efficienies of the protocol of Ref. [51], the protocol of Ref. [52], the first protocol of Ref.[53], the second protocol of Ref.[53] and the protocol of Ref.[54] are $\frac{1}{50}$, $\frac{1}{42}$, $\frac{1}{50}$, $\frac{1}{14}$ and $\frac{1}{38}$, respectively. In the proposed MSQPC protocol, when $N = 2$, the corresponding qudit efficiency is $\frac{1}{51}$. With respect to qudit efficiency, compared to the protocols of Refs. [51–55], our MSQPC protocol does not have an advantage, but is very close to the protocol of Ref. [51] and the first protocol of Ref. [53]. The protocols of Refs. [51–55] can only achieve the private comparison between two semiquantum users. Fortunately, the proposed hybrid protocol can achieve the semiquantum private comparison, the semiquantum multiplication and the semiquantum summation simultaneously among more than two semiquantum participants, which may decrease the qudit efficiency.

In addition, we compare the proposed MSQPC protocol with the present SQPC protocols of size relationship in Refs. [51–55], as shown in Table 2. In accordance with Table 2, the proposed MSQPC protocol is superior to the protocols of Refs. [51, 52, 54] in quantum resources, as d-dimensional single-particle states are much easier to produce than d-dimensional Bell states and d-dimensional GHZ states; on the usage of a pre-shared key, the proposed MSQPC protocol defeats the protocols of Refs. [51–55], as it has no demand for a pre-shared key; due to no use of unitary operations, the proposed MSQPC protocol exceeds the second protocol of Ref. [53]; as for the quantum measurements from quantum parties, the proposed MSQPC protocol takes advantage over the protocols of Refs. [51, 52, 54], due to that it doesn't require d-dimensional GHZ state measurements

Table 2 Comparison of the proposed MSQPC protocol with the present SQPC protocols of size relationship

	Quantum resources	Number of users	Number of TPs	TPs' knowledge about the comparison results	Type of TPs	Usage of quantum entanglement swapping	Usage of pre-shared key	Usage of unitary operations	Quantum measurements from semiquantum parties	Quantum measurements from quantum parties	Qudit efficiency
Ref. [51]	d-dimensional Bell states	2	1	Yes	Semi-honest	No	Yes	No	d-dimensional single-particle measurements	d-dimensional Bell state measurements and d-dimensional single- particle measurements	$\frac{1}{50}$
Ref. [52]	d-dimensional GHZ states	2	1	Yes	Semi-honest	No	Yes	No	d-dimensional single-particle measurements	d-dimensional GHZ state measurements, d-dimensional Bell state measurements and d-dimensional single-particle measurements	$\frac{1}{42}$
The first protocol of Ref. [53]	d-dimensional single-particle states	2	1	Yes	Semi-honest	No	Yes	No	d-dimensional single-particle measurements	d-dimensional single-particle measurements	$\frac{1}{50}$
The second protocol of Ref. [53]	d-dimensional single-particle states	2	1	Yes	Semi-honest	No	Yes	Yes	d-dimensional single-particle measurements	d-dimensional single-particle measurements	$\frac{1}{14}$
Ref. [54]	d-dimensional Bell states	2	1	Yes	Semi-honest	No	Yes	No	No	d-dimensional Bell state measurements and d-dimensional single- particle measurements	$\frac{1}{38}$
Ref. [55]	d-dimensional single-particle states	2	1	No	Semi-honest	No	Yes	No	d-dimensional single-particle measurements	d-dimensional single- particle measurements	$\frac{1}{51}$
The proposed MSQPC protocol	d-dimensional single-particle states	N	2	Yes	Semi-honest	No	No	No	d-dimensional single-particle measurements	d-dimensional single- particle measurements	$\frac{2}{N^2+49N}$

or d-dimensional Bell state measurements; and the proposed MSQPC protocol, aiming to determine the size relationship of more than two semiquantum participants' private inputs within one round implementation, is the only one which doesn't require a pre-shared key.

In conclusion, in this paper, by utilizing d-dimensional single-particle states, the first MSQPC protocol without a pre-shared key, aiming to judge the size relationship of more than two semiquantum users' secret integers, is put forward; the first MSQM protocol integrating the concept of semiquantumness into quantum multiplication is put forward, which is devoted to computing the modulo d multiplication of secret integers from more than two semiquantum participants; and the first MSQS protocol which can calculate the modulo d addition of private inputs from more than three semiquantum users is put forward. It is noteworthy that only under the control of two TPs can the goals of the three proposed protocols be achieved, where the semi-honest TPs are allowed to launch arbitrary attacks but cannot cooperate with anyone else.

The three proposed protocols have no demand for quantum entanglement swapping and unitary operations. Both the outside attacks and the participant attacks can be resisted in the three proposed protocols.

Funding
the National Natural Science Foundation of China (Grant No.62071430), the Fundamental Research Funds for the Provincial Universities of Zhejiang (Grant No. JRK21002) and the Project Supported by Scientific Research Fund of Zhejiang Provincial Education Department (Grant No. Y202352615).

Abbreviations
MSQPC, Multi-party semiquantum private comparison; MSQM, Multi-party semiquantum multiplication; MSQS, Multi-party semiquantum summation; TP, Third party; QKD, Quantum key distribution; QSS, Quantum secret sharing; QPC, Quantum private comparison; QM, Quantum multiplication; QS, Quantum summation; SQPC, Semiquantum private comparison; SQS, Semiquantum summation; SQM, Semiquantum multiplication; SQKD, Semiquantum key distribution; CNOT, Controlled-not.

Data availability
The datasets used during the current study are available from the corresponding author on reasonable request

Declarations

Ethics approval and consent to participate
Not applicable

Consent for publication
Not applicable

Competing interests
The authors declare no competing interests.

Author contributions
Jiang-Yuan Lian wrote the manuscript; and Tian-Yu Ye reviewed and checked the paper

Received: 5 September 2023 Accepted: 4 March 2024 Published online: 13 March 2024

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems and signal processing. Bangalore. 1984. p. 175–9.
2. Hillery M, Buzek V, Berthiaume A. Quantum secret sharing. Phys Rev A. 1999;59:1829.
3. Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. Phys Rev A. 1999;59:162–8.
4. Zhang ZJ, Yang J, Man ZX, Li Y. Multiparty secret sharing of quantum information using and identifying Bell state. Eur Phys J D. 2005;33(1):133–6.
5. Deng FG, Li XH, Zhou HY. Efficient high-capacity quantum secret sharing with two-photon entanglement. Phys Lett A. 2008;372(12):1957–62.
6. Chen XB, Niu XX, Zhou XJ, Yang YX. Multi-party quantum secret sharing with the single-particle quantum state to encode the information. Quantum Inf Process. 2013;12:365.

7. Ye CQ, Ye TY. Circular semi-quantum secret sharing using single particles. Commun Theor Phys. 2018;70:661–71.
8. Li CY, Ye CQ, Tian Y, Chen XB, Li J. Cluster-state-based quantum secret sharing for users with different abilities. Quantum Inf Process. 2021;20(12):385.
9. Sutradhar K, Om H. Enhanced (*t*, *n*) threshold *d*-level quantum secret sharing. Sci Rep. 2021;11:17083.
10. Sutradhar K, Om H. An efficient simulation of quantum secret sharing. 2021. arXiv:2103.11206.
11. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A, Math Theor. 2009;42(5):055305.
12. Chen XB, Xu G, Niu XX, Wen QY, Yang YX. An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt Commun. 2010;283:1561–5.
13. Guo FZ, Gao F, Qin SJ, Zhang J, Wen QY. Quantum private comparison protocol based on entanglement swapping of *d*-level Bell states. Quantum Inf Process. 2013;12(8):2793–802.
14. Ye TY. Quantum private comparison via cavity QED. Commun Theor Phys. 2017;67(2):147–56.
15. Song XL, Wen AJ, Gou R. Multiparty quantum private comparison of size relation based on single-particle states. IEEE Access. 2019;99:1–7.
16. Cao H, Ma WP, Lü LD, He YF, Liu G. Multi-party quantum comparison of size based on *d*-level GHZ states. Quantum Inf Process. 2019;18:287.
17. Wang B, Gong LH, Liu SQ. Multi-party quantum private size comparison protocol with *d*-dimensional Bell states. Front Phys. 2022;10:981376.
18. Lian JY, Li X, Ye TY. Multi-party quantum private comparison of size relationship with two third parties based on *d*-dimensional Bell states. Phys Scr. 2023;98:035011.
19. Sutradhar K, Om H. A privacy-preserving comparison protocol. IEEE Trans Comput. 2023;72(6):1815–21.
20. Shi RH, Mu Y, Zhong H, Cui J, Zhang S. Secure multiparty quantum computation for summation and multiplication. Sci Rep. 2016;6:19655.
21. Lv SX, Jiao XF, Zhou P. Multiparty quantum computation for summation and multiplication with mutually unbiased bases. Int J Theor Phys. 2019;58(9):2872–82.
22. Sutradhar K, Om H. Hybrid quantum protocols for secure multiparty summation and multiplication. Sci Rep. 2020;10:9097.
23. Sutradhar K, Om H. A cost-effective quantum protocol for secure multi-party multiplication. Quantum Inf Process. 2021;20(11):380.
24. Sutradhar K, Om H. Secret sharing based multiparty quantum computation for multiplication. Int J Theor Phys. 2021;60:3417–25.
25. Li FL, Hu H, Zhu SX. A (*k*, *n*)-threshold dynamic quantum secure multiparty multiplication protocol. Quantum Inf Process. 2022;21:394.
26. Heinrich S. Quantum summation with an application to integration. J Complex. 2002;18(1):1–50.
27. Chen XB, Xu G, Yang YX, Wen QY. An efficient protocol for the secure multi-party quantum summation. Int J Theor Phys. 2010;49(11):2793–804.
28. Zhang C, Sun ZW, Huang X, Long DY. Three-party quantum summation without a trusted third party. Int J Quantum Inf. 2015;13(02):1550011.
29. Shi RH, Zhang S. Quantum solution to a class of two-party private summation problems. Quantum Inf Process. 2017;16(9):225.
30. Liu W, Wang YB, Fan WQ. An novel protocol for the quantum secure multi-party summation based on two-particle bell states. Int J Theor Phys. 2017;56(9):2783–91.
31. Yang HY, Ye TY. Secure multi-party quantum summation based on quantum Fourier transform. Quantum Inf Process. 2018;17(6):129.
32. Ji Z, Zhang H, Wang H, Wu F, Jia J, Wu W. Quantum protocols for secure multi-party summation. Quantum Inf Process. 2019;18(6):168.
33. Sutradhar K, Om H. A generalized quantum protocol for secure multiparty summation. IEEE Trans Circuits Syst II. 2020;67(12):2978–82.
34. Ye TY, Xu TJ. A lightweight three-user secure quantum summation protocol without a third party based on single-particle states. Quantum Inf Process. 2022;21(9):309.
35. Ye TY, Hu JL. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. Int J Theor Phys. 2021;60(3):819–27.
36. Sutradhar K. Secure multiparty quantum aggregating protocol. Quantum Inf Comput. 2023;23:245–56.
37. Venkatesh R, Savadatti Hanumantha B. A privacy-preserving quantum blockchain technique for electronic medical records. IEEE Eng Manage Rev. 2023;51(4):137–44.
38. Venkatesh R, Savadatti Hanumantha B. Electronic medical records protection framework based on quantum blockchain for multiple hospitals. Multimed Tools Appl. 2023. https://doi.org/10.1007/s11042-023-16848-y.
39. Sutradhar K, Om H. An efficient simulation for quantum secure multiparty computation. Sci Rep. 2021;11:2206.
40. Sutradhar K. A quantum cryptographic protocol for secure vehicular communication. IEEE Trans Intell Transp Syst. 2023;1–10.
41. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99(14):140501.
42. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. Phys Rev A. 2009;79(3):032341.
43. Ye TY, Li HK, Hu JL. Semi-quantum key distribution with single photons in both polarization and spatial-mode degrees of freedom. Int J Theor Phys. 2020;59:2807–15.
44. Ye TY, Geng MJ, Xu TJ, Chen Y. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. Quantum Inf Process. 2022;21(4):123.
45. Chou WH, Hwang T, Gu J. Semi-quantum private comparison protocol under an almost-dishonest third party. 2016. arXiv:1607.07961.
46. Zhang C, Huang Q, Long YX, Sun ZW. Secure three-party semi-quantum summation using single photons. Int J Theor Phys. 2021;60:3478–87.
47. Ye TY, Ye CQ. Measure-resend semi-quantum private comparison without entanglement. Int J Theor Phys. 2018;57(12):3819–34.

48. Lang YF. Semi-quantum private comparison using single photons. Int J Theor Phys. 2018;57:3048–55.
49. Lin PH, Hwang T, Tsai CW. Efficient semi-quantum private comparison using single photons. Quantum Inf Process. 2019;18:207.
50. Ye CQ, Li J, Chen XB, Yuan T. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. Quantum Inf Process. 2021;20:262.
51. Zhou NR, Xu QD, Du NS, Gong LH. Semi-quantum private comparison protocol of size relation with *d*-dimensional Bell states. Quantum Inf Process. 2021;20:124.
52. Wang B, Liu SQ, Gong LH. Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states. Chin Phys B. 2022;31:010302.
53. Li YC, Chen ZY, Xu QD, Gong LH. Two semi-quantum private comparison protocols of size relation based on single particles. Int J Theor Phys. 2022;61:157.
54. Luo QB, Li XY, Yang GW, Lin C. A mediated semi-quantum protocol for millionaire problem based on high-dimensional Bell states. Quantum Inf Process. 2022;21:257.
55. Geng MJ, Xu TJ, Chen Y, Ye TY. Semiquantum private comparison of size relationship based *d*-level single-particle states. Sci Sin Phys Mech Astron. 2022;52(9):290311.
56. Ye TY, Lian JY. A novel multi-party semiquantum private comparison protocol of size relationship with d-dimensional single-particle states. Physica A. 2023;611:128424.
57. Ye TY, Xu TJ, Geng MJ, Chen Y. Two-party secure semiquantum summation against the collective-dephasing noise. Quantum Inf Process. 2022;21:118.
58. Hu JL, Ye TY. Three-party secure semiquantum summation without entanglement among quantum user and classical users. Quantum Inf Process. 2022;61:170.
59. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74:145.
60. Deng FG, Zhou P, Li XH, et al. Robustness of two-way quantum communication protocols against Trojan horse attack. 2005. arXiv:quant-ph/0508168.
61. Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A. 2006;351:23.
62. Li XH, Deng FG, Zhou HY. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A. 2006;74:054302.
63. Krawec WO. Mediated semiquantum key distribution. Phys Rev A. 2015;91(3):032323.

Publisher's Note