Multi-party quantum privacy comparison of size based on $d$-level GHZ states

Hao Cao¹,² · Wenping Ma¹ · Liangdong Lü¹,³ · Yefeng He⁴ · Ge Liu¹

Received: 20 September 2018 / Accepted: 31 July 2019 / Published online: 8 August 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2019

Abstract
Quantum privacy comparison (QPC) plays an important role in secret ballot elections, private auctions and so on. To date, many multi-party QPC (MQPC) protocols have been proposed to compare the equality of $k$ ($k \geq 3$) participants. However, few examples of MQPC can be used to compare the sizes or values of their privacies. In this paper, we propose a MQPC protocol by which any $k$ ($k \geq 3$) participants can compare the sizes of their privacies with executing the protocol just once. The proposed MQPC protocol takes the $d$-level GHZ states as quantum resources, and a semi-honest TP is introduced to help the participants to determine the relationship of their privacies. Furthermore, only single-particle unitary transformations and measurements are involved, and the participants need not to share a private key beforehand which makes the proposed protocol much more efficient. Analysis shows that our protocol is secure against internal and external attack in theory.

Keywords Quantum cryptography · Multi-party quantum privacy comparison (MQPC) · Quantum Fourier transform (QFT) · Third party (TP) · GHZ state

Hao Cao caohao2000854@163.com
Wenping Ma wp_ma@mail.xidian.edu.cn
Liangdong Lü kelinglv@163.com

¹ State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an 710071, China
² School of Information and Network Engineering, Anhui Science and Technology University, Chuzhou 233100, China
³ Department of Basic Sciences, Air Force Engineering University, Xi’an 710071, China
⁴ School of Telecommunications and Information Engineering, Xi’an University of Posts and Telecommunications, Xi’an 710121, China
1 Introduction

Privacy comparison originates from the concept of millionaire problem introduced by Yao which can be described as follows: Two millionaires want to know who is richer without divulging any information about their wealth, and a novel solution for the problem was proposed by him [1]. Later, many solutions [2,3] have been proposed, and the millionaire problem, especially privacy comparison, became an important topic in classical cryptography. On the other hand, with the revolutionary application, known as BB84, of the quantum mechanics in the cryptography [4], quantum cryptography attracts much more attention from all over the world, and many kinds of cryptography protocols such as quantum key distribution (QKD) [5,6], quantum secret sharing (QSS) [7–9], quantum direct communication (QDC) [10], and quantum key agreement (QKA) [11] have been proposed. As an important topic, privacy comparison in the quantum circumstances, i.e., quantum privacy comparison (QPC), has attracted wide attention from many cryptographers.

In 2009, the first two-party QPC protocol for comparing information of equality based on bell states and hash function was proposed by Yang and Wen [12]. Thereafter, several two-party QPC protocols [13–15] based on entangled quantum resources, such as GHZ states and \( \chi \)-type states, were proposed. However, only two parties were involved in the above protocols. Until 2013, the first multi-party QPC (MQPC) was proposed by Chang et al. [16]. Since then, various two-party [17–21] and multi-party [22–25] structures were proposed. However, the aforementioned protocols are only suitable for comparing the equality of information. When it comes to size comparison, these protocols are powerless.

Fortunately, in 2011, Jia et al. presented the first two-party QPC protocol for comparing the sizes of privacies based on \( d \)-level three-particle GHZ states [26], in which the information of sizes was encoded into the phase of GHZ states. Later, in 2013, three two-party QPC protocols [27–29] for comparing the information of sizes based on \( d \)-level bell states were proposed. In the same year, Yu et al. [30] proposed another one based on \( d \)-level single particles. However, the five QPC protocols mentioned above are only related to the comparison of the size of two parties. Until 2014, the first protocol of size comparison in multi-party circumstance [31] was proposed by Luo et al. However, the participants needed to share a private key \( K \) beforehand by using QKA protocol which will waste a lot of quantum resources. Besides, each participant and TP need to establish an authenticated classical channel beforehand. Later, Huang et al [32] proposed another MQPC protocol based on GHZ states, which can also be used to compare the sizes of all privacies. However, we found that there exists a serious security flaw in the protocol after close analysis, i.e., an internal participant can get the privacy of any other participant without being found.

In this paper, we will propose a novel MQPC protocol by which any \( k (k \geq 3) \) participants can compare the sizes of their privacies with executing the protocol just once. In this protocol, a semi-honest third party (TP) [31] is introduced to help the participants to compare the sizes of their information. The semi-honest TP means that the TP will always execute the protocol honestly, record the information of the participants, and try to extract their privacies from the records, but he will not conspire with any participant or outside eavesdropper. First, TP prepares some \( d \)-level \( k \)-particle
GHZ states and distributes them to every participant. Second, each participant encodes them with unitary operations based on a random sequence, and sends them back to TP. Next, each participant encrypts his size by the random sequence and sends it to TP. At last, TP measures the GHZ states on the Z-basis separately, compares them with the encrypted size, and obtains the results of comparison. The proposed MQPC protocol can ensure that

(1) correctness: all participants can get the size relationship of their privacy correctly with the help of TP if they execute the protocol honestly.

(2) security: the semi-honest party TP cannot get any information about the privacies of participants except the size relationship. Besides, each participant cannot deduce privacy of others from the comparison result.

The structure of our paper is as follows. Section 2 is devoted to the details and correctness of our proposed protocol, and a novel example is presented. Section 3 analyzes the proposed protocol and compares it to the existed protocols, and a brief conclusion is given in Sect. 4.

2 Results

Before going further, firstly we recall some definitions and quantum resources which will be used in the description of our protocol.

2.1 Preparation for the protocol

The quantum resource used in our protocol is the $d$-level $k$-particle GHZ state which can be represented as

$$|\Phi\rangle = \frac{1}{\sqrt{d}} \left( |0\rangle |0\rangle \cdots |0\rangle + |1\rangle |1\rangle \cdots |1\rangle + \cdots + |d-1\rangle |d-1\rangle \cdots |d-1\rangle \right)$$  \hspace{1cm} (1)

For a $d$-level quantum system, there are two indistinguishable orthogonal bases, Z-basis and X-basis:

$$Z = \{|0\rangle, |1\rangle, |2\rangle, \ldots, |d-1\rangle\}$$

$$X = \{\text{QFT}|0\rangle, \text{QFT}|1\rangle, \text{QFT}|2\rangle, \ldots, \text{QFT}|d-1\rangle\}$$  \hspace{1cm} (2)

where QFT : $|z\rangle \rightarrow \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} \exp \left( \frac{2\pi i x z}{d} \right) |x\rangle$ is the quantum Fourier transform (QFT). Let us introduce an unitary operation (we call it shift operator) as follows:

$$U_r = \sum_{t=0}^{d-1} \exp \left( \frac{2\pi i t (t \oplus r)}{d} \right) |t \oplus r\rangle \langle t|$$  \hspace{1cm} (3)
Hereafter, the symbols $\oplus$ and $\ominus$ denote modular $d$ addition and subtraction. It is easy to verify that the shift operator is an one-to-one map from Z-basis to itself and X-basis to itself, i.e.,

$$U_r(|s\rangle) = |s \oplus r\rangle$$

$$U_r($$ QFT$|s\rangle) = \text{QFT}|s \oplus r\rangle \quad (s = 0, 1, 2, \ldots, d - 1) \quad (4)$$

### 2.2 The MQPC protocol for comparing the sizes of information

Let TP be a semi-honest party and $P_0, P_1, P_2, \ldots, P_{k-1}$ be $k$ participants. Each participant $P_i(i \in \{0, 1, 2, \ldots, k - 1\})$ possesses a $m$-length privacy $p_i = (p_{i,1}, p_{i,2}, \ldots, p_{i,m}) \in \{0, 1, \ldots, l\}^m$ (here $d = 2l + 1$). They want to compare the size of $p_{0,j}, p_{1,j}, \ldots, p_{k-1,j}(j = 1, 2, \ldots, m)$ without revealing any information. Through executing the following protocol, they could achieve their goals with the help of TP. The detailed description of our MQPC protocol can be seen as follows:

**Step 1 Preparation** TP prepares $m$ identical $d$-level $k$-particle GHZ states in the form of Eq. (1), and splits them into $k$ particle sequences: $S_0, S_1, \ldots, S_{k-1}$. The $i$-th sequence $S_i(i = 0, 1, \ldots, k - 1)$ consists of the $i$-th particles of these GHZ states. Next, he will get a series of new sequence $S'_0, S'_1, \ldots, S'_{k-1}$ by inserting $m$ decoy particles which are selected from X-basis or Z-basis [see Eq. (2)] randomly into each sequence $S_i$, and sends the resulted sequence $S'_i(i = 0, 1, \ldots, k - 1)$ to the $i$-th participant $P_i$.

**Step 2 Eavesdropping Checking** After confirming that each participant $P_i$ has received the sequence $S'_i$, TP publishes the position and measurement basis (X-basis or Z-basis) of each decoy particle in $S'_i$. $P_i$ and TP execute eavesdropping checking similar to BB84. If the safety of the channel is not acceptable, the protocol goes to Step 1. Otherwise, the protocol will continue. After successfully passing the eavesdropping checking, each participant $P_i$ will recover the sequence $S_i$ by deleting the decoy particles from $S'_i$.

**Step 3 Encoding** Each participant $P_i$ selects a $m -$ length random sequence $r_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,m}) \in \{0, 1, \ldots, d - 1\}^m$, and performs the shift operator $U_{r,j}(j = 1, 2, \ldots, m)$ in the form of Eq. (3) to the $j$-th particle of the sequence $S_i$. Then, he sends the resulted sequence $S_{i}'$ together with $k$ decoy particles (similar to Step 1) to TP.

**Step 4 Measurement** Having received the sequence from every participant $P_i$, TP will execute eavesdropping checking with every $P_i$ separately similar to Step 2. After successfully passing the eavesdropping checking, TP will extract $S_{i}'$ by deleting the decoy particles. Next, he measures each particle in $S_{i}'$ on the Z-basis and denotes the measurement result as $|w_{i} \rangle = |w_{i,1} \rangle |w_{i,2} \rangle \cdots |w_{i,m} \rangle$.

**Step 5 Transmitting privacy** Each participant $P_i$ encrypts his privacy $p_i = (p_{i,1}, p_{i,2}, \ldots, p_{i,m})$ into $\overline{p_i} = (\overline{p_{i,1}}, \overline{p_{i,2}}, \ldots, \overline{p_{i,m}}) = (p_{i,1} \ominus r_{i,1}, p_{i,2} \ominus r_{i,2}, \ldots, p_{i,m} \ominus r_{i,m})$, and sends it to TP through an authenticated channel.
Step 6 Comparison Having received $\overline{p}_i$ from every participant $P_i$, TP calculates:

$$t_i = (t_{i,1}, t_{i,2}, \ldots, t_{i,m}) = (\overline{p}_i \oplus w_{i,1}, \overline{p}_i \oplus w_{i,2}, \ldots, \overline{p}_i \oplus w_{i,m})$$

$$t(i, i) = (t_{i,1} \oplus t_{i,1}, t_{i,2} \oplus t_{i,2}, \ldots, t_{i,m} \oplus t_{i,m})$$

$$s(i, i) = (s(i, i)_1, s(i, i)_2, \cdots, s(i, i)_m)$$

$$= (\text{Sign}[t_{i,1} \oplus t_{i,1}], \text{Sign}[t_{i,2} \oplus t_{i,2}], \ldots, \text{Sign}[t_{i,m} \oplus t_{i,m}])$$

where $i, i' \in \{0, 1, \ldots, k - 1\}, i < i', i < j$, and $\text{Sign}[.]$ is the signal function which is defined by:

$$\text{Sign}[x] = \begin{cases} 
1 & x \in \{1, 2, \ldots, l\} \\
0 & x = 0 \\
-1 & x \in \{l + 1, l + 2, \ldots, 2l\}
\end{cases}$$

For the $j$th ($j = 1, 2, \ldots, m$) elements of all participants’ privacies $p_{0,j}, p_{1,j}, \ldots, p_{k-1,j}$, TP can deduce the size relationship of them from the values of $s(i, i')(i, i' = 0, 1, \ldots, k - 1)$. The rules of judgment are as follows:

If $s(i, i')_j = 1$, then $p_{i,j} > p_{i',j}$;

If $s(i, i')_j = 0$, then $p_{i,j} = p_{i',j}$;

If $s(i, i')_j = -1$, then $p_{i,j} < p_{i',j}$.

Next, TP arranges the elements $p_{0,j}, p_{1,j}, \ldots, p_{k-1,j}$ in ascending order together with a relationship symbol $<$ or $=$ between every two elements, and gets a relation expression $p_{0,j}^l < p_{1,j}^l < \cdots < p_{k-1,j}^l$, where $i_0^l, i_1^l, \ldots, i_{k-1}^l$ is a permutation of $0, 1, \ldots, k - 1$, and $<$ denotes the symbol $<$ or $=$.

At last, for each $j \in \{1, 2, \ldots, m\}$, TP publishes the information $R_j \triangleq i_0^l < i_1^l < \cdots < i_{k-1}^l$, which consists of subscripts information of the relation expression. So far, all participants can get the comparison results from $R_j(j \in \{1, 2, \ldots, m\})$.

2.3 Correctness of the protocol

For the convenience of description, the phase of eavesdropping checking in Step 2 is not considered. Next, we will show that our protocol can work efficiently if all participants and TP execute the protocol honestly. Consider the $j$th elements $p_{0,j}, p_{1,j}, \ldots, p_{k-1,j}(j = 1, 2, \ldots, m)$ of all participants.

(a) TP prepares a sequence of $d$-level $k$-particle GHZ states:

$$|\Phi\rangle_{0,1,\ldots,k-1} = \frac{1}{\sqrt{d}} (|0\rangle|0\rangle \cdots |0\rangle + |1\rangle|1\rangle \cdots |1\rangle + \cdots + |d-1\rangle|d-1\rangle \cdots |d-1\rangle)_{0,1,\ldots,k-1}$$

He splits it into $k$ single particle sequence $S_0, S_1, \ldots, S_{k-1}$ and sends the $i$th sequence $S_i$ to $P_i$. 

\[ Springer \]
Then, TP will get

\[ \Phi \] 

Each participant \( \Pi_j \) (c) In the Step 4, the final state of the privileges are encoded into \( \Theta_p \) to TP.

\[ \Sigma_{i=0}^{l} \left( \frac{\tan \rho_i}{\rho_i} \right) \]

\[ \left[ (\Pi_{i,j} \oplus r_{i,j}) \oplus (c_j \oplus r_{i,j}) \right] \oplus \left[ (\Pi_{i,j} \oplus r_{i,j}) \oplus (c_j \oplus r_{i,j}) \right] \]

Then, TP will get

\[ \text{Sign}[t(i, i')] = \begin{cases} 
1 & \text{if } p_{i,j} > p_{i',j} \\
0 & \text{if } p_{i,j} = p_{i',j} \\
-1 & \text{if } p_{i,j} < p_{i',j} 
\end{cases} \]

...
From $s(i, i') = \text{Sign}[t_{i,j} \otimes t_{i', j}] (i, i' \in \{0, 1, \ldots, d - 1\})$, TP can give the size relationship of $p_0, j, p_1, j, \ldots, p_k j (j = 1, 2, \ldots, m)$ correctly.

2.4 A novel example of the protocol

Here, we will give a novel example for illustration without considering the eavesdropping checking. Let $k = 3, m = 2, l = 4$, and $d = 2l + 1 = 9$. The privacies of $P_0, P_1,$ and $P_2$ are $p_0 = (1, 4), p_1 = (2, 2)$, and $p_2 = (2, 3)$.

1. TP prepares two identical 9-level 3-particle GHZ states $|\Phi\rangle_{0, 1, 2}^1 = |\Phi\rangle_{0, 1, 2}^2 = \frac{1}{2}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + \cdots + |8\rangle|8\rangle|8\rangle)_{0, 1, 2}$, splits them into 3-particle $S_0, S_1,$ and $S_2$, and sends them to $P_0, P_1$ and $P_2$ separately.

2. $P_0(P_1, P_2)$ selects a 2-length random sequence $r_0 = (4, 6), (r_1 = (2, 5), r_2 = (6, 1))$, performs the shift operator $U_{r_0} U_{r_1} U_{r_2}$ to the $j$th particle of the sequence $S_0(S_1, S_2)$, where $j = 1, 2$, and sends the resulted particle sequence to TP.

3. At this moment, TP possesses the 3-particle GHZ states $|\Phi\rangle_{0, 1, 2}^1$ and $|\Phi\rangle_{0, 1, 2}^2$ which will be

$$|\Phi\rangle_{0, 1, 2}^1 = \frac{1}{3}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + |2\rangle|2\rangle|2\rangle + |3\rangle|3\rangle|3\rangle + |4\rangle|4\rangle|4\rangle + |5\rangle|5\rangle|5\rangle + |6\rangle|6\rangle|6\rangle + |7\rangle|7\rangle|7\rangle + |8\rangle|8\rangle|8\rangle)_{0, 1, 2}$$

$$|\Phi\rangle_{0, 1, 2}^2 = \frac{1}{3}(|0\rangle|0\rangle|0\rangle + |1\rangle|1\rangle|1\rangle + |2\rangle|2\rangle|2\rangle + |3\rangle|3\rangle|3\rangle + |4\rangle|4\rangle|4\rangle + |5\rangle|5\rangle|5\rangle + |6\rangle|6\rangle|6\rangle + |7\rangle|7\rangle|7\rangle + |8\rangle|8\rangle|8\rangle)_{0, 1, 2}$$

4. TP measures each particle in $|\Phi\rangle_{0, 1, 2}^1$ and $|\Phi\rangle_{0, 1, 2}^2$ on the Z-basis, and he will get $|w_0\rangle = |w_{0, 1}\rangle|w_{0, 2}\rangle = |c_1 \oplus r_{0, 1}\rangle|c_2 \oplus r_{0, 2}\rangle, |w_1\rangle = |w_{1, 1}\rangle|w_{1, 2}\rangle = |c_1 \oplus r_{1, 1}\rangle|c_2 \oplus r_{1, 2}\rangle, |w_2\rangle = |w_{2, 1}\rangle|w_{2, 2}\rangle = |c_1 \oplus r_{2, 1}\rangle|c_2 \oplus r_{2, 2}\rangle$, where $c_1, c_2 \in \{0, 1, \ldots, 8\}$. For example, if $|w_0\rangle = |4\rangle|7\rangle$, then $c_1 = 0, c_2 = 1, |w_1\rangle = |2\rangle|6\rangle, |w_2\rangle = |6\rangle|2\rangle$.

5. $P_0(P_1, P_2)$ encodes his privacy into $\overline{p_0} = (p_{0, 1} \oplus r_{0, 1}, p_{0, 2} \oplus r_{0, 2}) = (6, 7)$ (similarly, $\overline{p_1} = (0, 6), \overline{p_2} = (5, 2)$ ) by $r_0(r_1, r_2)$, and sends it to TP through an authenticated channel.

6. TP calculates:

$$t_0 = \overline{p_0} \oplus w_0 = (6, 7) \oplus (4, 7) = (1, 5)$$
$$t_1 = \overline{p_1} \oplus w_1 = (0, 6) \oplus (2, 6) = (2, 3)$$
$$t_2 = \overline{p_2} \oplus w_2 = (5, 2) \oplus (6, 2) = (2, 4)$$
$$t(0, 1) = t_0 \oplus t_1 = (8, 2)$$
$$t(0, 2) = t_0 \oplus t_2 = (8, 1)$$
\( t(1, 2) = t_1 \oplus t_2 = (0, 8) \)
\( s(0, 1) = (\text{Sign}[8], \text{Sign}[2]) = (-1, 1) \)
\( s(0, 2) = (\text{Sign}[8], \text{Sign}[1]) = (-1, 1) \)
\( s(1, 2) = (\text{Sign}[0], \text{Sign}[8]) = (0, -1) \)

From Eq. (7) and \( s(0, 1) = (-1, 1) \), \( TP \) will get \( p_{0,1} < p_{1,1} \) and \( p_{0,2} > p_{1,2} \). Similarly, \( TP \) will get \( p_{0,1} < p_{2,1} \) and \( p_{0,2} > p_{2,2}, p_{1,1} = p_{2,1} \) and \( p_{1,2} < p_{2,2} < p_{0,2} \). At last, he publishes the information \( R_1 \triangleq 0 < 1 = 2 \) and \( R_2 \triangleq 2 < 3 < 0 \).

### 3 Security analysis and efficiency comparison

In this section, we will analyze the security of our protocol from both external and internal attacks. Also, we will analyze the efficiency of our protocol and compare it with other existing protocols.

#### 3.1 Security analysis of the protocol

**Case 1 External attack** Suppose that an outsider eavesdropper, Eve, tries to obtain the privacies of participants. From the procession of the protocol, the privacy of each participant \( P_i \) is transmitted only once and is encrypted by a random sequence \( r_i = (r_{i,0}, r_{i,1}, \ldots, r_{i,m}) \). Hence, Eve must find a way to intercept the sequence \( r_i = (r_{i,0}, r_{i,1}, \ldots, r_{i,m}) \) in Step 3 and the encrypted sequence \( \overline{p_i} = (p_{i,1} \oplus r_{i,1}, p_{i,2} \oplus r_{i,2}, \ldots, p_{i,m} \oplus r_{i,m}) \) in Step 5. To obtain \( r_i \), he must carry out intercept-resend attack, i.e., he intercepts and takes measurements on the particles of \( S_i \) and the particles of \( \overline{S_i} \), and resents them to receiver. Let us take the intercept-resend attack on the particles of \( S_i \) for example. Due to the existence of the decoy states, Eve need to choose the correct position and measurement basis of each decoy state in order not to detected by the eavesdropping checking. However, he does not have any information on the position and measurement basis of each decoy state. If he chooses the right position and right basis, no error will be introduced, or else, the probability of introducing error will be at least \( \frac{d-1}{d} \). Hence, his eavesdropping behavior will be detected with \( 1 - (\frac{d-1}{2d})^m \), which will approach to 1 when \( m \) is large enough. It is the same with the case of intercept-resend attack on the particles of \( \overline{S_i} \). Therefore, Eve cannot obtain the random sequence \( r_i = (r_{i,0}, r_{i,1}, \ldots, r_{i,m}) \). Also, he can not obtain the sequence \( \overline{p_i} = (p_{i,1} \oplus r_{i,1}, p_{i,2} \oplus r_{i,2}, \ldots, p_{i,m} \oplus r_{i,m}) \) in Step 5 because the channels between the TP and participants are authenticated. From the analysis above, the protocol is immune to external attack.

**Case 2 Internal attack from participants** Suppose that a participant, \( P_0 \), is a dishonest participant who tries to obtain the privacies of other participants, and TP is the semi-honest party who will not collude with anyone. If \( P_0 \) wants to steal the privacy of a
certain participant $P_i (i \in \{1, 2, \cdots, d-1\})$, he could firstly measures the particles in the sequence of $S_0$ on the $Z$-basis before performing the random shift operators on them, and the measurement results are identical to the particles in $S_i$. Next, to obtain the random sequence $r_i$, $P_0$ needs to measure the particles in the sequence $\overline{S_i}$ by using the intercept-resend attack. In this environment, $P_0$ can be considered as an outside attacker, and his interception behavior will be caught by $P_i$ and TP similar to the case of external attack. Also, $P_0$ cannot obtain the sequence $\overline{p_i}$ in Step 5 because the channel between TP and $P_i$ is authenticated. The collusion attack from multiple participant is the same.

Case 3 Internal attack from the semi-honest third party TP Obviously, the dishonest third party TP is the one who can get the most information during the execution of the protocol. However, due to his semi-honesty, he will prepare the $k$-particle $d$-level GHZ states rather than other types of particles such as single particles (even if he prepared other quantum states, his dishonest behavior would be discovered by participants in the following way. Before step 3, all participants consult to select some positions of particles randomly, and measure each particle of these positions using either X-basis or Z-basis. They can verify whether these quantum states are GHZ states or not by publishing the measurement results). Next, TP will execute the protocol honestly. The only way to derive the privacy of $P_i$ relies on the analysis of information received from $P_i$. Firstly, he can obtain $\overline{p_i} = (p_{i,1} \oplus r_{i,1}, p_{i,2} \oplus r_{i,2}, \cdots, p_{i,m} \oplus r_{i,m})$ legally in Step 5. So he needs to get the random sequence $r_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,m}) \in \{0, 1, \ldots, d-1\}^m$ and next extracts the privacy of $P_i$. Apparently, the random sequence $r_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,m}) \in \{0, 1, \ldots, d-1\}^m$ is encoded into the sequence $\overline{S_i}$ which is entangle with $\overline{S_j}$s. When it comes to measure the particles in the sequence $\overline{S_i}$, TP will randomly get one of the following states: $|r_{i,1}r_{i,2}\cdots r_{i,m}|, |r_{i,1}\oplus 1r_{i,2}\oplus 1\cdots r_{i,m}\oplus 1|, \cdots, |r_{i,1}\oplus (d-2)r_{i,2}\oplus (d-2)\cdots r_{i,m}\oplus (d-2)|$ and $|r_{i,1}\oplus (d-1)r_{i,2}\oplus (d-1)\cdots r_{i,m}\oplus (d-1)|$. Hence, TP cannot obtain $r_i = (r_{i,1}, r_{i,2}, \ldots, r_{i,m}) \in \{0, 1, \ldots, d-1\}^m$ accurately, and cannot derive the privacy of $P_i$.

3.2 Efficiency comparison with existed protocols

Here, we will compare the protocol with four existing MQPC protocols in the following five aspects: quantum resources used, the category of MQPC (size or equality comparison), the qubit or qudit efficiency which is defined as $\eta = c\overline{q+p}$ (here $c$ is the length of privacies of participants, $q$ and $b$ are the numbers of qudits and classical bits used in transmission and eavesdropping checking, whether participants need to share privacy common key beforehand, and security). For the sake of discussion, it is assumed that the length of the privacies is $m$, and the number of decoy particles is equal to the number of quantum particles transmitted in each MQPC protocol. The four existing MQPC protocols are CTH2013 protocol [16], HHH2017 protocol [25], LYS2014 protocol [31], and HHG2015 protocol [32]. Now, we will show the comparison result in Table 1.

(1) CTH2013 protocol. The authors proposed a 4-party QPC protocol, and a multi-party (say $k$-party hereafter) QPC protocol which are used to compare the equality
| QPC protocol       | Quantum resources          | Category of QPC | Efficiency $\eta$ | Need to share privacy key | Security  |
|--------------------|---------------------------|-----------------|-------------------|----------------------------|-----------|
| CTH2013 [16]       | 2-level GHZ-class states  | Equality        | $\frac{1}{4}$    | No                         | Secure    |
| HHH2017 [25]       | 2-level Bell states       | Equality        | $\frac{1}{3k}$   | No                         | Secure    |
| LYS2014 protocol [31] | $d$-level entangled states | Size           | $\frac{1}{3}$   | Yes                        | Secure    |
| HHG2015 protocol [32] | $d$-level GHZ and entangled particles | Size           | $\frac{1}{6k}$  | No                         | Insecure  |
| Ours               | $d$-level GHZ states      | Size            | $\frac{1}{3k}$  | No                         | Secure    |
of the privacies. We only consider the case of $k$-party. The quantum resources used in this protocol are 2-level $k$-particle GHZ-class states. The transmission of information includes two stages. First, TP prepares $m$ $k$-particle GHZ-class states. Then, he splits them into $k$ particle sequence and sends every sequence to the corresponding participant with $m$ decoy particles. Second, each participant sends his encoded privacy which is $m$ bits to TP. Hence, the efficiency $\eta = \frac{m}{mk + mk + mk} = \frac{1}{3k}$. Besides, the participants need not to share privacy common key beforehand, and the protocol is secure at present because there is no efficient attack for it.

(2) HHH2017 protocol. The authors proposed a $k$-party QPC protocol of comparing the equality in which two TPs are introduced to deal with the comparison in a strange environment. The quantum resources used in this protocol are 2-level $k$-particle GHZ-class states. The transmission of information includes three stages. First, TP$_1$ prepares $2m$ $k$-particle GHZ-class states. Then, he splits them into $k$ particle sequence and sends every sequence to the corresponding participant with $2m$ decoy particles. Second, TP$_1$ sends the information of the GHZ states to TP$_2$ using quantum secure direct communication and the quantum resource used here is at least $2mk$ qubits. Third, each participant sends his encoded privacy which is $m$ bits to TP$_1$ and TP$_2$. Hence, the efficiency $\eta = \frac{m}{2mk + mk + 2mk + mk + mk} = \frac{1}{8k}$. Besides, the participants also need not to share privacy common key beforehand, and the protocol is secure at present.

(3) LYS2014 protocol. The authors proposed a $k$-party QPC protocol of comparing the sizes of privacies. The quantum resources used in this protocol are $d$-level entangled states, and the participants need to share a privacy common key $K$ beforehand through a secure QKA protocol. The transmission of information contains three step. First, TP prepares $mk$ $d$-particle $d$-level GHZ states. Then, he splits the $mk$ particle sequence into $k$ particle sequences and sends each sequence to the corresponding participant with $m$ decoy particles. Second, each participant measures the received particle sequence which will be transformed into a classical $m-bit$ sequence, and he encrypts his privacy by the classical bit sequence and the privacy common key $K$ using one-time pad. At last, each participant sends his encrypted privacy information ($m$-bit sequence) to TP through an authenticated channel. Hence, the efficiency $\eta = \frac{m}{mk + mk + mk} = \frac{1}{3k}$. However, the actual efficiency is lower than $\frac{1}{3k}$ because the participants need to share a privacy common key $K$ beforehand through a QKA protocol which will waste a lot of quantum resource. This protocol is secure at present because there is no efficient attack for it.

(4) HHG2015 protocol. The authors proposed a $k$-party QPC protocol of comparing the sizes of privacies. The quantum resources used in this protocol are $d$-level GHZ states and $d$-level entangled states. The transmission of information includes two stages. First, TP prepares $m$ $k$-particle $d$-level GHZ states and $mk$ $d$-level entangled states. Then, TP splits the $mk$ $k$-particle $d$-level GHZ states into $k$ particle sequences and sends them to the corresponding participant with $m$ decoy particles. Also, he splits the $mk$ $k$-particle $d$-level entangled states into $k$ particle sequences and sends them to the corresponding participant.
with \(m\) decoy particles. Second, each participant measures the first \(k\)-particle sequence. Then, he performs the unitary operations, which are decided by the measurement results and his privacy, on the second \(k\)-particle sequence and sends the resulted \(k\)-particle sequence with \(m\) decoy particles to TP. The efficiency 
\[
\eta = \frac{m}{2mk+2mk+mk+mk} = \frac{1}{6k}
\]
Besides, the participants need not to share a privacy common key beforehand. Hence, the HHG2015 protocol is much more efficient than LYS2014 protocol. However, there is a serious bug in the HHG2015 protocol. From Step 4 and Step 6, we can easily get that \(p_i = p_j\) and \(q_i = q_j\) for each \(i\) and \(j\). If a dishonest participant (say \(P_1\)) wants to steal the privacy of another one (say \(P_2\)), he will firstly intercept the particles sent from \(P_2\) and resents forged particles to TP in Step 4. Secondly, he deletes the decoy particles and measures the remaining particles after \(P_2\) published the positions of decoy states. Therefore, \(P_1\) will get the value of \(MR_2 = (s_2 + p_2 + q_2) mod d\) and \(s_2 = (MR_2 - p_2 - q_2) mod d\) which is the privacy of \(P_2\). Although this attack will be discovered by TP and \(P_2\), but they did not know the identity of the attacker. Hence, \(P_1\) succeeded in obtaining the privacy of \(P_2\). Similarly, he can get the privacy of any other participant without being found. So, this protocol is insecure.

5. Our protocol. We proposed a \(k\)-party QPC protocol of comparing the sizes of privacies by using \(k\)-particle \(d\)-level GHZ states, and the participants need not to share privacy common key beforehand. The transmission of information includes three stages. First, TP prepares \(mk\)-particle GHZ-class states. Then, he splits them into \(k\) particle sequence and sends each sequence to the corresponding participant with \(m\) decoy particles. Second, after encoding the received sequence by a series of random unitary operations, each participant inserts \(m\) decoy particles into it and sends it back to TP. Third, every participant transmits \(m\) classical bits to TP separately. Hence, the efficiency 
\[
\eta = \frac{m}{mk+mk+mk} = \frac{1}{3k}
\]
which is as good as that of the LYS2014 protocol and CTH2013 protocol, and our protocol is secure against external and internal attacks. However, owing to the waste of quantum resource in sharing the common key beforehand through a QKA protocol in the LYS2014 protocol, our protocol is more efficient than it because the participants need not to share private common key beforehand in our protocol. Besides, the CTH2013 protocol only solves the problem of equality comparison. Therefore, our protocol is better than the LYS2014 protocol and CTH2013 protocol.

4 Conclusion

We presented a MQPC protocol with \(k\)-particle \(d\)-level GHZ states. In the protocol, all participants can compare the size of their privacy with the help of a semi-honest party TP. Besides, we gave a novel example of the proposed protocol. Security analysis shows that it is immune to both external attack and internal attack in theory, and efficiency comparison shows that it is prior to all existing protocols of the same type. However, our protocol is only suitable for scenarios in an ideal environment. How to
improve the agreement to adapt to a more complicated environment is our main work in the future.

Acknowledgements This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802400, the National Science Foundation of China under Grant 61373171 and 11801564, the 111 Project under Grant B08038, the Program for Excellent Young Talents in University of Anhui Province under Grant gxyqZD2019060, the Basic Research Project of Natural Science of Shaanxi Province under Grant 2017JM6037 and 2017JQ1032, and the Key Project of Science Research of Anhui Province under Grant KJ2017A519.

References

1. Yao, A.C.C.: Protocols for secure computations [C]. FOCS 82, 160–164 (1982)
2. Ioannidis, I., Grama, A.: An efficient protocol for Yao’s millionaires’ problem. In: Proceedings of the 36th Annual Hawaii International Conference on System Sciences. IEEE, 6 pp (2003)
3. Lin, H.Y., Tzeng, W.G.: An efficient solution to the millionaires problem based on homomorphic encryption. In: International Conference on Applied Cryptography and Network Security, pp. 456–466. Springer, Berlin (2005)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: public-key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computer System and Signal Processing, pp. s175–179, (1984)
5. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science 283, 2050–2056 (1999)
6. Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94, 230504 (2005)
7. Hillery, M., Buzek, V., Berthaume, A.: Quantum secret sharing. Phys. Rev. A 59, 1829–1834 (1999)
8. Bai, C.M., Li, Z.H., Liu, C.J., et al.: Quantum secret sharing using orthogonal multiqudit entangled states. Quantum Inf. Process. 16(12), 304 (2017)
9. Cao, H., Ma, W.: (t, n) threshold quantum state sharing scheme based on linear equations and unitary operation. IEEE Photonics J. 9(1), 1–7 (2017)
10. Zhang, W., Ding, D.S., Sheng, Y.B., et al.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. 118(22), 220501 (2017)
11. Cao, H., Ma, W.: Multiparty quantum key agreement based on quantum search algorithms. Sci. Rep. 7, 45046 (2017)
12. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum privacy comparison protocol with decoy photons and two-photon entanglement. J. Phys. A Math. Theor. 42(5), 055305 (2009)
13. Chen, X.B., Xu, G., Niu, X.X., et al.: An efficient protocol for the privacy comparison of equal information based on the triplet entangled state and single-particle measurement. Optics Commun. 283(7), 1561–1565 (2010)
14. Xu, G.A., Chen, X.B., Wei, Z.H., et al.: An efficient protocol for the quantum privacy comparison of equality with a four-qubit cluster state. Int. J. Quantum Inf. 10(04), 1250045 (2012)
15. Tseng, H.Y., Lin, J., Hwang, T.: New quantum privacy comparison protocol using EPR pairs. Quantum Inf. Process. 11(2), 373–384 (2012)
16. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user privacy comparison protocol using GHZ class states. Quantum Inf. Process. 12, 1–12 (2013)
17. Zhang, B., Liu, X., Wang, J., et al.: Cryptanalysis and improvement of quantum privacy comparison of equality protocol without a third party. Quantum Inf. Process. 14(12), 4593–4600 (2015)
18. Sun, Z., Yu, J., Wang, P., et al.: Quantum privacy comparison with a malicious third party. Quantum Inf. Process. 14(6), 2125–2133 (2015)
19. Liu, B., Xiao, D., Huang, W., et al.: Quantum privacy comparison employing single-photon interference. Quantum Inf. Process. 16(7), 180 (2017)
20. He, G.P.: Quantum privacy comparison protocol without a third party. Int. J. Quantum Inf. 15(02), 1750014 (2017)
21. Xu, L., Zhao, Z.: Quantum privacy comparison protocol based on the entanglement swapping between $\chi^+$ state and W-Class state. Quantum Inf. Process. 16(12), 302 (2017)
22. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum privacy comparison protocol with n-level entangled states. Quantum Inf. Process. 13, 2370–2389 (2014)
23. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum privacy comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. 55(6), 2969–2976 (2016)
24. Ye, T.Y.: Multi-party quantum privacy comparison protocol based on entanglement swapping of Bell entangled states. Commun. Theor. Phys. 66(3), 280 (2016)
25. Hung, S.M., Hwang, S.L., Hwang, T., et al.: Multiparty quantum privacy comparison with almost dishonest third parties for strangers. Quantum Inf. Process. 16(2), 36 (2017)
26. Jia, H.Y., Wen, Q.Y., Song, T.T., et al.: Quantum protocol for millionaire problem. Optics Commun. 284(1), 545–549 (2011)
27. Lin, S., Sun, Y., Liu, X.F., et al.: Quantum privacy comparison protocol with d-dimensional Bell states. Quantum Inf. Process. 12(1), 559–568 (2013)
28. Guo, F.Z., Gao, F., Qin, S.J., et al.: Quantum privacy comparison protocol based on entanglement swapping of d-level Bell states. Quantum Inf. Process. 12(8), 2793–2802 (2013)
29. Zhang, W.W., Li, D., Zhang, K.J., et al.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. 12(6), 2241–2249 (2013)
30. Yu, C.H., Guo, G.D., Lin, S.: Quantum privacy comparison with d-level single-particle states. Phys. Scr. 88(6), 065013 (2013)
31. Luo, Q., Yang, G., She, K., et al.: Multi-party quantum privacy comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. 13(10), 2343–2352 (2014)
32. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum privacy comparison with an almost-dishonest third party. Quantum Inf. Process. 14(11), 4225–4235 (2015)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.