Hou et al. *EPJ Quantum Technology* (2025) 12:10
https://doi.org/10.1140/epjqt/s40507-025-00311-y

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

A quantum solution to blind millionaire problem with only single-particle states

Kunchi Hou[1,4], Huixin Sun[1,4], Yao Yao[1,4], Yu Zhang[1,4] and Kejia Zhang[2,3,4*]

*Correspondence:
zhangkejia@hlju.edu.cn
[2]School of Computer Science and Big Data (School of Cybersecurity), Heilongjiang University, Xuefu, Harbin, 150080, Asia, China
[3]State Key Laboratory of Public Big Data, Guizhou University, Huaxi, Guiyang, 550000, Asia, China
Full list of author information is available at the end of the article

Abstract

Blind millionaire (BM) problem is an extended version of the initial millionaire problem required to compare the sum of the participants' secrets between different groups. As a new topic of quantum secure multiparty computing, existing protocols with some special entangled states may not be easily achieved in practice. This study proposes a non-entangled method of solving the quantum blind millionaire (QBM) problem with special d-level single-particle states for the first time. To protect the confidentiality of transmission secrets, this protocol exploits the property of randomly generated d-level single-particle states. Furthermore, simple shift operations are used to encode the respective secrets. Detailed security analysis demonstrates that this protocol is impervious to internal and external threats. The presented methods can not only be used to solve the blind millionaire problem but also be used as a basic module to solve other secure multiparty computing problems.

Keywords: Quantum blind millionaire problem; Quantum security multiparty summation; Quantum private comparison; Single-particle states

1 Introduction

With the rapid development of information technology, multiparty collaboration to achieve established task goals has become an important way of information exchange. However, due to the sensitivity of personal privacy data, it is necessary to fully protect the data from being leaked during the above process. As a critical area of cryptography, the Secure Multiparty Computing (SMC) technique has been widely used to solve this problem. The SMC originated from the millionaire problem by Yao [1], where two millionaires want to find out who richer without sharing any information about their financial situation. The millionaire problem has received a lot of attention in SMC. In 2001, Boudot et al. proposed a protocol to compare whether two millionaires have the same value of wealth [2]. In 2009, Li et al. presented symmetric cryptographic protocols for the extended millionaire problem [3].

Through the extensive research on the millionaire problem, a new issue called the blind millionaire (BM) problem is proposed. The BM problem has a wide range of application scenarios, covering many domains such as smart auctions in financial cooperative unions [4], smart medical outcome assessment [5], smart cities [6], smart grids [7] and

Springer

more. The BM problem provides a secure way to compare multiple sets of data while protecting data privacy. It promotes industry research and information exchange. In the simplest BM problem, Alice, Bob, and Charlie are three participants with wealth of a, b, and c. They want to calculate the difference between $a + b$ and c without revealing their true assets. The blind millionaire problem extends Yao's definition by introducing a new application scenario for the traditional millionaire problem. In 2020, Li et al. introduced the first secret shift addition method to address the blind millionaire problem, leveraging shift register concepts and probabilistic encryption techniques [8].

With the rapid development of quantum technologies and the significant improvement of quantum computing capabilities, there is a severe challenge to classical SMC protocols designed based on large integer factorization and discrete logarithm problems. Since the security of these classical protocols relies on computational complexity assumptions, they may become vulnerable in a quantum computing environment. Therefore, constructing quantum SMC using quantum technologies [9–12] is of paramount importance. In terms of describing them, some new issues of quantum SMC protocols have been explored, such as quantum multiparty summation [13–19], quantum private set intersection [20–25], quantum private comparison [26–31] and quantum anonymous ranking [32–34], etc. However, the research of quantum solutions to the blind millionaire problem is still in the stage of starting. In order to simplify the expression, the corresponding problem is named the quantum blind millionaire (QBM) problem. Intuitively, the solution to the QBM problem divides into two parts: quantum private summation (QPS) and quantum private comparison (QPC). However, directly applying the existing QPC and QPS methods will result in an excessively complex QBM protocol process, while making private messages more prone to leakage. In response to this set of problems, research has emerged on the QBM problem.

In 2023, Zhang et al. proposed a solution to the QBM problem with the special entangled states for the first time [35]. In this case, the parties in two distinct groups can compare the sum of their secrets. However, the solution of Zhang et al. can only achieve comparisons in cases where the total number of participants in two groups is equal. Then Yao et al. used d-level Bell states to solve the QBM problem with any amount of participants in two distinct groups [36]. As the preparation of entangled states is difficult and costly, it is very urgent to propose a more practical scheme for the QBM problem without entangled states. In recent years, d-level single-particle states have received extensive attention in the field of quantum information. Compared with entangled states, single-particle states are simpler to prepare and more stable in laboratory environments. The cost of using single-particle states for quantum communication or quantum computation is usually lower than that of using entangled states. Single-particle states are relatively easy to control and can be operated and measured more flexibly.

In this work, inspired by the relative simplicity of making single-particle states and their low consumption of quantum resources [37–39], under the assumption of no noise losses, we propose a new approach to solving the QBM problem using single-particle states combined with summation and comparison ideas. To facilitate the participants' comparison of the extent of their secrets, a semi-honest party (TP) is presented. Two groups of participants can achieve an overall comparison. Furthermore, the security analysis shows that there are no internal or external risks that can harm our solution.

In general, our contributions to this paper are summarized as follows.

(1) We solve the QBM problem using only d-level single particles for the first time. Compared with entangled states, the preparation of single-particle states is relatively simple and does not require complex experimental setups or significant resource investment.

(2) We give a new solution to the BM problem for any participant with higher quantum efficiency compared to the recent ones.

(3) We simulate the core processes of the proposed protocol with the IBM cloud platform to verify its correctness and feasibility.

The remainder of this paper is structured as follows. In Sect. 2, some preliminary knowledge is introduced. In Sect. 3, a new quantum solution to the QBM problem is described in detail. In Sect. 4, an example is provided to help understand the protocol process. In Sects. 5, 6, 7, and 8, the correctness, comparison and discussion, simulation, and security of this protocol are examined. Finally, Sect. 9 provides a brief discussion and conclusion.

2 Preliminary knowledge

In this section, we first describe the particular structure and characteristics of the d-level single-particle states used in the following protocols. Then the applied shift operation is expressed.

2.1 *d*-Level single quantum states

In a d-level quantum system, single particles have two common conjugate groups. It can be respectively described as

$$G_1 = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\} \tag{1}$$

and

$$G_2 = \{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}. \tag{2}$$

Here, F is the d-level discrete quantum Fourier transform, and $F|t\rangle = \frac{1}{\sqrt{d}} \sum_{\delta=0}^{d-1} e^{\frac{2\pi i \delta t}{d}} |\delta\rangle$, $t = 0, 1, \ldots, d-1$. It is not difficult to see that G_1 and G_2 constitute mutually unbiased bases.

2.2 Shift operation

For the d-level computational basis states, the form of shift operation U_r is shown as follows:

$$U_r = \sum_{h=0}^{d-1} |h \oplus r\rangle \langle h|, \tag{3}$$

where $\oplus$ also defines the modulo d, and $h \in \{0, 1, \ldots, d-1\}$. In the matrix representation, U_r is expressed as a $d \times d$ permutation matrix, where the elements are defined as:

$$[U_r]_{i,j} = \begin{cases} 1, & \text{if } i = j \oplus r; \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Apparently, for a d-level computational basis state $|w\rangle$ ($w \in \{0, 1, \ldots, d-1\}$), after the operation U_r is performed on it, the result will be

$$U_r|w\rangle = |w \oplus r\rangle. \tag{5}$$

3 The proposed solution to QBM problem

In this section, we present a new method for solving the QBM problem, an extension of the classical millionaire problem. The QBM problem is designed within a secure framework to compare the sums of two secret sets without revealing the individual elements of the sets. Our proposed method utilizes only single-particle states and includes three main phases: the initialization phase, the transmission phase, and the comparison phase. Previously, some specific assumptions are seen as follows:

1. There are two groups of participants, group A and group B, who want to compare the sum of their private data. Each group has some participants, $Alice_i$ and Bob_j, where $i \in \{0, 1, \ldots, n\}$, $j \in \{0, 1, \ldots, m\}$ and $m \neq n$.

2. The parties $Alice_i$ and Bob_j possess the secret integers X_i and Y_j, respectively, where X_i and $Y_j \in \{0, 1, \ldots, d-1\}$.

3. A semi-honest third party (TP) [40, 41] is introduced, capable of conducting only individual attacks, without colluding with participants in groups A and B.

4. With the help of TP, the participants in any group will carry out the subsequent stages to fulfill the size relation comparison's objective.

3.1 Initialization phase

Step I1 (*Selecting Random Numbers*): For each participant in any group, $Alice_i$ and Bob_j prepare random number sequences as $R_{ai} = \{R_{ai}^1, R_{ai}^2, \ldots, R_{ai}^L\}$ and $R_{bj} = \{R_{bj}^1, R_{bj}^2, \ldots, R_{bj}^L\}$, where the numbers are chosen randomly from the set $\{0, 1, \ldots, d-1\}$.

Step I2 (*Secret Encoding*): According to the Equation (6), the secrets X_i and Y_j are represented as sequences A_i and B_j. Here $A_i = \{a_i^0, a_i^1, \ldots, a_i^{d-1}\}$ and $B_j = \{b_j^0, b_j^1, \ldots, b_j^{d-1}\}$, where $a_i^t, b_j^t \in \{0, 1\}$, $t \in \{0, 1, \ldots, d-1\}$.

$$a_i^t = \begin{cases} 0, & t \leq X_i - 1 \\ 1, & t > X_i - 1 \end{cases}, \quad b_j^t = \begin{cases} 0, & t \leq Y_j - 1 \\ 1, & t > Y_j - 1 \end{cases}. \tag{6}$$

Step I3 (*Secrets Dividing*): The encoded sequences A_i and B_j are divided into parts d/w by $Alice_i$ and Bob_j as

$$\begin{aligned} &P_{ai}^1, P_{ai}^2, \ldots, P_{ai}^{d/w}, \\ &P_{bj}^1, P_{bj}^2, \ldots, P_{bj}^{d/w}, \end{aligned} \tag{7}$$

where d is an even multiple of w, each part has w bits, and w denotes a positive integer less than d ($1 \leq w \leq d$). Let $d/w = L$; in this case, L is also a positive integer (see Fig. 1).

3.2 Transmission phase

Step T1 (*Quantum States Selecting*): TP prepares two single-particle strings S_a and S_b of length L randomly from G_1 and G_2, where $S_a = \{|S_a^1\rangle, |S_a^2\rangle, \ldots, |S_a^L\rangle\}$ and $S_b = \{|S_b^1\rangle, |S_b^2\rangle, \ldots, |S_b^L\rangle\}$. Then, some decoy states are inserted to form the new sequences M_1 and N_1, where the decoy states are chosen randomly from G_1 and G_2. Then, the sequences M_1 and N_1 are sent to $Alice_1$ and Bob_1, respectively.

Step T2 (*Eavesdropping Detection*): After confirming that $Alice_1$ and Bob_1 have received the sequence M_1 and N_1, the location and measurement basis of every decoy state are released by TP in M_1 and N_1.

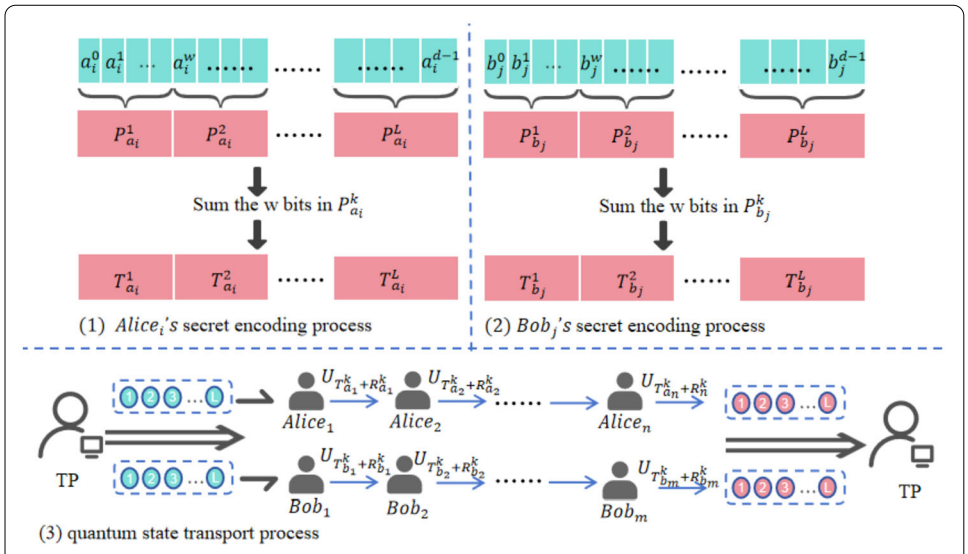

Figure 1 Protocol Flowchart. The first part represents the process of secret coding by the participants of Group A. The second part represents the secret coding process for Group B participants. The third part represents the quantum state transmission process. The participants encode the quantum state by shift operation

According to the measurement results, they carry out eavesdropping checks. The procedure will end and resume at Step T_1 if the error rate exceeds the threshold value; if not, it will move on to the following step. After passing the eavesdropping check successfully, $Alice_1$ and Bob_1 recover the sequences S_a and S_b.

Step T3 (*Secret Transmission*): For $Alice_1$, she firstly computes the sum of w bits in P_{a1}^k and gets the results denoted by T_{a1}^k, here $k \in \{1, \ldots, L\}$. Similarly, Bob_1 computes the sum of w bits in P_{b1}^k and gets the results T_{b1}^k. Then, each of them respectively executes the shift operation $U_{T_{a1}^k + R_{a1}^k}$, $U_{T_{b1}^k + R_{b1}^k}$ on the corresponding $|S_a^k\rangle$, $|S_b^k\rangle$ of S_a and S_b.

In this case, $T_{a1}^k + R_{a1}^k$ is encoded in the k-th particle $|S_a^k\rangle$ of S_a. $Alice_1$ repeats the above process, and the corresponding $T_{a1}^L + R_{a1}^L$ is encoded on the particle $|S_a^L\rangle$. Meanwhile, Bob_1 performs the same operation as $Alice_1$, and encodes $T_{b1}^k + R_{b1}^k$ on $|S_b^k\rangle$ of S_b. Hence, the result sequences $S_{a1} = \{|S_{a1}^1\rangle, |S_{a1}^2\rangle, \ldots, |S_{a1}^L\rangle\}$ and $S_{b1} = \{|S_{b1}^1\rangle, |S_{b1}^2\rangle, \ldots, |S_{b1}^L\rangle\}$ are generated. Then, $Alice_1$ and Bob_1 send the sequences S_{a1} and S_{b1} with the decoy states to $Alice_2$ and Bob_2.

After passing the detection of eavesdropping, $Alice_2$ and Bob_2 recover the sequences and execute the shift operation $U_{T_{a2}^k + R_{a2}^k}$ and $U_{T_{b2}^k + R_{b2}^k}$ on the corresponding k-th particle of the quantum sequences and get $S_{a2} = \{|S_{a2}^1\rangle, |S_{a2}^2\rangle, \ldots, |S_{a2}^L\rangle\}$ and $S_{b2} = \{|S_{b2}^1\rangle, |S_{b2}^2\rangle, \ldots, |S_{b2}^L\rangle\}$. Similarly, $Alice_2$ and Bob_2 send the sequences S_{a2} and S_{b2} with the decoy states to $Alice_3$ and Bob_3. After that, move on to the following participants, until the last participants $Alice_n$ and Bob_m perform the operations $U_{T_{an}^k + R_{an}^k}$ and $U_{T_{bm}^k + R_{bm}^k}$ on the corresponding quantum sequences, and send $S_{an} = \{|S_{an}^1\rangle, |S_{an}^2\rangle, \ldots, |S_{an}^L\rangle\}$ and $S_{bm} = \{|S_{bm}^1\rangle, |S_{bm}^2\rangle, \ldots, |S_{bm}^L\rangle\}$ with the decoy states back to TP securely.

Step T4 (*Quantum State Measurement*): TP performs eavesdropping checks for all particles received. After passing the eavesdropping check successfully, TP measures the quan-

tum states S_{an} and S_{bm} and obtains the sum of $2l$ secret groups and random numbers,

$$\begin{aligned} M_a^k &= \sum_{i=1}^{n} \left(T_{ai}^k + R_{ai}^k\right), \\ M_b^k &= \sum_{j=1}^{m} \left(T_{bj}^k + R_{bj}^k\right), \end{aligned} \tag{8}$$

here, $k \in \{1, 2, \ldots, L\}$.

3.3 Comparison phase

Step C1 (*Data Publication*): Each participant $Alice_i$ and Bob_j has prepared a sequence of random numbers $R_{ai} = \{R_{ai}^1, R_{ai}^2, \ldots, R_{ai}^L\}$ and $R_{bj} = \{R_{bj}^1, R_{bj}^2, \ldots, R_{bj}^L\}$ in Step I1. Each participant $Alice_i$ and Bob_j sums all elements in their random number sequences,

$$\begin{aligned} R_{ai} &= \sum_{k=1}^{L} R_{ai}^k, \\ R_{bj} &= \sum_{k=1}^{L} R_{bj}^k, \end{aligned} \tag{9}$$

and sends R_{ai} and R_{bj} to TP. Meanwhile, the number of participants in Group A, the number of participants in Group B, and the encoded secret bits are announced as n, m and d.

Step C2 (*Compare Size*): With the received sequences, TP firstly computes

$$\begin{aligned} C_a &= \sum_{k=1}^{L} M_a^k, \\ C_b &= \sum_{k=1}^{L} M_b^k. \end{aligned} \tag{10}$$

After that, TP deducts the corresponding random numbers to obtain

$$\begin{aligned} C_a' &= C_a - \sum_{i=1}^{n} R_{ai}, \\ C_b' &= C_b - \sum_{j=1}^{m} R_{bj}. \end{aligned} \tag{11}$$

Finally, TP calculates

$$H = (n - m)\, d - \left(C_a' - C_b'\right). \tag{12}$$

With the value of H, the size relationship between X and Y can be compared according to the following rule

$$\begin{cases} H > 0, & X > Y \\ H = 0, & X = Y \\ H < 0, & X < Y \end{cases}, X = \sum_{i=1}^{n} X_i, Y = \sum_{j=1}^{m} Y_j \tag{13}$$

Here, X represents the secret sum of group A and Y represents the secret sum of group B. The exact proof process will be shown in the correct analysis.

Table 1 relevant data for groups A and B

Participant	Size	Encoding	Sum
$Alice_1$	2	0 0 1 1 1 1 1 1	6
$Alice_2$	1	0 1 1 1 1 1 1 1	7
$Alice_3$	2	0 0 1 1 1 1 1 1	6
Bob_1	1	0 1 1 1 1 1 1 1	7
Bob_2	5	0 0 0 0 0 1 1 1	3

In the above protocol, although the security of participants' secret information can be ensured, TP can still obtain the sum of the two groups' secrets. To further enhance security and prevent TP from gaining access to the true sum of the two groups' secrets, the technology of quantum key distribution (QKD) can be introduced, if possible. The specific steps are as follows:

1. $Alice_1$ from group A and Bob_1 from group B securely share a key y during the initial phase of the protocol through QKD.

2. In Step T3, the original shift operations of $Alice_1$ and Bob_1 are updated to execute the shift operation $U_{T^k_{a1}+R^k_{a1}+y}$, $U_{T^k_{b1}+R^k_{b1}+y}$.

3. Even if TP subtracts the random number during calculations, it cannot recover the true sum of the two groups' secrets, thereby ensuring a higher level of security.

This approach effectively prevents TP from obtaining the true sum of the two groups' secrets during interactions, further strengthening the security of the protocol.

4 Example

We give the following example to show the execution of the protocol. For groups A and B with participants $Alice_i$ and Bob_j, $Alice_i$ and Bob_j have respective private secrets X_i and Y_j, where $i \in \{1, 2, \ldots, n\}$, $j \in \{1, 2, \ldots, m\}$. They encode their secrets according to the rules of the above protocol

$$\begin{aligned} A_i &= \{a_i^0, a_i^1, \ldots, a_i^{d-1}\} = \{0_0, 0_1, \ldots, 0_{X_i-1}, 1_{X_i+1}, \ldots, 1_{d-1}\}, \\ B_j &= \{b_j^0, b_j^1, \ldots, b_j^{d-1}\} = \{0_0, 0_1, \ldots, 0_{Y_j-1}, 1_{Y_j+1}, \ldots, 1_{d-1}\}. \end{aligned} \tag{14}$$

Since random numbers are subtracted in the final stage, their effect is not considered here. After completing step C2, TP will get the results of $\sum_{i=1}^{n}\sum_{t=1}^{d-1} a_i^t$ and $\sum_{j=1}^{m}\sum_{t=1}^{d-1} b_j^t$ as C'_a, C'_b. Then, TP will be able to compare the size of group A secrets with group B secrets by the value of H.

In order to simplify the description, the detection of eavesdropping is ignored. Suppose group A has 3 participants, group B has 2 participants, and the length of the sequence is 8, that is, $n = 3$, $m = 2$, and $d = 8$. The secrets of $Alice_1$, $Alice_2$, and $Alice_3$ are 2, 1, 2. The secrets of Bob_1 and Bob_2 are 1, 5. The comprehensive analysis is displayed in Table 1.

$$\begin{aligned} A_1 &= (0, 0, 1, 1, 1, 1, 1, 1) \\ A_2 &= (0, 1, 1, 1, 1, 1, 1, 1) \\ A_3 &= (0, 0, 1, 1, 1, 1, 1, 1) \\ B_1 &= (0, 1, 1, 1, 1, 1, 1, 1) \\ B_2 &= (0, 0, 0, 0, 0, 1, 1, 1) \end{aligned} \tag{15}$$

Hence,

$$C'_a = \sum_{i=1}^{3} \sum_{t=1}^{d-1} a_i^t = 19, \tag{16}$$

$$C'_b = \sum_{j=1}^{2} \sum_{t=1}^{d-1} b_j^t = 10. \tag{17}$$

According to the Equation (12), TP calculates $H = 8 - 9 = -1 < 0$. The rule for H shows the secret sum of $Alice_1$, $Alice_2$, and $Alice_3$ is smaller than the secret sum of Bob_1 and Bob_2.

5 Correctness analysis

In this section, we present a rigorous mathematical analysis to establish the correctness of the protocol, proving its verifiability. TP can accurately compare the secret sums of any two groups of participants based on the values taken by H.

Theorem 1 *The proposed performance in Sect. 3 can solve the QBM problem correctly.*

Proof In this protocol, it can be seen that the value of H is used to compare the size of the secret sum of Group A and Group B, i.e.

$$H = (n - m)\, d - \left(C'_a - C'_b\right) = \sum_{i=1}^{n} X_i - \sum_{j=1}^{m} Y_j. \tag{18}$$

The procedure for proving Equation (18) is as follows: In the initialization phase, it is established that the secrets of $Alice_i$ and Bob_j are represented by the sequences $A_i = \{a_i^0, a_i^1, \ldots, a_i^{d-1}\}$ and $B_j = \{b_j^0, b_j^1, \ldots, b_j^{d-1}\}$, where $a_i^t, b_j^t \in \{0, 1\}$, $t \in \{0, 1, \ldots, d-1\}$. According to the encoding rules, there are

$$\begin{aligned} X_i + \sum_{t=0}^{d-1} a_i^t &= d, i = 1, 2, \ldots, n, \\ Y_j + \sum_{t=0}^{d-1} b_j^t &= d, j = 1, 2, \ldots, m. \end{aligned} \tag{19}$$

Summing the two sets of equations in Equation (18) yields the following equation

$$\begin{aligned} \sum_{i=1}^{n} X_i + \sum_{i=1}^{n} \sum_{t=0}^{d-1} a_i^t &= nd, \\ \sum_{j=1}^{m} Y_j + \sum_{j=1}^{m} \sum_{t=0}^{d-1} b_j^t &= md. \end{aligned} \tag{20}$$

Then the equations in Equation (20) are subtracted correspondingly to obtain the following Equation (21)

$$\left(\sum_{i=1}^{n} X_i - \sum_{j=1}^{m} Y_j \right) + \left(\sum_{i=1}^{n} \sum_{t=0}^{d-1} a_i^t - \sum_{j=1}^{m} \sum_{t=0}^{d-1} b_j^t \right) = (n - m)\, d. \tag{21}$$

According to the summation process of TP in the comparison phase, it can be obtained that

$$\begin{aligned} C'_a &= \sum_{k=1}^{L}\sum_{i=1}^{n}\left(T_{ai}^k + R_{ai}^k\right) - \sum_{i=1}^{n} R_{ai} = \sum_{i=1}^{n}\sum_{k=1}^{L} T_{ai}^k, \\ C'_B &= \sum_{k=1}^{L}\sum_{j=1}^{m}\left(T_{bj}^k + R_{bj}^k\right) - \sum_{j=1}^{m} R_{bj} = \sum_{j=1}^{m}\sum_{k=1}^{L} T_{bj}^k. \end{aligned} \tag{22}$$

Due to $T_{ai}^k = \sum_{p=0}^{w-1} a_i^p$ and $T_{bj}^k = \sum_{p=0}^{w-1} b_j^p$, $k \in \{1, 2, \ldots, L\}$,

$$C'_a = \sum_{i=1}^{n}\sum_{t=0}^{d-1} a_i^t; C'_b = \sum_{j=1}^{m}\sum_{t=0}^{d-1} b_j^t. \tag{23}$$

Substituting into Equation (20), the collation yields

$$H = (n-m)\,d - \left(C'_a - C'_b\right) = \sum_{i=1}^{n} X_i - \sum_{j=1}^{m} Y_j. \tag{24}$$

This shows that the value of H determines the size of the sum of the secret values of Group A and Group B. □

6 Comparison and discussion

Recently, a series of new QBM protocols have been proposed [42–45]. All of them make positive developments in this new topic. In this section, we analyze the performance of this protocol and compare it with existing QBM protocols in terms of quantum resources, quantum operations, number of participants, and quantum efficiency in Table 2.

Here the quantum efficiency is previously defined as:

$$\eta = \frac{c}{q+b}$$

where b represents the number of classical bits exchanged to decode the message, c represents the total number of bits in the classical plaintext message, and q represents the total number of quantum bits used in the protocol.

Compared to the two-party protocol in Ref. [42], our protocol supports a larger number of participants by introducing a QBM protocol designed for n-party participation. This enhanced scalability significantly improves the practicality and flexibility of our protocol. Moreover, our protocol also demonstrates superior quantum efficiency compared to Ref. [42], further highlighting its practical value.

Compared with the protocols in Ref. [43], Ref. [44] and Ref. [45], our protocol exhibits a clear advantage in quantum efficiency. In particular, compared to Ref. [43], our protocol also supports a broader range of functions. That is Ref. [43] only enables equality comparisons, whereas our protocol is capable of both size comparisons, making it more versatile and applicable in various scenarios.

Table 2 Comparison of Protocols

Protocol Name	Our Protocol	Ref. [42]	Ref. [43]	Ref. [44]	Ref. [45]
Participants numbers	n	2	n	n	n
Quantum Operations	Shift Operation	H, I	Rotation, Swap	Shift Operation	Phase Shift, CNOT
Quantum Resources	d-level single particle states	single-photon states	d-level Bell states	d-level two-particle entangled states	d-level n-particle entangled states
Efficiency	$\frac{1}{\frac{2L}{l+n}} \leq \frac{1}{n+2}$, $L \leq l$	$\frac{1}{n+\lambda}$, when $\lambda > 1$	$\frac{1}{n+2}$	$\frac{1}{2n+2} \geq \frac{1}{2n}$, when $n \geq 1$	$\frac{1}{n(2n+2)} \geq \frac{1}{3n+2}$, when $n \geq l$

In summary, our protocol demonstrates significant advantages in terms of participant scalability, quantum efficiency, and functional versatility. These features highlight the protocol's technical innovation and its high potential for practical applications.

7 Simulation

In order to verify the underlying principles of the protocols, we use the IBM Quantum Simulator (IBMQS) to simulate the experiment of encoding and measurement for d-level single-particle quantum states, omitting the eavesdropping check steps and disregarding random numbers. The following simulation of the test procedure is carried out.

Briefly, we suppose that TP generates two quantum states $F|18\rangle$ and $|21\rangle$, and sends them to two groups of participants, respectively. Firstly, the quantum state $F|18\rangle$ is sent to Group A, which represents it in binary form as $q[0]$, $q[1]$, $q[2]$, $q[3]$, $q[4]$. Here, Group A has participants $Alice_1$ and $Alice_2$. According to the shift operation $U_m|w\rangle = |w \oplus r\rangle$, the quantum state $F|18\rangle$ is shifted 5 bits for the first time by $Alice_1$, that is, $U_m F|18\rangle = F|18 \oplus 5\rangle = F|23\rangle$ and then 6 bits by $Alice_2$, i.e., $U_m F|23\rangle = F|23 \oplus 6\rangle = F|29\rangle$. Similarly, TP generates the second quantum state, $|21\rangle$, which is also represented in binary form as $q[0]$, $q[1]$, $q[2]$, $q[3]$, $q[4]$ and sent to Group B, consisting of participants Bob_1 and Bob_2. The quantum state $|21\rangle$ is shifted 3 bits for the first time by Bob_1, that is, $U_m|21\rangle = |21 \oplus 3\rangle = |24\rangle$ and 7 bits by Bob_2, i.e. $U_m|24\rangle = |24 \oplus 7\rangle = |31\rangle$. The simulation encoding process is shown in Fig. 2 and Fig. 3.

Then, the final two quantum states are returned to the TP. After 20,000 simulations, TP measures the quantum states as shown in Fig. 4. According to the principle of decimal to binary conversion, 29 = 11101 and 31 = 11111. The measurement frequencies of the two

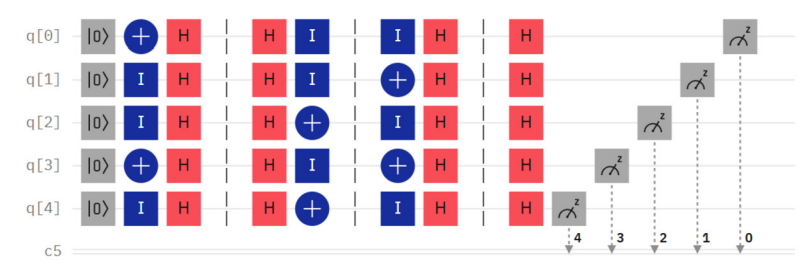

Figure 2 The line diagram of quantum evolution for the summation of Group A. In the image, $q[0]$, $q[1]$, $q[2]$, $q[3]$, $q[4]$ represent the process of shifting the quantum state of the binary form of $F|18\rangle$. The classical bits $c[5]$ will reflect the measurement results of TP

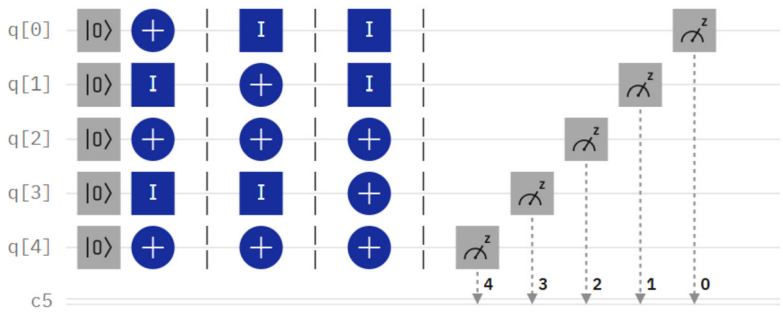

Figure 3 The line diagram of quantum evolution for the summation of Group B. In the image, $q[0]$, $q[1]$, $q[2]$, $q[3]$, $q[4]$ represent the process of shifting the quantum state of the binary form of $|21\rangle$. The classical bits $c[5]$ will reflect the measurement results of TP

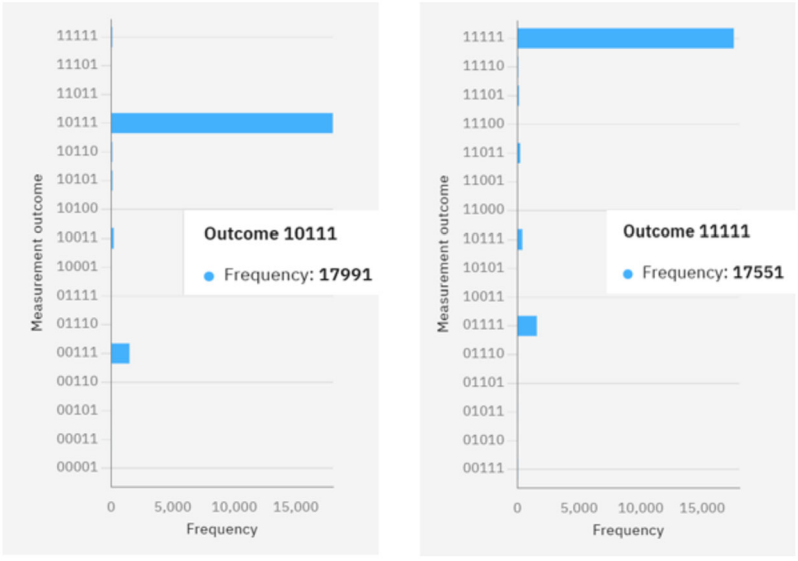

Figure 4 Quantum state measurements of group A is on the left and Quantum state measurements of group B is on the right

sets of experimental results are 17,991 and 17,551, respectively. Although there are minor errors due to qubit noise and measurement inaccuracies, the overall results are highly consistent with the theoretical expectations.

Based on the analysis above, it can be seen that the measurement results are consistent with the results of our protocol. It means that the proposed protocol conforms to the underlying logic and can be achieved in the practical equipment.

8 Security analysis

In this section, we will show that the developed protocol can withstand both internal and external attacks. Here, it should be noted that the internal attack mainly comes from the semi-honest TP and malicious participants. As TP is not directly involved in the secret transmission process, it may obtain the secrets by entangle-measure attack and intercept-resend attack. Malicious participants may obtain secrets through independent participant attacks and collusion attacks. The external attack comes from external attackers. Since

TP and participants are involved in the protocol process, they can gather some private messages more successfully than outside attackers. That is, external attacks will not be feasible if internal attacks are preventable. The security analysis of this protocol is shown below.

8.1 Intercept-resend attack from the semi-honest TP

Without loss of generality, TP intends to get the secret of $Alice_i$ without working with anybody else. However, since TP and $Alice_i$ do not directly transfer particles in the protocol, it may perform an intercept-resend attack to realize his goal. In the transmission phase, TP first finds a way to intercept the quantum bits when the qubits are transferred from $Alice_i$ to $Alice_{i+1}$. Then it replaces them with fake ones and sends them to $Alice_{i+1}$. However, because of the existence of decoy states, it is impossible to determine which bits contain secrets in the sequence. In this sense, for every decoy state, TP must select the appropriate measurement basis. We assume that δ is the number of decoy states and there is a particle that carries the secret in the sequence. If TP intercepts one of the particles passing from $Alice_i$ to $Alice_{i+1}$, the successful detection probability of TP will be

$$P_1 = 1 - (\tfrac{1}{2})^{1+\delta}. \tag{25}$$

It can be seen that P_1 will approach 1 with the increment of δ (see Fig. 5). Therefore, TP will not be able to get $Alice_i$'s secret without being caught.

8.2 Entangle-measure attack from the semi-honest TP

In addition to that, TP may also perform entangle-measure attack to obtain $Alice_i$'s secret. In this sense, TP performs a unitary operation U_E to intercept the particle sequence that is transferred from $Alice_{i-1}$ to $Alice_i$ and entangles it with an auxiliary particle $|e\rangle$ in order to extract additional information, which is designated as

$$\begin{aligned} U|0\rangle|e\rangle &= \mu|0\rangle|e_{00}\rangle + \delta|1\rangle|e_{01}\rangle = \mu|0\rangle|e_{00}\rangle, \\ U|1\rangle|e\rangle &= \omega|0\rangle|e_{10}\rangle + \lambda|1\rangle|e_{11}\rangle = \lambda|1\rangle|e_{11}\rangle. \end{aligned} \tag{26}$$

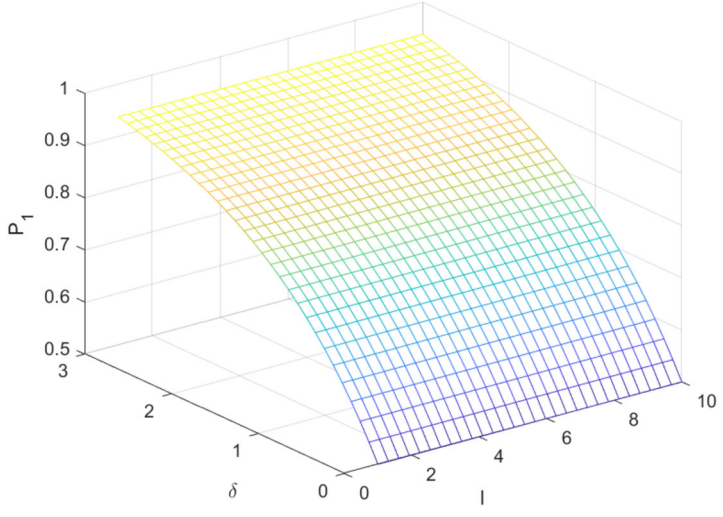

Figure 5 The probability of being detected when TP carries out Intercept-resend attack

It should be mentioned that the four distinct quantum states are $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$, and the coefficient relationships are $||\mu||^2 + ||\delta||^2 = 1$ and $||\omega||^2 + ||\lambda||^2 = 1$. The decoy states are taken from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The corresponding operations can be seen as follows:

$$\begin{aligned} U|+\rangle|e\rangle &= \tfrac{1}{\sqrt{2}}(\mu|0\rangle|e_{00}\rangle + \delta|1\rangle|e_{01}\rangle) + \tfrac{1}{\sqrt{2}}(\omega|0\rangle|e_{10}\rangle + \lambda|1\rangle|e_{11}\rangle) \\ &= \tfrac{1}{2}(|+\rangle(\mu|e_{00}\rangle + \delta|e_{01}\rangle)) + \tfrac{1}{2}(|+\rangle(\omega|e_{10}\rangle + \lambda|e_{11}\rangle)) \\ &+\tfrac{1}{2}(|-\rangle(\mu|e_{00}\rangle - \delta|e_{01}\rangle)) + \tfrac{1}{2}(|-\rangle(\omega|e_{10}\rangle - \lambda|e_{11}\rangle)), \end{aligned} \tag{27}$$

$$\begin{aligned} U|-\rangle|e\rangle &= \tfrac{1}{\sqrt{2}}(\mu|0\rangle|e_{00}\rangle + \delta|1\rangle|e_{01}\rangle) - \tfrac{1}{\sqrt{2}}(\omega|0\rangle|e_{10}\rangle + \lambda|1\rangle|e_{11}\rangle) \\ &= \tfrac{1}{2}(|+\rangle(\mu|e_{00}\rangle + \delta|e_{01}\rangle)) - \tfrac{1}{2}(|+\rangle(\omega|e_{10}\rangle + \lambda|e_{11}\rangle)) \\ &+\tfrac{1}{2}(|-\rangle(\mu|e_{00}\rangle - \delta|e_{01}\rangle)) - \tfrac{1}{2}(|-\rangle(\omega|e_{10}\rangle - \lambda|e_{11}\rangle)). \end{aligned} \tag{28}$$

The equation needs to meet these requirements in order to avoid errors and pass eavesdropping detection. Hence, the result will be

(1) $\delta = \omega = 0$ occurs when the decoy particles are selected from $|0\rangle$ and $|1\rangle$.

(2) After selecting the fictitious particles from $|+\rangle$ and $|-\rangle$, it will become

$$\begin{aligned} &\mu|e_{00}\rangle - \delta|e_{01}\rangle + \omega|e_{10}\rangle - \lambda|e_{11}\rangle = 0, \\ &\mu|e_{00}\rangle + \delta|e_{01}\rangle - \omega|e_{10}\rangle - \lambda|e_{11}\rangle = 0. \end{aligned} \tag{29}$$

Based on the above conclusions, we can derive

$$\mu|e_{00}\rangle = \lambda|e_{11}\rangle. \tag{30}$$

Thus, TP is unable to discriminate between $\mu|e_{00}\rangle$ and $\lambda|e_{11}\rangle$. It is evident that the entanglement measurement assault is unsuccessful since the measurement of the auxiliary particles yields no useful information.

8.3 Independent attack by the participant in each group

In the proposed protocol, Alice in Group A and Bob in Group B participate in similar actions. Without loss of generality, $Alice_{i+1}$ is taken to be dishonest, and $Alice_{i+1}$ wants to acquire $Alice_i$'s secret from Group A as an example to analyze the security. Here, it is necessary to obtain the random number R_A^i and each part of the secret sum of $Alice_i$. The difference from TP is that $Alice_{i+1}$ can have secret transfers directly with $Alice_i$.

With the particle received by $Alice_{i+1}$, $Alice_{i+1}$ can know the particle state after $Alice_i$ performs the shift operation. Therefore, in order to obtain the shift operation of $Alice_i$, $Alice_{i+1}$ only needs to guess the initial state of $Alice_i$. However, due to the presence of random numbers, he is unable to gather any knowledge about $Alice_i$'s secret. As the probability of guessing each secret correctly is $\frac{1}{d}$, the probability that $Alice_{i+1}$ correctly guesses the secret of $Alice_i$ is P_2. (see Fig. 6).

$$P_2 = \tfrac{1}{d} \times \tfrac{1}{d} \cdots \times \tfrac{1}{d} = (\tfrac{1}{d})^L \tag{31}$$

8.4 Internal attack by the participants collusion

As we know, the most serious attack is the collusion attack. In particular, the most powerful case is that the $n-1$ parties are dishonest in total. Collusion attacks fall into two

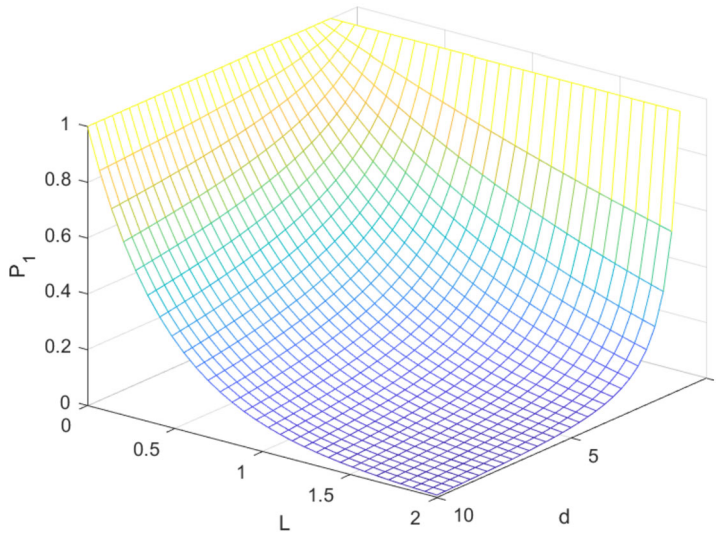

Figure 6 The possibility of participants having access to others' secrets

categories: inter-group collusions, in which certain members of the group have the desire to steal another member's secret; cross-group collusions, in which a few members from one group team up with some members from the other group to obtain a member's secret.

(1) Inter-group collusive attack

We assume that $Alice_1$, $Alice_3$ to $Alice_n$ are dishonest participants conspiring to obtain the secret of $Alice_2$. According to the secret transmission process, $Alice_n$ can collect all participants' secret sum with random numbers. Since $Alice_1$, $Alice_3$ to $Alice_{n-1}$ publish the secret with random numbers, they will get

$$C_a - \sum_{k=1}^{L}\left[\left(T_{a1}^k + R_{a1}^k\right) + \sum_{i=3}^{n}\left(T_{ai}^k + R_{ai}^k\right)\right] = \sum_{k=1}^{L}\left(T_{a2}^k + R_{a2}^k\right). \tag{32}$$

Since the participants only published the sum of the random numbers R_{ai}, they do not have access to the secret information of $Alice_2$. Thus, they can only achieve their goal by guessing $Alice_2$'s random number. The probability that they will obtain $Alice_2$'s secret is P_3 as

$$P_3 = (\frac{1}{d})^L. \tag{33}$$

(2) Cross-group collusive attack

We suppose $Alice_1$, $Alice_2$ to $Alice_n$ conspires with Bob_1, Bob_3 to Bob_m and want to steal Bob_2's secret. In this instance, there is a simultaneous external and internal attack since we can view $Alice_1$, $Alice_2$ to $Alice_n$ as external attackers and Bob_1, Bob_2 to Bob_m as the collusion of inside attackers. However, these two attacks are ineffective according to our analysis above. Here, P_4 is the probability of accurately guessing the secret, and P_5 is the

probability that they will be discovered, where δ is the number of decoy states.

$$P_4 = (\frac{1}{d})^L \tag{34}$$

$$P_5 = 1 - (\frac{1}{2})^{1+\delta} \tag{35}$$

In all, internal attackers cannot get the private secrets of legal participants. In addition, for outside attackers, their abilities are limited. It seems that only the entangle-measure and intercept-resend attacks may be performed since they do not take part in the participant's secret transmission process. According to the analysis above, the attacks are invalid. Therefore, the presented protocol can effectively resist these attacks.

8.5 External attack

In the analysis, we assume that the external eavesdropper, Eve, attempts to steal confidential information from the participants. Since Eve is not involved in the process of secret transmission between participants, Eve is limited to employing entangle-measure attacks and intercept-resend attacks. However, the unique role of TP in the protocol grants TP access to significantly more information than Eve. Based on the prior security analysis, the protocol has been shown to effectively resist both intercept-resend attacks and entangle-measure attacks. Consequently, Eve is unable to successfully compromise the participants' confidential information.

9 Conclusion

In this paper, for two groups A and B each with a different number of n and m participants, a private comparison of the secret sum of Group A and Group B can be obtained. During it, the new vector coding method for d-level single-particle states is used to protect the participant's secret. Meanwhile, the chosen random numbers and decoy states are also included. Additionally, the protocol can effectively reduce the number of particle transmissions by not requiring shared keys or entangled states. In the future, we hope that more efficient and universal solutions will be provided to the QBM problem without TP, and the present attempts could lead to positive developments in QSMC.

Abbreviations

BM, blind millionaire; QBM, quantum blind millionaire; SMC, secure Multiparty Computing; QPS, quantum private summation; QPC, quantum private comparison..

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant 62271234, the Open Foundation of State Key Laboratory of Public Big Data (Guizhou University) under Grant No. PBD2022-16, the Fundamental Research Funds for Heilongjiang Universities under Grant 2022-KYYWF-1042, Double First-Class Project for Collaborative Innovation Achievements in Disciplines Construction in Heilongjiang Province under Grant No. LJGXCG2022-054 and LJGXCG2023-028. In addition, we sincerely thank IBM cloud platform for providing access to the IBM Quantum Simulator (IBMQS), which played a crucial role in supporting the experimental work and simulations conducted in this research.

Author contributions

Kunchi Hou completed the methodology, conceptualization, validation and writing-original draft of manuscript. Kejia Zhang supervised, modified and writing-review & editing. Huixin Sun handled the investigaion, formal analysis and modification of manuscript. Yao Yao supervised and supported the methodology of manuscrip. Yu Zhang supervised and all authors reviewed the manuscript.

Funding
This work was supported by the National Natural Science Foundation of China under Grant 62271234, the Open Foundation of State Key Laboratory of Public Big Data (Guizhou University) under Grant No. PBD2022-16, the Fundamental Research Funds for Heilongjiang Universities under Grant 2022-KYYWF-1042, Double First-Class Project for Collaborative Innovation Achievements in Disciplines Construction in Heilongjiang Province under Grant No. LJGXCG2022-054 and LJGXCG2023-028.

Data Availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
The Author confirms: that the work described has not been published before; that it is not under consideration for publication elsewhere; that its publication has been approved by all co-authors.

Competing interests
The authors declare no competing interests.

Author details
[1]School of Mathematical Science, Heilongjiang University, Xuefu, Harbin, 150080, Asia, China. [2]School of Computer Science and Big Data (School of Cybersecurity), Heilongjiang University, Xuefu, Harbin, 150080, Asia, China. [3]State Key Laboratory of Public Big Data, Guizhou University, Huaxi, Guiyang, 550000, Asia, China. [4]Institute for Cryptology and Network Security, Heilongjiang University, Xuefu, Harbin, 150080, Asia, China.

Received: 30 June 2024 Accepted: 8 January 2025 Published online: 23 January 2025

References

1. Yao AC. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science. Los Alamitos: IEEE; 1982. p. 160–4.
2. Boudot F, Schoenmakers B, Traore J. A fair and efficient solution to the socialist millionaires' problem. Discrete Appl Math. 2001;111(1–2):23–36.
3. Li SD, Wang DS, Dai YQ. Symmetric cryptographic protocols for extended millionaires' problem. Sci China, Ser F, Inf Sci. 2009;52(6):974–82.
4. Damle S, Faltings B, Gujar S. Blockchain-based practical multi-agent secure comparison and its application in auctions. In: IEEE/WIC/ACM international conference on web intelligence and intelligent agent technology. 2021. p. 430–7.
5. Li D, Liao X, Tao X, et al. Privacy-preserving self-serviced medical diagnosis scheme based on secure multi-party computation. Comput Secur. 2020;90:101701.
6. Sucasas V, Aly A, Mantas G, et al. Secure multi-party computation-based privacy-preserving authentication for smart cities. IEEE Trans Cloud Comput. 2023.
7. Khan HM, Khan A, Jabeen F, et al. Fog-enabled secure multiparty computation based aggregation scheme in smart grid. Comput Electr Eng. 2021;94:107358.
8. Li SD, Zhang MY. An effcient solution to the blind millionaires' problem. Int J Found Comput Sci. 2020;26:1–2. https://doi.org/10.11897/SPJ.1016.2020.01755.
9. Yi X, Huo JC, Gao YP, et al. Iterative quantum algorithm for combinatorial optimization based on quantum gradient descent. Results Phys. 2024;56:107204.
10. Ye TY, Geng MJ, Xu TJ, et al. Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. Quantum Inf Process. 2022;21(4):123.
11. Chen G, Wang Y, Jian L, et al. Quantum identity authentication based on the extension of quantum rotation. EPJ Quantum Technol. 2023;10(1):11.
12. Mishra S, Thapliyal K, Parakh A, et al. Quantum anonymous veto: a set of new protocols. EPJ Quantum Technol. 2022;9(1):14.
13. Tsai CW, Lin J, Yang CW. Cryptanalysis and improvement of quantum secure multi-party summation using single photons. Phys Scr. 2024.
14. Wang N, Tian X, Zhang X, et al. Quantum secure multi-party summation with identity authentication based on commutative encryption. MDPI. 2023;10(5):558.
15. Yi X, Cao C, Fan L, et al. Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. In: Quantum information processing. vol. 20. 2021. p. 249.
16. Sutradhar K, Om H. Hybrid quantum protocols for secure multiparty summation and multiplication. Sci Rep. 2020;10(1):9097.
17. Yi X, Cao C, Fan L, et al. Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. In: Quantum information processing. vol. 20. 2021. p. 249.
18. Yi X, Cao C, Fan L, et al. Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform. In: Quantum information processing. vol. 20. 2021. p. 249.
19. Zhang Y, Yao Y, Sun H, et al. A New Hybrid Protocol that Simultaneously Achieves Quantum Multiparty Summation and Ranking. Adv Quantum Technol. 2400078.

20. Mohanty T, Srivastava V, Debnath SK, et al. Quantum secure threshold private set intersection protocol for iot-enabled privacy preserving ride-sharing application. IEEE Internet Things J. 2023.
21. Chen Y, Situ H, Huang Q, et al. A novel quantum private set intersection scheme with a semi-honest third party. Quantum Inf Process. 2023;22(12):429.
22. Shi RH, Li YF. Quantum private set intersection cardinality protocol with application to privacy-preserving condition query. IEEE Trans Circuits Syst I, Regul Pap. 2022;69(6):2399–411.
23. Liu W, Yin HW. A novel quantum protocol for private set intersection. Int J Theor Phys. 2021;60(6):2074–83.
24. Shi RH, Li YF. Quantum protocol for secure multiparty logical AND with application to multiparty private set intersection cardinality. IEEE Trans Circuits Syst I, Regul Pap. 2022;69(12):5206–18.
25. Chi YP, Zhang Y, Zhang KJ, et al. A New Protocol for Semi-quantum Private Set of Intersection and Union Mixed Cardinality for Any Tripartite Based on Bell States. Adv Quantum Technol. **2400137**.
26. Ye TY, Lian JY. A novel multi-party semiquantum private comparison protocol of size relationship with d-dimensional single-particle states. Phys A, Stat Mech Appl. 2023;611:128424.
27. Lian JY, Li X, Ye TY. Multi-party semiquantum private comparison of size relationship with d-dimensional Bell states. EPJ Quantum Technol. 2023;10(1):10.
28. 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(3):035011.
29. Geng MJ, Chen Y, Xu TJ, et al. Single-state semiquantum private comparison based on Bell states. EPJ Quantum Technol. 2022;9(1):36.
30. Gong LH, Chen ZY, Qin LG, et al. Robust Multi-Party Semi-Quantum Private Comparison Protocols with Decoherence-Free States against Collective Noises. Adv Quantum Technol. 2023;2300097.
31. Gong LH, Ye ZJ, Liu C, et al. One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations. Laser Phys Lett. 2024;21(3):035207.
32. Wang Q, Li Y, Yu C, et al. Quantum anonymous ranking and selection with verifiability. In: Quantum information processing. vol. 19. 2020. p. 1–19.
33. Li YR, Jiang DH, Liang XQ. A novel quantum anonymous ranking protocol. In: Quantum information processing. vol. 20. 2021. p. 1–33.
34. Shi WM, Liu S, Zhou YH, et al. A secure quantum multi-party ranking protocol based on continuous variables. Optik. 2021;241:166159.
35. Zhang Y, Zhang L, Zhang K, et al. A new quantum-inspired solution to blind millionaires' problem. Quantum Inf Process. 2023;22(1):80.
36. Yao Y, Zhang KJ, Song TT, et al. The complete new solutions to the blind millionaires' problem in d-dimensional quantum system. Phys A, Stat Mech Appl. 2023;627:129138.
37. Tavakoli A, Herbauts I, Zukowski M, et al. Secret sharing with a single d-level quantum system. Phys Rev A. 2015;92(3):030302.
38. Li YR, Jiang DH, Zhang YH, et al. A quantum voting protocol using single-particle states. In: Quantum information processing. vol. 20. 2021. p. 1–17.
39. Xu TJ, Gan ZG, Ye TY. Multiparty semiquantum key agreement with d-level single-particle states. Phys A, Stat Mech Appl. 2023;128991.
40. Chen Y, Situ H, Huang Q, et al. A novel quantum private set intersection scheme with a semi-honest third party. Quantum Inf Process. 2023;22(12):429.
41. Wu WQ, Zhao YX. Quantum private comparison of size using d-level Bell states with a semi-honest third party. Quantum Inf Process. 2021;20(4):155.
42. Hou M, Wu Y. Single-photon-based quantum secure protocol for the socialist millionaires' problem. Front Phys. 2024;12:1364140.
43. Huang X, Zhang W, Zhang S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. Phys A, Stat Mech Appl. 2024;637:129614.
44. Du G, Zhang Y, Mao X, et al. A new quantum solution to blind millionaires' problem without an honest third party. EPJ Quantum Technol. 2024;11(1):81.
45. Li X, Xiong Y, Zhang C. Secure multiparty quantum computation for summation and data sorting. Quantum Inf Process. 2024;23(9):321.

Publisher's Note