Du et al. *EPJ Quantum Technology* (2024) 11:81
https://doi.org/10.1140/epjqt/s40507-024-00293-3

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

A new quantum solution to blind millionaires' problem without an honest third party

Gang Du[1,2,3], Yu Zhang[3,4], Xinyue Mao[3,4], Hongwei Sun[1,3*†] and Lei Wang[1,3*†]

*Correspondence:
sunhw@hlju.edu.cn;
wanglei@hlju.edu.cn
[1]School of Data Science and Technology, Heilongjiang University, Harbin, 150080, China
[3]Institute for Cryptology and Network Security, Heilongjiang University, Harbin, 150080, China
Full list of author information is available at the end of the article
[†]Equal contributors

Abstract

The quantum blind millionaires' (QBM) problem is an expanded version of the millionaires' problem in a quantum environment. For any two sets with different members, the QBM problem represents the quantum solution of the private summation in each set and the private comparison of the results simultaneously. During it, the secrets of any participant should be protected. As a new topic in quantum secure multiparty computation (QSMC), current solutions to QBM problems usually require an honest third party to resist some potential attack strategies. However, the assumptions will affect their applicability in practical cooperative security systems. In this paper, we propose a new solution to the quantum blind millionaires' (QBM) problem without the help of an honest third party for the first time. In our solution, the shift operations are applied to the d-dimensional 2-particle entangled states to encode the secrets of the participants. According to our analysis, the proposed solution can effectively resist typical internal and external attacks by applying the detection methods generated by the participants. We hope that the research will make positive developments for QSMC.

Keywords: Quantum blind millionaires' problem; Private comparison; Secure multiparty summation; d-dimensional 2-particle entangled states

1 Introduction

In the rapidly advancing information society, collaborative computational tasks are increasingly common. For every participant, personal data usually involves privacy messages that cannot be known to others. In this view, it is necessary to protect private data from being leaked during the computation process. To solve this security risk, secure multiparty computation (SMC) techniques are applied in practice. SMC is a critical topic of cryptography derived from the millionaire problem in 1982 [1]. It refers to two millionaires who own wealth x and y, respectively, and wish to contrast the magnitudes of x and y without disclosing their respective wealth values. The millionaire's problem points out the idea of private comparison. After that, many experts have proposed a large number of protocols to solve it and discuss its applications [2–9]. In recent years, the field of Quantum Secure Multi-Party Computation (QSMC) has emerged, combining the principles

Springer

of quantum computing with SMC to enhance security. The security of QSMC relies on the unique properties of quantum mechanics, such as superposition and entanglement against potential quantum attacks. QSMC aims to perform secure computations among multiple parties using quantum protocols.

Expanding on the millionaire problem, the blind millionaires' (BM) problem is introduced. This problem involves grouping millionaires and comparing the sums of their wealth across groups while preserving the privacy of each individual's private wealth. The idea of the BM problem can be widely used in the fields of data analysis, market research, social surveys, etc. It offers an effective approach to balancing data utilization with personal privacy protection during information processing. In data analysis, the BM problem can be applied to process data sets that contain sensitive personal information. Participants can group data anonymously and compare and analyze the sums of different groups without revealing personal information. This approach enables effective data use and analysis while protecting individual privacy. Market research can use the BM problem to analyze consumer groups and compare preferences and behavioral habits between them without revealing personally identifiable information. This helps companies better understand market demand and develop more accurate marketing strategies. Social surveys and opinion polls can also benefit from the BM problem, as it helps researchers collect data and conduct subgroup analysis without violating the privacy rights of participants. This method allows for the collection of objective and valid survey results while safeguarding the confidentiality of participants' personal information.

In recent years, the rapid development of quantum computing has inspired new approaches to classical cryptographic protocols. Quantum parallel computing capability enables higher computational efficiency and exponential increases in computational speed. Additionally, quantum entanglement is utilized for long-distance information transfer and quantum communication. The generation of quantum randomness based on quantum mechanics is not restricted by classical physical systems. This provides new secure communication methods to improve the security of cryptographic protocols. In response to the advantages brought about by quantum computing, an increasing number of scholars have proposed quantum cryptographic protocols.

To solve the BM problem in a quantum environment, Zhang et al. introduced an honest third party to solve a special case of the BM problem [10]. Here, the quantum blind millionaires' (QBM) problem refers to dividing the participants into two sets with identical numbers. Participants can use quantum technology to compare the relationship between the size of the summation of the secrets of the two sets. Then Yao et al. solved the QBM problem of any number of participants in two different sets based on d-level Bell states [11]. However, it should be noted that during existing solutions, a trusted third-party is introduced to ensure security and reduce the implementation difficulty. As it is difficult to construct an absolutely honest party in practice, the assumption is not available and may lead to some potential attack strategies on the honest party. For example, attackers may destroy the communications between the honest server and the other participants and generate failure attacks of a key single point in the quantum communication network.

In this paper, we design a protocol for the QBM problem without a third party that allows for private comparisons and private summation between different numbers of participants. Previously, two-particle entangled states of d dimension were applied. Using shift operations, participants can encode their secrets and produce a binary sequence of

random integers in the entangled states. In the protocol, though an honest third party is not required, the privacy of the participants' data can be better protected against some internal and external threats, even if the majority of the malevolent participants conspire together.

The arrangement of this paper is as follows. In Sect. 2, we describe some related study on the QBM problem. In Sect. 3, the quantum resources and operations used in the presented solution are described. In Sect. 4, a new QBM solution is proposed without a third party. In Sect. 5, we briefly analyze the correctness of the solution. In Sect. 6, the necessary security analysis are provided. Finally, a conclusion is given in Sect. 7.

2 Related work

In 2009, Yang and Wen first suggested a method to employ two-photon entanglement to solve the millionaires' problem [12]. As an early attempt at quantum secure multiparty computation (QSMC), a few academics developed several methods to solve this problem with the help of an honest third party. For example, Zhang et al. proposed some solutions with better feasibility and security. The quantum blind millionaires' (QBM) problem is an extension of the millionaires' problem [13]-[14]. As seen in its definition, it combines multiparty quantum private summation and quantum private comparison.

For multiparty quantum Private Comparison, Ye and Ji et al. proposed some quantum secure multiparty private comparison protocols based on entanglement exchange in 2016 [15–17]. Then Li et al. and Ye et al. proposed some efficient solutions with novel quantum technologies [18–20]. In 2019, Ye et al. proposed a circular multiparty quantum private comparison protocol with n-level single-particle states [21]. In 2022 and 2023, Geng et al. [22] and Lian et al. [23] proposed semi-quantum private comparison protocols based on Bell states. Recently, Lian et al. proposed a hybrid protocol for multiparty semi-quantum private comparisons, multiplication, and summation based on single-particle states of d dimensions without previously sharing keys [24].

For quantum private summation, Wang et al. proposed a multiparty quantum summation protocol based on the entanglement of d-dimensional Bell states and d-dimensional cat states in 2021 [25]. Then, Zhang et al. proposed a multiparty quantum summation protocol based on entanglement exchange [26]. In 2022, Ye et al. proposed a three-party quantum summation protocol without the help of a third party [27]. Then, Duan and Ye et al. proposed some quantum private summation protocols based on d dimensional quantum systems [28]-[29].

With the development of the millionaires' problem, a new idea named blind millionaires' (BM) problem was proposed in 2020 [30]. Here, Li et al. used shift registers and probabilistic encryption algorithms to solve this problem. To give a quantum solution to the BM problem, Zhang et al. first pointed out the quantum blind millionaires' (QBM) problem and provided a solution to its special case with multiparty entangled states by introducing an honest third party [10]. Here, the QBM problem refers to the division of participants into two sets with identical numbers. Then Yao et al. solved the QBM problem of any number of participants in two different sets based on d-level Bell states in 2023 [11]. However, as a new attempt at QSMC, it still requires further research.

3 Preliminary knowledge

This section introduces the fundamental concepts of quantum states and the operation applied in the following solution.

3.1 Computational basis and Fourier basis

In the d-dimensional quantum system, there exist two different bases named computational basis and a Fourier basis. $\{|j\rangle_C, j = 0, 1, 2, \ldots, d-1\}$ makes up the computational basis, and $\{|j'\rangle_F, j = 0, 1, 2, \ldots, d-1\}$ makes up the Fourier basis. Additionally, after applying the quantum Fourier transform, each computational basis will be transformed into

$$\left|j'\right\rangle_F = \mathcal{F}|j\rangle_C = \frac{1}{\sqrt{d}} \sum_{r=0}^{d-1} \xi^{jr} |r\rangle \tag{1}$$

where $\xi = e^{2\pi i/d}$.

It is evident that applying the Fourier operation on the computational basis yields the Fourier basis.

3.2 d-dimensional 2-particle entangled states $|\chi_2\rangle$

For d-dimensional 2-particle entangled states $|\chi_2\rangle$, the computational basis is expressed as

$$|\chi_2\rangle = \frac{1}{\sqrt{d}} \sum_{j_1+j_2 mod d=0} |j_1\rangle_C |j_2\rangle_C, \tag{2}$$

and the Fourier basis is expressed as

$$|\chi_2\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j'_1\rangle_F |j'_2\rangle_F. \tag{3}$$

In the d-dimensional quantum system, the d-dimensional 2-particle entangled states $|\chi_2\rangle$ have two common properties.

(1) When it is measured using the computational basis, the result is

$$(j_1 + j_2) mod\, d = 0, \tag{4}$$

(2) When it is measured using the Fourier basis, the result is

$$j'_1 = j'_2. \tag{5}$$

3.3 Shift operation

In the following solutions, the secrets and random numbers are encoded using the shift operation, which is described as

$$QS_k = \sum_{j=0}^{d-1} |j \oplus k\rangle\langle j|, \tag{6}$$

where the sign $\oplus$ denotes the addition modulo $d (d \geq 2)$ and $k \in \{0, 1, \ldots, d-1\}$.

3.4 The formal definition of QBM

The quantum blind millionaire problem (QBM) is an extension of the millionaire problem, which is designed in a security framework to compare the sums of two secret sets without revealing the individual elements of the sets.

Given two sets Set A and Set B, where:

(1). Set A consists of n participants $Alice_1, \ldots, Alice_n$, each with a secret value $x_i = \{x_i(1), \ldots x_i(l)\}$.

(2). Set B consists of m participants $Bob_1, \ldots, Bob_m$, each with a secret value $y_j = \{y_j(1), \ldots y_j(l)\}$.

The QBM protocol that allows the participants to compare the sums of their secret values, $\sum_{i=1}^{n} x_i$ and $\sum_{j=1}^{m} y_j$, without revealing the individual secret values. Specifically, the protocol should satisfy the following conditions:

Correctness:

The protocol should correctly output the comparison result of $\sum_{i=1}^{n} x_i$ and $\sum_{j=1}^{m} y_j$.

Privacy:

(1)Privacy of Set A: Participants in Set B should only know the comparison result, not the secret values of Set A. Additionally, participants in Set A should not know the secret values of other participants within Set A.

(2) Privacy of Set B: Participants in Set A should only know the comparison result, not the secret values of Set B Additionally, participants in Set B should not know the secret values of other participants within Set B.

4 QBM solution for participants without a third party

For two different sets, Set A has n participants, $\text{Alice}_i (i = 1, 2, \ldots, n)$; Set B has m participants, $\text{Bob}_j (j = 1, 2, \ldots, m)$. In this section, Alice_i and Bob_j have one secret x_i and y_i, respectively. The secret of each participant is converted into a binary sequence with fixed lengths L, where $x_i, y_i \in \{0, \ldots, d-1\}$. They want to compare the summation $\sum_{i=1}^{n} x_i$, $\sum_{i=1}^{m} y_i$ without divulging their secrets. The specific steps of the solution can be seen as follows.

4.1 Initialization phase

Step I1 Alice_1 prepare l copies of the entangled states of d-dimensional 2-particle

$$|\chi_2\rangle_1, |\chi_2\rangle_2, \ldots, |\chi_2\rangle_l. \tag{7}$$

Alice_1 selects the first particle from each entangled state to form the particle sequence $P_1 = \{p_{11}, \ldots, p_{1l}\}$ and selects the second particle to form the particle sequence $P_2 = \{p_{21}, \ldots, p_{2l}\}$.

Step I2 Alice_1 randomly selects δ particles from d-dimensional 2-particle $|\chi_2\rangle$ to insert them into the sequence P_2, and sends the sequence $P_{2'}$ to the participant Bob_1. Alice_1 randomly selects the computational basis or Fourier basis to measure the test particles of the sequence, and publishes the position and measurement basis. The measurement results of Alice_1 and Bob_1 are m_1 and m_2, respectively, when Alice_1 selects the computational basis. He then confirms whether $(m_1 + m_2) mod\ d = 0$. If Alice_1 choose the Fourier basis, he will determine whether $m_1 = m_2$. If the test is unsuccessful, Bob_1 and Alice_1 will announce to stop and go back to Step 1. When the test is passed, it continues.

4.2 Transmission phase

Step T1 Firstly, Alice_1 converts his secrets into a binary sequence $x_1 = \{x_1(1), \ldots, x_1(t), \ldots, x_1(l)\}, x_1(t) \in \{0, 1\}$. Then he generates a string of random numbers $r_1 = \{r_{11}, \ldots, r_{1t}, \ldots, r_{1l}\}$, where $r_{1t} \in \{0, 1\}$. He encodes secret and random numbers x_1 and r_1 by performing the shift operation in the sequence P_1. Here, Alice_1 encodes $x_1(t)$ and r_{1t} on the corresponding particle p_{1t}, and receives a sequence P_1^1. For example, if Alice_1 encodes the secret and the random number in the sequence P_1, the sequence P_1 will become the sequence $P_1^1 = \{p_{11} \oplus x_1(1) \oplus r_{11}, p_{12} \oplus x_1(2) \oplus r_{12}, \ldots, p_{1l} \oplus x_1(l) \oplus r_{1l}\}$.

Step T2 Bob_1 generates a set of random numbers $r_{1'} = \{r_{11'}, \ldots, r_{1t'}, \ldots, r_{1l'}\}$, he performs the same encoding operations as Alice_1 and obtains particle sequence P_2^1. Alice_1 and Bob_1 randomly select δ particles from the d-dimensional 2-particle $|\chi_2\rangle$ as test particles and insert them into P_1^1, P_2^1, respectively. In this case, they will obtain the sequences $P_1^{1'}, P_2^{1'}$. Then Alice_1 sends the sequence $P_1^{1'}$ to Alice_2, and Bob_1 sends the sequence $P_2^{1'}$ to Bob_2. After receiving Alice_2 and Bob_2, Alice_1 and Bob_1 will publish the position of the test particles and measure the test particles.

Step T3 After discarding the test particles, Alice_2 obtains the sequences P_1^1 and Bob_2 obtains P_2^1. The participants emulate Alice_1 and Bob_1 in their encoding procedures and eavesdropping detection, and send sequences to the next participant. Therefore, Alice_n will get sequences P_1^n and Bob_m will get sequences P_2^m. Then Alice_n sends the sequence $P_1^{n'}$ to Bob_1. Similarly, Bob_m sends the sequence $P_2^{m'}$ to Alice_n.

Step T4 After discarding the test particles, Alice_n obtains the sequences P_2^m, Bob_1 gets the sequences P_1^n. Then Alice_n encodes his random number $r_n = \{r_{n1}, \ldots, r_{nt}, \ldots r_{nl}\}$ in the sequence P_2^m and inserts the test particles. He obtains the sequences $P_2^{m+1'}$ and sends it to Alice_{n-1}. The participants execute the same operation as Alice_n. Finally, Alice_1 receives the sequence P_2^{m+n}. The participants in Set B perform the same operations for the sequence P_1^n, and Bob $_m$ sends the sequence $P_1^{n+m'}$ to Alice_1.

4.3 Measurement comparison phase

Step M1 After discarding the test particles, Alice_1 obtains the sequences ${P_1}^{m+n}$ and ${P_2}^{m+n}$. Then he will use the Fourier basis to measure the l particles in the first particle sequence ${P_1}^{m+n}$ and obtain the result.

$$A_1 = \sum_{i=1}^{n}(x_i(1) + r_{i1}) + \sum_{j=1}^{m} r_{j1'} + p_{11} \tag{8}$$

$$\vdots$$

$$A_l = \sum_{i=1}^{n}(x_i(l) + r_{il}) + \sum_{j=1}^{m} r_{jl'} + p_{1l}. \tag{9}$$

Similarly, *Alice*$_1$ uses the Fourier basis to measure the particles in the second particle sequence ${P_2}^{m+n}$ and obtain the measurement results.

$$B_1 = \sum_{i=1}^{m}(y_i(1) + r_{i1'}) + \sum_{j=1}^{n} r_{j1} + p_{21} \tag{10}$$

$$\vdots$$

$$B_l = \sum_{i=1}^{m}(y_i(l) + r_{il'}) + \sum_{j=1}^{n} r_{jl} + p_{2l}. \tag{11}$$

Finally, $Alice_1$ publishes the measurement results to the participants

Step M2 As the secrets are encoded into binary numbers, the participants need to convert it back according to the value of $A_t(t = 1, \ldots, l)$ and B_t. To better compare the summation of the two sets of secrets, participants can perform the following calculations.

$$H = \sum_{t=1}^{l} 2^{l-t}(A_t - B_t). \tag{12}$$

(1) If $H > 0$, it means that the secret summation in Set A is greater than the secret summation in Set B;

(2) If $H < 0$, it means that the sum of secrets in Set A is less than the sum of secrets in Set B;

(3) If $H = 0$, it means that the sum of secrets in Set A is equal to the sum of secrets in Set B.

The detailed secret transmission process in the QBM solution is shown in Fig. 1, and the protocol flow is presented in Algorithm 1.

As shown in Fig. 1, the solid line indicates that the secret and random numbers are encoded when the shift operations are performed. The dotted line indicates that only the random numbers are encoded when the shift operations are performed. The pink arrow

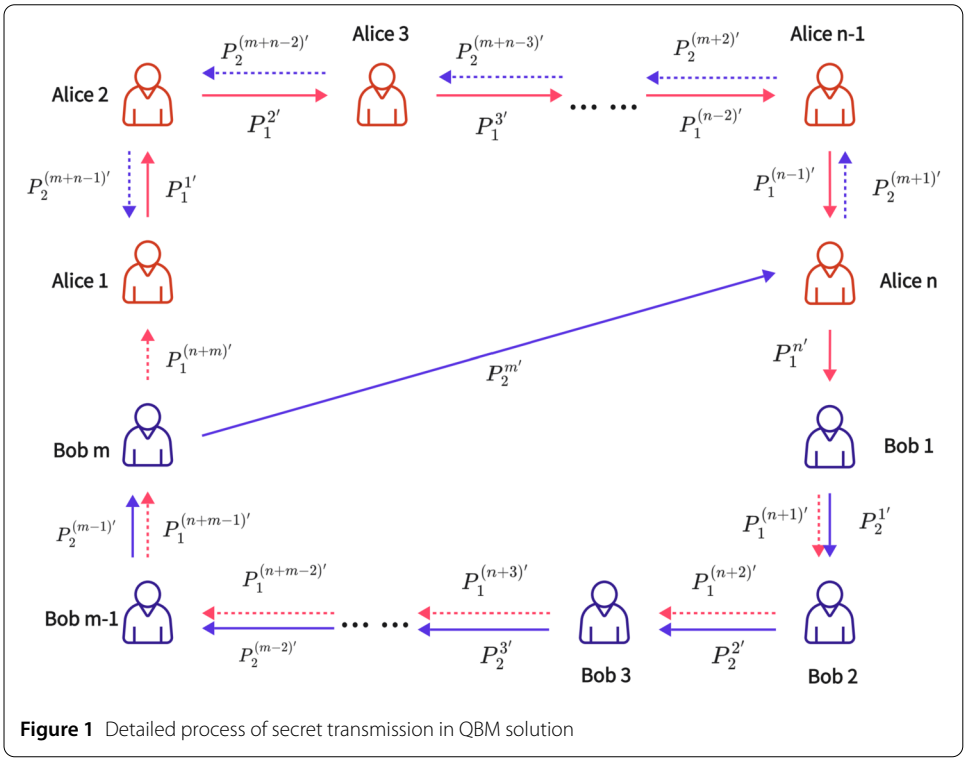

Figure 1 Detailed process of secret transmission in QBM solution

Algorithm 1 A blind millionaire's protocol without a third party

Require: $X_i = \{x_i(1), x_i(2), \ldots, x_i(l)\}$ and $Y_j = \{y_j(1), y_j(2), \ldots, y_j(l)\}$

for $i \leftarrow 1$ to $n+m$ **do**
  if $i \leq n$ **then**
    Shifting ${P_1}^{i-1} + X_i +$ **Rand** $R_i \rightarrow {P_1}^i$;
  else
    Shifting ${P_1}^{i-1} +$ **Rand** $R_{(i-n)'} \rightarrow {P_1}^i$;
  end if
  if $i \leq m$ **then**
    Shifting ${P_2}^{i-1} + Y_i +$ **Rand** $R_{i'} \rightarrow {P_2}^i$;
  else
    Shifting ${P_2}^{i-1} +$ **Rand** $R_{(n+m+1-i)} \rightarrow {P_2}^i$;
  end if
  $\left|P_1^{m+n}\right\rangle \rightarrow Alice_1$;
end for
Measurement $\left|P_1^{m+n}\right\rangle, \left|P_2^{m+n}\right\rangle \rightarrow A_k, B_k, (k = 1, 2, \ldots, l)$
$H = \sum_{t=1}^{l} 2^{l-t}(A_t - B_t)$;

Ensure: H.

indicates the route of operation performed by P_1 and the blue arrow indicates the route of operation performed by P_2 in this QBM scenario.

5 Correctness analysis

This section will examine whether Equation (12) may be used to compare the size connection between the sum of Set A and the sum of Set B to show that the proposed QBM solution is correct.

Proof According to Equation (12), it is possible to obtain

$$\begin{aligned} H &= \sum_{t=1}^{l} 2^{l-t}(A_t - B_t) \\ &= 2^{l-1}(A_1 - B_1) + 2^{l-2}(A_2 - B_2) + \cdots + 2(A_{l-1} - B_{l-1}) + (A_l - B_l) \end{aligned} \tag{13}$$

Substituting Equation (8) into Equation (11) and Equation (13), it will be

$$\begin{aligned} H &= 2^{l-1}\left[\sum_{i=1}^{n} x_i(1) - \sum_{i=1}^{m} y_i(1)\right] + 2^{l-2}\left[\sum_{i=1}^{n} x_i(2) - \sum_{i=1}^{m} y_i(2)\right] \\ &\quad + \cdots + 2\left[\sum_{i=1}^{n} x_i(l-1) - \sum_{i=1}^{m} y_i(l-1)\right] + \left[\sum_{i=1}^{n} x_i(l) - \sum_{i=1}^{m} y_i(l)\right] \\ &= \sum_{i=1}^{n}\left(\sum_{t=1}^{l} 2^{l-t} \sum_{j=1}^{l} x_i(j)\right) - \sum_{i=1}^{m}\left(\sum_{t=1}^{l} 2^{l-t} \sum_{j=1}^{l} y_i(j)\right) \end{aligned} \tag{14}$$

According to the encoding rules, there are

$$\begin{aligned} X_i &= \sum_{t=1}^{l} 2^{l-t} \sum_{k=1}^{l} x_i(k), i = 1, 2, \ldots, n, \\ Y_j &= \sum_{t=1}^{l} 2^{l-t} \sum_{k=1}^{l} y_j(k), j = 1, 2, \ldots, m. \end{aligned} \tag{15}$$

Substituting Equation (15) into Equation (14) yields

$$H = \sum_{i=1}^{n} X_i - \sum_{i=1}^{m} Y_i \tag{16}$$

In summary, Equation (12) can be used to determine the size of the secret sum of set A and set B. □

To facilitate understanding, we illustrate the correctness of the QBM solution with a simple example. The Set A has three participants $\text{Alice}_i (i = 1, 2, 3)$, whose secrets are 0111, 1010, 0110 after they convert it into binary. The Set B has two participants $\text{Bob}_j (j = 1, 2)$, they have secrets 1100, 1001. Alice_1 prepares four copies of d-level 2-particles. Alice_1 generated an entangled state $|\chi_2\rangle$ and the first particle form sequence $P_1 = \{p_{11}, p_{12}, p_{13}, p_{14}\}$, the second particle form sequence $P_2 = \{p_{21}, p_{22}, p_{23}, p_{24}\}$. He sends the sequence P_2 to Bob_1, and performs the shift operation on the sequence P_1. Alice_1 generates the random number $r_1 = \{1, 1, 0, 1\}$ and performs the shift operation to encode x_1 and r_1 into the particle sequence P_1. Thus, he will get the sequence $P_1^1 = \{h_1 \oplus 0 \oplus 1, \ldots, h_4 \oplus 1 \oplus 1\}$. Bob_1 performs the same operations as Alice_1, obtaining the sequences P_2^1. The random numbers of participants in sets A and B are shown in Fig. 2.

Alice_1 and Bob_1 insert test particles into P_1^1, P_2^1 and obtain the sequences $P_1^{1'}$, $P_2^{1'}$. Then Alice_1 sends the sequence $P_1^{1'}$ to Alice_2, and Bob_1 sends the sequence $P_2^{1'}$ to Bob_2.

After discarding the test particles, Alice_2 and Bob_2 perform similar operations as Alice_1 and Bob_1 and send the sequences to the next participants. Therefore, Alice_n and Bob_m obtain the sequences P_1^n, P_2^m. Then Alice_n sends the sequence $P_1^{n'}$ to Bob_1, here the random numbers are encoded in the sequence. The participant in Set B performs the similar operation as Bob_1, which is finally sent back to Alice_1 by Bob_n. Similarly, Alice_n encodes his random number in the sequence, the other participants perform similar operations, and Alice_2 sends the final sequence to Alice_1.

Alice_1 obtains the sequences P_1^{n+m} and P_2^{n+m}, then Alice_1 measures the received particle sequences and publishes the measurement results as Table 1 and Table 2. Therefore, the

Figure 2 The random numbers of participants

$$r_i, r_j = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

Table 1 The summation of the participants' random numbers and the participants' secret summation in Set A

State	P_1	A_t
$\|\chi_2\rangle_1$	$h_1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0$	$h_1 \oplus 3$
$\|\chi_2\rangle_2$	$h_2 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1$	$h_2 \oplus 6$
$\|\chi_2\rangle_3$	$h_3 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 0$	$h_3 \oplus 6$
$\|\chi_2\rangle_4$	$h_4 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0$	$h_4 \oplus 3$

Table 2 The summation of the participants' random numbers and the participants' secret summation in Set B

State	P_2	B_t
$\|\chi_2\rangle_1$	$h_1 \oplus 1 \oplus 1 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0$	$h_1 \oplus 4$
$\|\chi_2\rangle_2$	$h_2 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \oplus 1 \oplus 1 \oplus 0$	$h_2 \oplus 5$
$\|\chi_2\rangle_3$	$h_3 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1$	$h_3 \oplus 3$
$\|\chi_2\rangle_4$	$h_4 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 1 \oplus 0 \oplus 1$	$h_4 \oplus 3$

result of the calculation H is as follows.

$$\begin{aligned} H &= 2^3(A_1 - B_1) + 2^2(A_2 - B_2) + 2^1(A_3 - B_3) + 2^0(A_4 - B_4) \\ &= 8 \times (-1) + 4 \times 1 + 2 \times 3 + 1 \times 0 \\ &= 2 \end{aligned} \tag{17}$$

The secret summation of the participants in Set A is greater than the secret summation of the participants in Set B, as shown from $H > 0$.

6 Security analysis

According to the steps above, it is clear that the actions of the participants in Set A and Set B are absolutely identical. Thus, we take the example of the participants in Set A to analyze the security of the solution to the QBM problem. In this section, we will analyze the security of the solution against both internal and external threats.

6.1 The internal attack

In most cryptography protocols, the security loopholes caused by malicious participants may be more serious. As some necessary actions are performed in the protocol, they have more chances to intercept the transmitted sequences to obtain the secrets of other participants. In this section, we discuss internal attacks from both independent and collusive aspects.

(1) Participant-independent attack

a. When a participant performs an independent attack, it is assumed that the participant Alice_k wants to get the secret of the participant Alice_{k-1} without being detected. Therefore, after Alice_{k-1} and Alice_k perform eavesdropping detection, Alice_k will obtain the particle sequence P_1^{k-1}. He can directly perform single-particle measurements on the sequence. In Step 1, it can be seen that the sequences P_1^{k-1} and P_2^{k-1} are entangled with each other. When Alice_k performs a single-particle measurement in the sequence, the result is seen as

$$C_1 = \sum_{i=1}^{k-1}(x_i(1) \oplus r_{i1}) \oplus h_1, \tag{18}$$

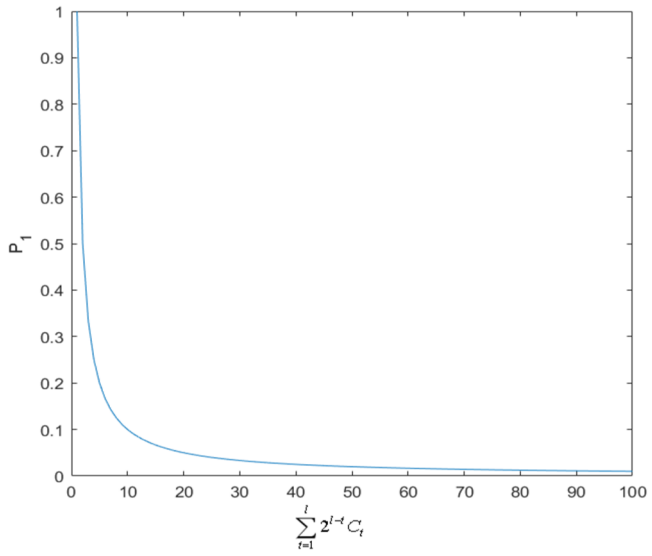

Figure 3 Trends in the probability of Alice$_k$ obtains the secret of Alice$_{k-1}$

$$\vdots$$

$$C_l = \sum_{i=1}^{k-1} (x_i(l) \oplus r_{il}) \oplus h_l, \tag{19}$$

Since the participant encoded his secret into a binary sequence in Step 2, for participant Alice$_k$ to obtain participant Alice$_{k-1}$'s secret, the probability that participant Alice$_k$ obtains the secret of participant Alice$_{k-1}$ is

$$P_1 = \frac{1}{\sum_{t=1}^{l} 2^{l-t} C_t}. \tag{20}$$

It can be seen that the probability tends to 0 (see Fig. 3), so he cannot get Alice$_{k-1}$'s secret.

b. When Bob$_j$, a participant in Set B, intercepts the sequence $P_1^{i'}$ sent by Alice$_i$ to Alice$_{i+1}$. As he does not know the location of the test particles despite the fact that he can measure the sequence with Fourier basis, the probability of getting Alice$_i$' secret is

$$P_e = 1 - \frac{1}{d^{\delta}} \tag{21}$$

It can be seen that the probability tends to be 1 (see Fig. 4), so he will definitely be found.

c. Specifically, it is assumed that Alice$_1$ wants to obtain the secret of Alice$_2$. Since Alice$_1$ generated the initial quantum states, after Alice$_2$ performs the shifting operation, Alice$_1$ intercepts the particle sequence that Alice$_2$ sends to Alice$_3$. However, this sequence contains δ decoy particles, which means the probability of Alice$_1$ being detected is very high, approaching 1. Furthermore, Alice$_1$ does not know the random numbers chosen by Alice$_2$, so he will not be able to obtain Alice$_2$'s secret.

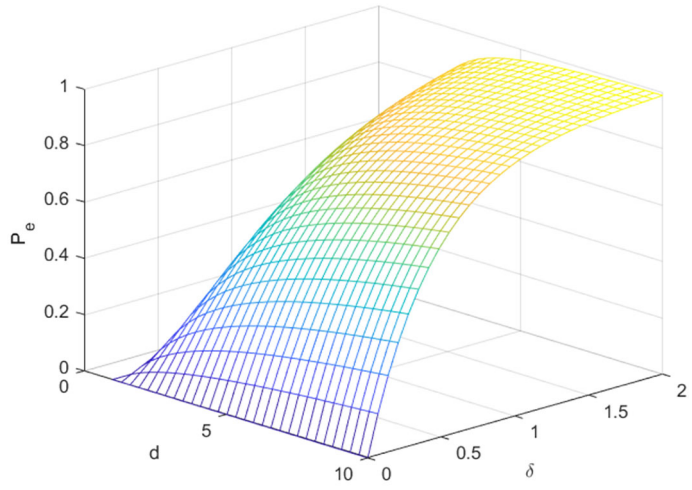

Figure 4 Trends in the probability of Alice$_{i+1}$ being detected

(2) Conspiracy to attack by the same set of participants

In a practical situation, it is inevitable that more than one malicious participant will appear to perform some special attack. We assume that the participants Alice$_k$, ..., Alice$_q$($k < q$) in Set A are dishonest. They conspire to obtain the secret of Alice$_h$. Depending on the order in which participants encode their secrets, the collusion attack can be categorized into three scenarios.

a. $h < k$: this means that the particle sequence encoded by Alice$_h$ will eventually pass to Alice$_k$. After detecting eavesdropping, Alice$_k$ obtains the particle sequence P_1^{k-1}. Therefore, after performing a single particle measurement on the received sequence, the probability that these malicious participants obtain Alice$_h$'s secret is P_1.

b. $h > q$: this means that the participants Alice$_k$, ..., Alice$_q$($k < q$) need to intercept the sequence $P_1^{h'}$ from Alice$_h$ to Alice$_{h+1}$. Since the participant Alice$_{h+1}$ is honest, a malicious participant that intercepts the particles cannot detect eavesdropping with Alice$_h$. Obviously, the malicious participant cannot distinguish between the particle encoding the secret and the test particles, so the malicious participant cannot obtain useful messages about Alice$_h$' secret. If the malicious participant does not send any particles to Alice$_{h+1}$, Alice$_{h+1}$ will realize the presence of the attacker and notify Alice$_h$ to terminate the protocol and restart from Step 1. If the malicious participant prepares a large number of particles and sends them to Alice$_{h+1}$, the attacker will inform Alice$_h$ and terminate the protocol. The probability that the malicious participant will be detected when Alice$_h$ and Alice$_{h+1}$ are eavesdropping is P_e converges to 1. In summary, it can be seen that if malicious participants intercept the secret sequence of Alice$_h$, they will definitely be detected and cannot obtain the secret sequence of Alice$_h$.

c. $k < h < q$: this means that the participant Alice$_h$ encodes the secret in a sequence between the malicious participants, but he is not malicious. In this case, the malicious participant Alice$_{h-1}$ will get the sequence $P_1^{(h-1)'}$. After Alice$_h$ encodes the secret, he will send the secret sequence to malicious participants. After Alice$_h$ and Alice$_{h+1}$ have detected eavesdropping, the malicious participant Alice$_{h+1}$ will receive the sequence $P_1^{h'}$. Here, malicious participants can perform single-particle measurements on the sequences $P_1^{h-1} \oplus P_1^h$, the

result is

$$D_1 = x_h(1) \oplus r_{h1}, \tag{22}$$

$$\vdots$$

$$D_l = x_h(l) \oplus r_{hl}, \tag{23}$$

Therefore, the probability that malicious participants $\text{Alice}_k, \ldots, \text{Alice}_q$ obtains the secret of participant Alice_h is

$$P_2 = \frac{1}{\sum_{t=1}^{l} 2^{l-t} D_t}. \tag{24}$$

d. Specifically, it is assumed that Alice_1 colludes with other participants in Set A to obtain the secret of Alice_2. When Alice_1 measures the final sequence P_1^{m+n}, the sequence includes random numbers $\sum_{j=1}^{m} r_{jt'}$ from participants in Set B and random numbers r_{2t} from Alice_2, which Alice_1 does not know. Therefore, even with collusion among the participants in Set A, they cannot obtain Alice_2's secret.

(3) Conspiracy to attack different sets of participants

In order to obtain Alice_1's secret, Alice_2, a participant in Set A, wants to conspire with Bob_1, a participant in Set B. When Alice_2 detects the eavesdropping with Alice_1, Alice_1 will obtain the sequence P_1^1 and measure it, and obtain the measurement result $h1 \oplus r1 \oplus x1$. At the same time, Bob_1 measures the particles P_2^1 in his hand on the Fourier basis, so Bob_1 will get the measurement result h_1. At this point, the probability that they will get Alice_1's secret is $P_2(h = 1)$. This is the maximum probability of getting the participant's secret.

6.2 The external attack

Assuming that Eve is the external attacker, he seeks to obtain the secret of $\text{Alice}_i (i = 1, \ldots, n)$. To get Alice_i's secret, Eve needs to intercept the particle sequence $P_1^{i'}$ transmitted from Alice_i to Alice_{i+1} in Step 5. Obviously, the sequence of intercepted particles includes the secrets, the random numbers of the first i participants, and the test particles. When Eve wants to get the secret of Alice_i from the intercepted particle sequence $P_1^{i'}$, he needs to measure it. The sequence $P_1^{i'}$ can be measured in two ways to obtain useful information about the secret.

(1) Intercept-measure-resend attack: To avoid being detected, Eve may prepare a large number of d-level 2-particle entanglement states $|\chi_2\rangle$ as forged particles to be sent to Alice_{i+1}. When Eve performs single-particle measurements on the particles, he cannot distinguish between the encoded secret particle and the test particle. As a result, he will undoubtedly be discovered and will be unable to get any valuable information regarding the secret. After Alice_{i+1} receives the particle sequence, he first conducts a detection eavesdropping with Alice_i. Since $P_1^{i'}$ contains the test particles, the probability of Eve's detection is P_e.

(2) Entangle–measure attack: After intercepting the particles, the external attacker Eve uses the operation U_E to entangle the intercepted quantum state with the constructed

auxiliary state that contains the quantum system. Thus, it can be seen as

$$U_E|j\rangle|e\rangle = \sum_{k=0}^{d-1} a_{jk}|k\rangle|e_{jk}\rangle \tag{25}$$

where $|j\rangle \in \{0,\ldots,d-1\}$ and $\sum_{k=0}^{d-1}|a_{jk}|^2 = 1$.

When it is measured using a computational basis, in order to avoid introducing any inaccuracies and pass eavesdropping detection, the equation

$$a_{jk} = \begin{cases} 0, j \neq k \\ 1, j = k \end{cases} \tag{26}$$

needs to satisfy Equation (25).

When it is measured using the Fourier basis, the equation is

$$\begin{aligned} U_E|f_j\rangle|e\rangle &= U_E(\sum_{i=0}^{d-1} a^{ji}|i\rangle)|e\rangle \\ &= \sum_{i=0}^{d-1} a^{ji} U_E|i\rangle|e\rangle \\ &= \sum_{i=0}^{d-1} a^{ji} \sum_{r=0}^{d-1} \omega_{ir}|r\rangle|e_{ir}\rangle \\ &= \sum_{i=0}^{d-1}\sum_{r=0}^{d-1} a^{ji}\omega_{ir}|r\rangle|e_{ir}\rangle \\ &= \sum_{i=0}^{d-1} a^{ji} \sum_{l=0}^{d-1} a^{-il}|f_l\rangle|e_{ii}\rangle \\ &= \sum_{i=0}^{d-1}\sum_{l=0}^{d-1} a^{ji-il}|f_l\rangle|e_{ii}\rangle \end{aligned} \tag{27}$$

which leads to

$$|e_{00}\rangle = |e_{11}\rangle = \cdots = |e_{d-1,d-1}\rangle \tag{28}$$

As a result, Eve cannot get the secrets of the participants. It demonstrates that the proposed method is immune to entanglement measurement attack strategies.

7 Comparison and discussion

The quantum blind millionaire problem is a novel research topic. In this section, we compare the existing QBM protocols with our proposed protocol in terms of quantum resources, quantum operations, qubit efficiency, number of participants, and third-party involvement, as shown in Table 3.

The qubit efficiency of secure quantum communication was defined as

$$\eta = \frac{c}{q+b} \tag{29}$$

Table 3 Comparison of quantum blind millionaires' protocol in Ref. [10, 11] and the proposed protocol

	Ref [18]	Ref [19]	Ours
Quantum resource	d-level 2-particle entangled states	d-level Bell states and d-level single-photon state	d-level 2-particle entangled states
Quantum operations	shift operation	shift operation	shift operation
Third-party involvement	Yes	Yes	No
Qubit efficiency	$\frac{1}{2n+10}$	$\frac{1}{4n+10}$	$\frac{1}{4n+2}$
Number of participants	$2n$	$n+m$	$n+m$

where c denotes the total number of the classical message bits, q represents the number of the used qubits and b denotes the number of classical bits exchanged for decoding the message. For simplicity, we assume that each set has n participants, and the number of decoy particles used to check eavesdropping is equal to the secret length, both of which are l.

From Table 3, we can conclude the following: Ref [18] and Ref [19] both require the participation of a third party (TP). TP is assumed to be a semi-honest who may perform an attack but cannot conspire with any party. However, the involvement of TP may compromise the security of the protocols. Therefore, we further extend the QBM protocol to scenarios without a third party, allowing for the secure comparison of the sums of secrets between participants in two sets without the need for a third party. With this improvement, our protocol can exhibit higher security, making our protocol suitable for a wider range of practical applications.

8 Conclusion

In this paper, a novel non-third-party solution is provided to the quantum blind millionaires' problem, which encodes the participant's secret into d-dimensional 2-particle entangled states using the shift operations. In our solution, a simple encoding method is used to encode two sets of secrets to the entangled state of two particles in d dimensional. Furthermore, the correctness of the solution is illustrated. The security analysis shows that the solution is secure against both external and internal attacks, even if most of the participants are malicious. As a first solution to QBM problem, we hope that the work will lead to positive developments in quantum-secure multiparty computation in future.

Abbreviations

QBM, Quantum Blind Millionaires; QSMC, Quantum Secure Multiparty Computation; SMC, Secure Multiparty Computation; BM, Blind Millionaires.

Author contributions

Gang Du, Hong-Wei Sun, and Lei Wang wrote the main manuscript text, Yu Zhang and Xin-Yue Mao prepared all the figures. All authors reviewed the manuscript.

Funding

This work was supported by the National Natural Science Foundation of China under Grant 62271234, the Fundamental Research Funds for Heilongjiang Universities under Grant No. 2022-KYYWF-1123 and 2022-KYYWF-1042, Open Foundation of State Key Laboratory of Public Big Data (Guizhou University) under Grant No. PBD2022-16, Double First-Class Project for Collaborative Innovation Achievements in Disciplines Construction in Heilongjiang Province under Grant No. LJGXCG2022-054 and LJGXCG2023-028, and Advanced Programs of Heilongjiang Province for the overseas scholars.

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 Data Science and Technology, Heilongjiang University, Harbin, 150080, China. [2]State Key Laboratory of Public Big Data, Guizhou University, Guiyang, 550000, China. [3]Institute for Cryptology and Network Security, Heilongjiang University, Harbin, 150080, China. [4]School of Mathematical Science, Heilongjiang University, Harbin, 150080, China.

Received: 2 May 2024 Accepted: 6 November 2024 Published online: 25 November 2024

References

1. Yao AC. Protocols for secure computations. In: 23rd annual symposium on foundations of computer science (sfcs 1982). 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. Ioannidis I, Grama A. An efficient protocol for yao's millionaires' problem. In: 36th annual Hawaii international conference on system sciences. Proceedings of the. vol. 2003. IEEE; 2003. p. 6.
4. Lin H-Y, Tzeng W-G. An efficient solution to the millionaires' problem based on homomorphic encryption. In: Applied cryptography and network security: third international conference, ACNS 2005, New York, NY, USA, June 7-10, 2005. Proceedings. vol. 3. Springer; 2005. p. 456–66.
5. Shundong L, Daoshun W, Yiqi D, Ping L. Symmetric cryptographic solution to yao's millionaires' problem and an evaluation of secure multiparty computations. Inf Sci. 2008;178(1):244–55.
6. Jia H-Y, Wen Q-Y, Song T-T, Gao F. Quantum protocol for millionaire problem. Opt Commun. 2011;284(1):545–9.
7. Li S, Guo Y, Zhou S, Dou J, Wang D. Efficient protocols for the general millionaires' problem. Chin J Electron. 2017;26(4):696–702.
8. Liu X, Li S, Chen X, Xu G, Zhang X, Zhou Y, et al. Efficient solutions to two-party and multiparty millionaires' problem. Secur Commun Netw. 2017;2017:5207386.
9. Nakai T, Misawa Y, Tokushige Y, Iwamoto M, Ohta K. How to solve millionaires' problem with two kinds of cards. New Gener Comput. 2021;39:73–96.
10. Zhang Y, Zhang L, Zhang K, Wang W, Hou K. A new quantum-inspired solution to blind millionaires' problem. Quantum Inf Process. 2023;22(1):80.
11. Yao Y, Zhang K-J, Song T-T, Zhang L, Wang S-N. The complete new solutions to the blind millionaires' problem in d-dimensional quantum system. Phys A, Stat Mech Appl. 2023;627:129138.
12. Yang Y-G, Wen Q-Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A, Math Theor. 2009;42(5):055305.
13. Zhang W-W, Li D, Zhang K-J, Zuo H-J. A quantum protocol for millionaire problem with bell states. Quantum Inf Process. 2013;12:2241–9.
14. He GP. Simple quantum protocols for the millionaire problem with a semi-honest third party. Int J Quantum Inf. 2013;11(02):1350025.
15. Ye T-Y. Multi-party quantum private comparison protocol based on entanglement swapping of bell entangled states. Commun Theor Phys. 2016;66(3):280.
16. Zhao-Xu J, Tian-Yu Y. Multi-party quantum private comparison based on the entanglement swapping of d-level cat states and d-level bell states. Quantum Inf Process. 2017;16:1–20.
17. Ji Z-X, Ye T-Y. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun Theor Phys. 2016;65(6):711.
18. Li S, Guo Y, Zhou S, Dou J, Wang D. Efficient protocols for the general millionaires' problem. Chin J Electron. 2017;26(4):696–702.
19. Ye T-Y. Quantum private comparison via cavity qed. Commun Theor Phys. 2017;67(2):147.
20. Ye T, Ji Z. Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci China, Phys Mech Astron. 2017;60:1–10.
21. Chong-Qiang Y, Tian-Yu Y. Circular multi-party quantum private comparison with n-level single-particle states. Int J Theor Math Phys. 2019;58:1282–94.
22. Geng M-J, Chen Y, Xu T-J, Ye T-Y. Single-state semiquantum private comparison based on bell states. EPJ Quantum Technol. 2022;9(1):36.
23. Lian J-Y, Li X, Ye T-Y. Multi-party semiquantum private comparison of size relationship with d-dimensional bell states. EPJ Quantum Technol. 2023;10(1):10.
24. Lian J-Y, Ye T-Y. Hybrid protocols for multi-party semiquantum private comparison, multiplication and summation without a pre-shared key based on d-dimensional single-particle states. EPJ Quantum Technol. 2024;11(1):17.
25. Wang Y, Hu P, Xu Q. Quantum secure multi-party summation based on entanglement swapping. Quantum Inf Process. 2021;20:1–13.
26. Zhang C, Long Y, Li Q. Quantum summation using d-level entanglement swapping. Quantum Inf Process. 2021;20(4):137.
27. Ye T-Y, Xu T-J. A lightweight three-user secure quantum summation protocol without a third party based on single-particle states. Quantum Inf Process. 2022;21(9):309.

28. Ming-Yi D. Multi-party quantum summation within a d-level quantum system. Int J Theor Math Phys. 2020;59(5):1638–43.
29. Ye T-Y, Hu J-L. Quantum secure multiparty summation based on the phase shifting operation of d-level quantum system and its application. Int J Theor Math Phys. 2021;60(3):819–27.
30. Li S, Zhang M. An efficient solution to the blind millionaires problem. Chinese J Comput. 2020;43:1755–68.

Publisher's Note