Multi-party quantum private comparison of size relation with \(d\)-level single-particle states

Chong-Qiang Ye \(^1\) · Tian-Yu Ye \(^1\)

Received: 4 May 2018 / Accepted: 6 August 2018 / Published online: 16 August 2018
© Springer Science+Business Media, LLC, part of Springer Nature 2018

Abstract
In this paper, by using \(d\)-level single-particle states, two novel multi-party quantum private comparison protocols for size relation comparison with two semi-honest third parties and one semi-honest third party are constructed, respectively. Here, each protocol can compare the size relation of secret integers from \(n\) parties rather than just the equality within one time execution. In each protocol, every third party is assumed to be semi-honest in the sense that she may misbehave on her own but is not allowed to collude with anyone else; and each party employs the qudit shifting operation to encode her secret integer. Each protocol can resist both the outside attack and the participant attack. Specially, each party’s secret integer can be kept unknown to other parties and the third parties. The proposed protocol with two third parties is workable in a stranger environment, as there are no communication and no pre-shared key between each pair of party. The proposed protocol with one third party is workable in an acquaintance environment, as all parties need to share a common private key beforehand.

Keywords Quantum cryptography · Multi-party quantum private comparison · Size relation comparison · Semi-honest third party · \(d\)-level single-particle state

1 Introduction
Quantum cryptography can be regarded as the combination of quantum mechanics and classical cryptography. Depending on the fundamental principles of quantum mechanics, quantum cryptography has the prominent advantage of security over classical cryptography whose security relies on the computational complexity of solving mathematical problems. Since the first quantum cryptographic protocol was proposed by Bennett and Brassard [1], many quantum cryptographic protocols have been designed
to accomplish various cryptographic tasks that are intractable with classical cryp-
tography, such as quantum key distribution (QKD) [1–7], quantum secure direct
communication (QSDC) [8–10], quantum secret sharing (QSS) [11–21], quantum
teleportation [22–24], quantum private query [25–28] and so on.

Secure multi-party computation (SMC) aims to calculate a function with private
inputs from different parties in a distributed network on the basis of not disclosing
the genuine content of each private input and has been deeply studied in classical
cryptography so far. SMC can be applied into many circumstances including private
comparison, anonymous bidding and auctions, secret ballot elections, e-commerce
and date mining, etc. As an important branch of SMC, private comparison was first
introduced by Yao [29] in the millionaires’ problem. In the millionaires’ problem,
two millionaires want to judge who is richer without knowing each other’s actual
property. Afterward, Boudot et al. [30] suggested a private comparison protocol to
determine whether two millionaires are equally rich or not. However, the security of
classical private comparison protocols relies on the computation complexity of solving
mathematical problems, which is vulnerable to the strong ability of parallel quantum
computation.

As the generalization of classical private comparison into the realm of quantum
mechanics, quantum private comparison (QPC) was first suggested by Yang and Wen
[31] in 2009. In recent years, the design and analysis of QPC protocols have suc-
cessfully attracted much attention. Many QPC protocols [31–48] have been proposed.
Since it is impossible to construct a secure equality function in a two-party scenario
[49], all previous QPC protocols [31–48] have drawn support from a third party (TP).
However, all of these protocols [31–48] can only compare whether two parties’ secrets
are equal or not instead of their size relation. Fortunately, Lin et al. [50] successfully
proposed a QPC protocol for comparing the size relation by using \(d\)-level Bell states.
Guo et al. [51] successfully put forward a QPC protocol for comparing the size relation
based on entanglement swapping of \(d\)-level Bell states. Yu et al. [52] successfully put
forward a QPC protocol for comparing the size relation by using \(d\)-level single-particle
states.

The protocols described above can only compare the secrets for just two parties.
Chang et al. [53] put forward the first multi-party quantum private comparison (MQPC)
protocol by using multi-particle GHZ class states, which can accomplish arbitrary
pair’s comparison of equality among \(n\) parties within one-time execution of the pro-
tocol. Since then, MQPC has attracted more and more attention so that many MQPC
protocols within the multi-level system [54–59] have been designed. For example,
Luo et al. [57] proposed a MQPC protocol for comparing the size relation based on \(d\)-
dimensional entangled states; Huang et al. [58] proposed a MQPC protocol, in which
\(n\) parties can accomplish the comparison of size relation with the help of an almost-
dishonest TP within one time execution of the protocol; and Hung et al. [59] proposed
a MQPC protocol for strangers to accomplish the equality comparison with the help
of two almost-dishonest TPs within one time execution of the protocol.

Based on the above analysis, in this paper, by using \(d\)-level single-particle states, we
propose two novel MQPC protocols for size relation comparison with two semi-honest
TPs and one semi-honest TP, respectively. In each protocol, \(n\) parties can compare the
size relation of their secret integers within one time execution of the protocol. Here,
each TP is semi-honest in the sense that she may misbehave on her own but is not allowed to collude with anyone else. The proposed MQPC protocol with two TPs is suitable for strangers to accomplish the size relation comparison, as there are no requirements of communication and pre-shared key between each pair of party. The proposed MQPC protocol with one TP is suitable for acquaintances to accomplish the size relation comparison, as all parties need to share a common private key beforehand.

The rest of this paper is organized as follows. In Sect. 2, we present a MQPC protocol for comparing the size relation of secret integers from different parties with the help of two semi-honest TPs and analyze its security against several famous attacks; in Sect. 3, we present a MQPC protocol for comparing the size relation of secret integers from different parties with the help of one semi-honest TP and analyze its security against several famous attacks; and finally, discussion and conclusion are given in Sect. 4.

2 The proposed MQPC protocol for size relation comparison with two semi-honest TPs

In a $d$-level quantum system, a common basis of single photons can be described as follows:

$$T_1 = \{|j\rangle\}, \quad j \in \{0, 1, \ldots, \frac{d}{2} - 1\}. \quad (1)$$

Each element in the set $T_1$ is orthogonal to the others. After performing the $d$th order discrete quantum Fourier transform $F$ on each state in $T_1$, another basis shown in Eq. (2) forms:

$$T_2 = \{F|j\rangle\} = \left\{ \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{2\pi ijk/d} |k\rangle \right\}, \quad j \in \{0, 1, \ldots, d - 1\}. \quad (2)$$

Each element in the set $T_2$ is also orthogonal to the others. The two sets, $T_1$ and $T_2$, are two common conjugate bases. The unitary operations shown in Eq. (3) represent the qudit shifting operations, where $m \in \{0, 1, \ldots, d - 1\}$.

$$U_m = \sum_{k=0}^{d-1} |k + m\rangle \langle k|. \quad (3)$$

2.1 Protocol description

Assume that the party $P_i$ has the secret integer $s_i$, where $i = 1, 2, \ldots, n$. There is a natural number $r$ satisfying $r > \{s_i\}_{\text{max}}$ and $d \geq 2r - 1$. The $n$ parties execute the following steps to complete the aim of size relation comparison with the help of two semi-honest TPs, $TP_1$ and $TP_2$. $TP_1$ ($TP_2$) is semi-honest in the sense that she may misbehave on her own but is not allowed to conspire with anyone else. Note that this kind of semi-honest TP belongs to the second semi-honest model of TP in Ref. [40]. Moreover, the term “semi-honest” here is equivalent to the term “almost-dishonest”
in Ref. [58]. It should be emphasized that to make the protocol effective, both TP1 and TP2 should authenticate the identity of $P_i$ before implementing the protocol. As a result, a key which can represent the identity of $P_i$ should be pre-shared between $P_i$ and TP1 (TP2).

**Step 1:** TP1 prepares $n$ single particles, $|k_1⟩, |k_2⟩, \ldots, |k_n⟩$, which are randomly chosen from the set $T_1$. It should be ensured that $k_i$ meets the relation of $k_i + k'_i = K$. Here, $k_i \in \{0, 1, \ldots, r - 1\}, k'_i \in \{0, 1, \ldots, d - 1\}, i = 1, 2, \ldots, n$ and $K$ is a constant. Note that only TP1 knows the genuine value of $K$.

**Step 2:** TP1 prepares $n$ groups of $l$ decoy photons, which are denoted as $G_1, G_2, \ldots, G_n$, respectively. Here, each decoy photon is one of the states randomly chosen from the set $T_1$ or $T_2$. Afterward, TP1 inserts the particle $|k_i⟩$ into $G_i$ at random positions to construct a new sequence $G'_{i}$. Finally, TP1 sends $G'_{i}$ to $P_i$, where $i = 1, 2, \ldots, n$.

**Step 3:** After confirming that $P_i$ ($i = 1, 2, \ldots, n$) has received all particles, TP1 and $P_i$ check the security of the transmission of $G'_{i}$. Concretely, TP1 announces the positions and the preparation bases of decoy photons to $P_i$. According to the announced information, $P_i$ uses the right bases to measure the corresponding decoy photons and returns the measurement results to TP1. Afterward, by comparing the measurement results of decoy photons with their corresponding initial prepared states, TP1 can check whether the transmission of $G'_{i}$ is secure or not. If it is secure, the protocol will proceed to the next step; otherwise, the protocol will be terminated and restarted from Step 1.

**Step 4:** After removing the decoy photons in $G'_{i}$ ($i = 1, 2, \ldots, n$), in order to encode her secret integer $s_i$, $P_i$ performs the operation $U_{s_i} = \sum_{k=0}^{d-1} |k + s_i⟩⟨k|$ on the particle $|k_i⟩$ to obtain the state $|k_i + s_i⟩$. It should be pointed out that $k_i + s_i < d$. Afterward, $P_i$ prepares a quantum state sequence $G''_{i}$ composed of $l$ decoy photons. Here, each decoy photon is also one of the states randomly chosen from the set $T_1$ or $T_2$. Then, $P_i$ inserts the particle $|k_i + s_i⟩$ into $G''_{i}$ at random positions to construct a new sequence $G'''_{i}$. Finally, $P_i$ sends $G'''_{i}$ to TP2.

**Step 5:** After confirming that TP2 has received all particles, $P_i$ ($i = 1, 2, \ldots, n$) and TP2 check the security of the transmission of $G'''_{i}$. Firstly, $P_i$ announces the positions and the preparation bases of decoy photons which are chosen from the set $T_2$. According to the announced information, TP2 uses the right bases to measure the corresponding decoy photons and returns the measurement results to $P_i$. Then, by comparing the measurement results of decoy photons with their corresponding initial prepared states, $P_i$ can calculate the error rate. If the error rate is greater than the threshold value, the protocol will be terminated and restarted from Step 1; otherwise, the protocol will proceed to the next step.

**Step 6:** TP2 drops out the decoy photons in $G'''_{i}$ ($i = 1, 2, \ldots, n$) which are chosen from the set $T_2$. For the remaining particles on the site of TP2, $P_i$ tells TP2 the positions and the preparation bases of decoy photons which are chosen from the set $T_1$. Afterward, TP2 uses the right bases to measure the corresponding decoy photons and returns the measurement results to $P_i$. Then, by comparing the measurement results of decoy photons with their corresponding initial prepared states, $P_i$ can calculate the error rate. If the error rate is greater than the threshold value, the protocol will be
Fig. 1 The flow chart of the proposed MQPC protocol with two TPs. Here, we ignore the security check processes and take TP1, P1 and TP2 for example. The solid line with an arrow denotes the quantum state transmission operation, while the dotted line with an arrow represents the classical information transmission operation.

terminated and restarted from Step 1; otherwise, the protocol will proceed to the next step.

**Step 7:** TP2 uses the correct base to measure the particle |k_i + s_i⟩ (i = 1, 2, ..., n) and obtains the value of k_i + s_i. Then, TP1 announces k_1', k_2', ..., k_n' to TP2 through the classical channel. Afterward, TP2 calculates the sum of k_i + s_i and k_i', i.e., M_i = k_i + s_i + k_i'. Because k_i + k_i' = K, the size relation of different M_i's is the same to that of different s_i's. As a result, TP2 can know the size relation of different s_i's, but cannot know the genuine value of s_i due to lack of knowledge about k_i. Finally, TP2 announces the size relation of different M_i's through the classical channel. According to the announced information, P1 can know the size relation of different s_i's.

Now it concludes the description of the proposed MQPC protocol with two TPs. For clarity, we further show its flow chart in Fig. 1, taking TP1, P1 and TP2 for example, after ignoring the security check processes.

### 2.2 Security analysis

In this subsection, we analyze the security of the proposed MQPC protocol with two TPs. Firstly, we show that the outside attack is invalid to the proposed MQPC protocol with two TPs. Secondly, we show that one or more parties cannot learn other parties’ secret integers. Moreover, the semi-honest TP1 and TP2 cannot learn these parties’ secret integers either.

#### 2.2.1 The outside attack

We analyze the possibility for an outside eavesdropper to steal the parties’ secret integers according to each step of the proposed MQPC protocol.

In Step 1, there is nothing transmitted. Hence, an outside eavesdropper has no chance to launch her attacks in this step.
In Step 2, TP1 sends $G'_i$ to $P_i$, and in Step 4, $P_i$ sends $G''''_i$ to TP2. Here, $i = 1, 2, \ldots, n$. An outside eavesdropper may utilize the qudit transmissions in these two steps to extract some useful information about the parties’ secret integers. Obviously, both of these two steps use the decoy photon technique [60, 61] to guarantee the security of qudit transmissions. The decoy photon technology can be thought as a variant of the eavesdropping check method of the BB84 protocol [1] which has been proven to be unconditionally secure [62]. The effectiveness of decoy photon technology for two-level quantum system toward the intercept–resend attack, the measure–resend attack and the entangle–measure attack has also been validated in Refs. [63, 64]. It is straightforward that the decoy photon technology for $d$-level quantum system is also effective toward these famous attacks. Therefore, an outside eavesdropper cannot extract any useful information about secret integers without being detected by the eavesdropping check processes in Steps 3, 5 and 6.

In Step 7, TP1 announces $k'_1, k'_2, \ldots, k'_n$ to TP2, and TP2 announces the size relation of different $M_i$s ($i = 1, 2, \ldots, n$) through the classical channel. Even though an outside eavesdropper may hear of $k'_1, k'_2, \ldots, k'_n$ and the comparison result of size relation, these pieces of information are still helpless for her to obtain the genuine values of secret integers.

In addition, it should be emphasized that in order to overcome the invisible photon eavesdropping Trojan horse attack [65], $P_i$ should insert a filter in front of her devices to filter out the photon signal with an illegitimate wavelength [66, 67]. Moreover, in order to resist the delay-photon Trojan horse attack [66, 68], $P_i$ should adopt a photon number splitter (PNS: 50/50) to split each sample quantum signal into two pieces and measure the signals after the PNS with proper measuring bases [66, 67]. If the multiphoton rate is unreasonably great, this attack will be discovered.

2.2.2 The participant attack

Gao et al. [69] first pointed out that the attack from a dishonest participant is generally more powerful and should be paid more attention to. Up to now, the participant attack has attracted much attention in the cryptanalysis of quantum cryptography [70–72]. In this subsection, we consider three cases of participant attack. Firstly, we discuss the attack from one or more dishonest parties; secondly, we discuss the participant attack from semi-honest TP1; and thirdly, we discuss the participant attack from semi-honest TP2.

Case 1 The participant attack from one or more dishonest parties

Two situations should be considered in this case. One is that one dishonest party wants to steal other parties’ secret integers; the other one is that two or more dishonest parties conclude together to steal other parties’ secret integers.

(a) The participant attack from one dishonest party

It is apparent that in the proposed MQPC protocol with two TPs, the roles of $n$ parties are the same. Without loss of generality, in this situation, we suppose that $P_1$ is the only dishonest party who wants to steal other parties’ secret integers.

In the proposed MQPC protocol with two TPs, there are qudits transmitted from TP1 to $P_j$ ($j = 2, 3, \ldots, n$) in Step 2 and from $P_j$ to TP2 in Step 4. However, there is not
any qudit transmitted between $P_1$ and $P_j$. As a result, $P_1$ is thoroughly independent from $P_j$. In order to obtain the secret integer of $P_j$, when $P_1$ tries to launch her attacks on the transmitted particles from TP$_1$ to $P_j$ in Step 2 or from $P_j$ to TP$_2$ in Step 4, she essentially acts as an outside eavesdropper. As analyzed in Sect. 2.2.1, she will inevitably be caught if she launches her attacks, as she has no knowledge about the positions and the preparation bases of transmitted decoy photons.

In addition, in Step 7, $P_1$ may hear of $k'_1, k'_2, \ldots, k'_n$ from TP$_1$ and the comparison result of size relation from TP$_2$. However, this information is still helpless for her to obtain the secret integer of $P_j$.

It can be concluded now that one dishonest party cannot obtain other parties’ secret integers.

(b) The participant attack from two or more dishonest parties

If the number of dishonest parties concluding together is $n - 1$, the dishonest parties will be the most powerful. Here, we only consider this extreme case. Without loss of generality, suppose that the dishonest $P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ collude together to get the secret integer of $P_m$.

It is apparent that $P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ are thoroughly independent from $P_m$. If $P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ try to launch their attacks on the transmitted particles from TP$_1$ to $P_m$ in Step 2 or from $P_m$ to TP$_2$ in Step 4, as analyzed in Sect. 2.2.1, they will inevitably be detected as an outside eavesdropper, since they have no knowledge about the positions and the preparation bases of transmitted decoy photons.

In addition, in Step 7, $P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ may hear of $k'_1, k'_2, \ldots, k'_n$ from TP$_1$ and the comparison result of size relation from TP$_2$. However, this information is still helpless for them to obtain the secret integer of $P_m$.

It can be concluded now that the dishonest $P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n$ cannot get the secret integer of $P_m$. It is straightforward that the colluding attack from two or more dishonest parties is invalid for them to steal the secret integers from other parties.

**Case 2:** The participant attack from semi-honest TP$_1$

In the proposed MQPC protocol with two TPs, TP$_1$ is not allowed to conspire with anyone else including TP$_2$. As a result, TP$_1$ cannot know the state of $|k_i + s_i\rangle$ ($i = 1, 2, \ldots, n$) from TP$_2$. In order to obtain the state of $|k_i + s_i\rangle$, TP$_1$ may further try to intercept the transmitted particles from $P_i$ to TP$_2$ in Step 4, measure them with the base $T_1$ and resend the measured particles to TP$_2$. However, this attack from TP$_1$ will be easily detected by the security check process in Step 5, as it alters the states of decoy photons chosen from the set $T_2$. It can be concluded that TP$_1$ has no knowledge about the state of $|k_i + s_i\rangle$ at all.

In Step 1, TP$_1$ knows the states of $|k_1\rangle, |k_2\rangle, \ldots, |k_n\rangle$ and the values of $k'_1, k'_2, \ldots, k'_n$. In Step 7, TP$_1$ may hear of the comparison result of size relation from TP$_2$. However, she still cannot infer out the secret integer of $P_i$ from this information, as she has no chance to know the state of $|k_i + s_i\rangle$.

**Case 3:** The participant attack from semi-honest TP$_2$

In the proposed MQPC protocol with two TPs, TP$_2$ is not allowed to conspire with anyone else including TP$_1$. The main task of TP$_2$ is to measure the state of $|k_i + s_i\rangle$.
(i = 1, 2, ..., n), calculate the sum of \( k_i + s_i \) and \( k_i’ \), and compare the size relation of secret integers from \( n \) parties. In Step 7, TP2 can know the state of \( |k_i + s_i\rangle \). In order to obtain the secret integer of \( P_i \), TP2 needs to know the state of \( |k_i\rangle \). As a result, TP2 may try to intercept the transmitted particles from TP1 to \( P_i \) in Step 2, measure them with the base \( T_1 \) and resend the measured particles to \( P_i \). However, he will inevitably be detected by the security check process in Step 3, as this attack alters the states of decoy photons chosen from the set \( T_2 \). As a result, TP2 has no chance to obtain the state of \( |k_i\rangle \). It can be concluded that TP2 cannot know the secret integer of \( P_i \).

3 The proposed MQPC protocol for size relation comparison with one semi-honest TP

3.1 Protocol description

Assume that the party \( P_i \) has the secret integer \( s_i \), where \( i = 1, 2, ..., n \). And \( n \) parties share a key (i.e., \( C \)) beforehand through the BB84 QKD protocol \([1]\), where \( C \) is a constant. There is a natural number \( r \) satisfying \( r > \{s_i\}_{\text{max}}, r > C \) and \( d \geq 3r - 1 \). The \( n \) parties execute the following steps to complete the aim of size relation comparison with the help of one semi-honest TP. Same to the protocol in Sect. 2.1, TP is semi-honest also in the sense that she may misbehave on her own but is not allowed to conspire with anyone else.

**Step 1:** TP prepares \( n \) single particles, \( |k_1\rangle, |k_2\rangle, ..., |k_n\rangle \), which are randomly chosen from the set \( T_1 \). It should be ensured that \( k_i + k_i’ = K \). Here, \( k_i \in \{0, 1, ..., r - 1\}, k_i’ \in \{0, 1, ..., d - 1\}, i = 1, 2, ..., n \) and \( K \) is a constant. Note that only TP knows the genuine value of \( K \).

**Step 2:** TP prepares \( n \) groups of \( l \) decoy photons, which are denoted as \( G_1, G_2, ..., G_n \), respectively. Here, each decoy photon is one of the states randomly chosen from the set \( T_1 \) or \( T_2 \). Afterward, TP inserts the particle \( |k_i\rangle \) into \( G_i \) at random positions to construct a new sequence \( G_i’ \). Finally, TP sends \( G_i’ \) to \( P_i \), where \( i = 1, 2, ..., n \).

**Step 3:** After confirming that \( P_i (i = 1, 2, ..., n) \) has received all particles, TP and \( P_i \) check the security of the transmission of \( G_i’ \). Concretely, TP announces the positions and the preparation bases of decoy photons to \( P_i \). According to the announced information, \( P_i \) uses the right bases to measure the corresponding decoy photons and returns the measurement results to TP. Afterward, by comparing the measurement results of decoy photons with their corresponding initial prepared states, TP can check whether the transmission of \( G_i’ \) is secure or not. If it is secure, the protocol will proceed to the next step; otherwise, the protocol will be terminated and restarted from Step 1.

**Step 4:** After removing the decoy photons in \( G_i’ (i = 1, 2, ..., n) \), in order to encode her secret integer \( s_i \), \( P_i \) performs the operation \( U_{s_i + C} = \sum_{k=0}^{d-1} |k + s_i + C\rangle\langle k| \) on the particle \( |k_i\rangle \) to obtain the state \( |k_i + s_i + C\rangle \). It should be pointed out that \( k_i + s_i + C < d \). Afterward, \( P_i \) prepares a quantum state sequence \( G_i'' \) composed of \( l \) decoy photons. Here, each decoy photon is also one of the states randomly chosen from the set \( T_1 \) or
Then, $P_i$ inserts the particle $|k_i + s_i + C\rangle$ into $G''_i$ at random positions to construct a new sequence $G'''_i$. Finally, $P_i$ sends $G'''_i$ to TP.

**Step 5:** After confirming that TP has received all particles, $P_i (i = 1, 2, \ldots, n)$ and TP check the security of the transmission of $G'''_i$. Firstly, $P_i$ announces the positions and the preparation bases of decoy photons which are chosen from the set $T_2$. According to the announced information, TP uses the right bases to measure the corresponding decoy photons and returns the measurement results to $P_i$. Then, by comparing the measurement results of decoy photons with their corresponding initial prepared states, $P_i$ can calculate the error rate. If the error rate is greater than the threshold value, the protocol will be terminated and restarted from Step 1; otherwise, the protocol will proceed to the next step.

**Step 6:** TP drops out the decoy photons in $G'''_i (i = 1, 2, \ldots, n)$ which are chosen from the set $T_2$. For the remaining particles on the site of TP, $P_i$ tells TP the positions and the preparation bases of decoy photons which are chosen from the set $T_1$. Afterward, TP uses the right bases to measure the corresponding decoy photons and returns the measurement results to $P_i$. Then, by comparing the measurement results of decoy photons with their corresponding initial prepared states, $P_i$ can calculate the error rate. If the error rate is greater than the threshold value, the protocol will be terminated and restarted from Step 1; otherwise, the protocol will proceed to the next step.

**Step 7:** TP uses the correct base to measure the particle $|k_i + s_i + C\rangle$ ($i = 1, 2, \ldots, n$) and obtains the value of $k_i + s_i + C$. Then, TP calculates the sum of $k_i + s_i + C$ and $k'_i$, i.e., $M_i = k_i + s_i + C + k'_i$. Because both $k_i + k'_i = K$ and $C$ are constant, the size relation of different $M_i$s is the same to that of different $s_i$s. As a result, TP can know the size relation of different $s_i$s, but cannot know the genuine value of $s_i$ due to lack of knowledge about $C$. Finally, TP announces the size relation of different $M_i$s through the classical channel. According to the announced information, $P_i$ can know the size relation of different $s_i$s.

Now it concludes the description of the proposed MQPC protocol with one TP. For clarity, we further show its flow chart in Fig. 2, taking TP and $P_i$ for example, after ignoring the security check processes.

### 3.2 Security analysis

In this subsection, we analyze the security of the proposed MQPC protocol with one TP by concentrating on the participant attack, since its security analysis on the outside attack is extremely similar to that of the proposed protocol with two TPs. In the
following, we show that one or more parties cannot learn other parties’ secret integers. Moreover, the semi-honest TP cannot learn these parties’ secrets either.

Case 1: The participant attack from one or more dishonest parties

Two situations should also be considered in this case. One is that one dishonest party wants to steal other parties’ secret integers; the other one is that two or more dishonest parties conclude together to steal other parties’ secret integers.

(a) The participant attack from one dishonest party

It is apparent that in the proposed MQPC protocol with one TP, the roles of \( n \) parties are the same. Without loss of generality, in this situation, we suppose that \( P_1 \) is the only dishonest party who wants to steal other parties’ secret integers.

In the proposed MQPC protocol with one TP, there are qudits transmitted from TP to \( P_j \) (\( j = 2, 3, \ldots, n \)) in Step 2 and from \( P_j \) to TP in Step 4. In order to obtain the secret integer of \( P_j \), when \( P_1 \) tries to launch her attacks on the transmitted particles from TP to \( P_j \) in Step 2 or from \( P_j \) to TP in Step 4, she essentially acts as an outside eavesdropper. As analyzed in Sect. 2.2.1, she will inevitably be caught if she launches her attacks, as she has no knowledge about the positions and the preparation bases of transmitted decoy photons.

In addition, in Step 7, \( P_1 \) may hear of the comparison result of size relation from TP. However, this information is still helpless for her to obtain the secret integer of \( P_j \).

It can be concluded now that one dishonest party cannot obtain other parties’ secret integers.

(b) The participant attack from two or more dishonest parties

If the number of dishonest parties concluding together is \( n-1 \), the dishonest parties will be the most powerful. Here, we only consider this extreme case. Without loss of generality, suppose that the dishonest \( P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n \) collude together to get the secret integer of \( P_m \).

If \( P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n \) try to launch their attacks on the transmitted particles from TP to \( P_m \) in Step 2 or from \( P_m \) to TP in Step 4, as analyzed in Sect. 2.2.1, they will inevitably be detected as an outside eavesdropper, since they have no knowledge about the positions and the preparation bases of transmitted decoy photons.

In addition, in Step 7, \( P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n \) may hear of the comparison result of size relation from TP. However, this information is still helpless for them to obtain the secret integer of \( P_m \).

It can be concluded now that the dishonest \( P_1, P_2, \ldots, P_{m-1}, P_{m+1}, \ldots, P_n \) cannot get the secret integer of \( P_m \). It is straightforward that the colluding attack from two or more dishonest parties is invalid for them to steal the secret integers from other parties.

Case 2: The participant attack from semi-honest TP

In Step 1, TP knows the states of \( |k_1\rangle, |k_2\rangle, \ldots, |k_n\rangle \) and the values of \( k_1', k_2', \ldots, k_n' \).

In Step 7, TP obtains \( k_i + s_i + C \) (\( i = 1, 2, \ldots, n \)) by measuring the state of \( |k_i + s_i + C\rangle \), calculates the sum of \( k_i + s_i + C \) and \( k_i' \), and compares the size relation of secret integers from \( n \) parties. However, she still cannot infer out the secret integer of \( P_i \) from this information, as she has no chance to know the pre-shared key (i.e., \( C \)) of \( P_i \).
|                                | The protocol of Ref. [50] | The protocol of Ref. [51] | The protocol of Ref. [52] | The proposed protocol with two TPs | The proposed protocol with one TP |
|--------------------------------|---------------------------|---------------------------|---------------------------|-----------------------------------|----------------------------------|
| Quantum state                  | $d$-level two-particle Bell state | $d$-level two-particle Bell state | $d$-level single-particle state | $d$-level single-particle state | $d$-level single-particle state |
| Number of parties              | 2                         | 2                         | 2                         | $n$                               | $n$                              |
| Pre-shared QKD key             | Yes                       | Yes                       | Yes                       | Yes                               | Yes                              |
| Number of times to compare $n$ parties | $n - 1 \sim \frac{n(n-1)}{2}$ | $n - 1 \sim \frac{n(n-1)}{2}$ | $n - 1 \sim \frac{n(n-1)}{2}$ | 1                                 | 1                                |
| Type of TP                     | The second semi-honest model of TP | The second semi-honest model of TP | The second semi-honest model of TP | The second semi-honest model of TP | The second semi-honest model of TP |
| Quantum measurement for TP     | No                        | $d$-level two-particle Bell state measurement | No                        | $d$-level single-particle measurement | $d$-level single-particle measurement |
| Quantum measurement for parties| $d$-level single-particle measurement | $d$-level two-particle Bell state measurement | $d$-level single-particle measurement | No                                | No                               |
| Comparison of size relation    | Yes                       | Yes                       | Yes                       | Yes                               | Yes                              |
| Quantum technology used        | Quantum fourier transform and unitary operation | Quantum entanglement swapping and unitary operation | Quantum fourier transform and unitary operation | Unitary operation | Unitary operation |
| Protocol of Ref. | Quantum state | Quantum measurement for TP | Quantum measurement for parties | Number of parties | Quantum technology used | Type of TP | Comparison of size relation | Pre-shared QKD key | Number of times to compare $n$ parties |
|------------------|---------------|--------------------------|-------------------------------|------------------|------------------------|-----------|----------------------------|------------------|-------------------------------|
| [53]             | $n$-particle GHZ class state | No | Single-particle measurement | $n$ | The entanglement correlation among different particles from one quantum entangled state | The first kind of semi-honest TP | No | No | 1 |
| [54]             | $d$-level $n$-particle entangled state | $d$-level single-particle measurement | No | $n$ | Quantum fourier transform and unitary operation | The first kind of semi-honest TP | No | No | 1 |
| [55] - A         | $d$-level $n$-particle entangled state and $d$-level two-particle entangled state | $d$-level single-particle measurement | $d$-level single-particle measurement | $n$ | Quantum fourier transform | The second semi-honest model of TP | No | No | 1 |
| [55] - B         | $d$-level two-particle entangled state | $d$-level two-particle collective measurement | No | $n$ | Unitary operation | The second semi-honest model of TP | No | Yes | 1 |
| [56]             | $d$-level $n+1$ -particle cat state and $d$-level two-particle Bell state | $d$-level $n+1$ -particle cat state measurement | $d$-level two-particle Bell state measurement | $n$ | Quantum entanglement swapping and unitary operation | The second semi-honest model of TP | No | No | 1 |
| [57]             | $d$-level $l$-particle entangled state | No | $d$-level single-particle measurement | $n$ | The entanglement correlation among different particles from one quantum entangled state | The second semi-honest model of TP | Yes | Yes | 1 |
| Quantum state                          | Quantum measurement for TP | Quantum measurement for parties | Number of parties | Quantum technology used | Type of TP | Comparison of size relation | Pre-shared QKD key | Number of times to compare $n$ parties |
|---------------------------------------|----------------------------|---------------------------------|-------------------|-------------------------|------------|-------------------------------|-------------------|---------------------------------------|
| The protocol of Ref. [58]             | $d$-level $n$-particle GHZ state and $l$-level $n$-particle GHZ state | $d$-level single-particle measurement | $n$                | Unitary operation       | Yes        | No                            | 1                 |
| The proposed MQPC protocol with two TPs| $d$-level single-particle state | $d$-level single-particle measurement | No                 | Unitary operation       | Yes        | Yes                           | 1                 |
| The proposed MQPC protocol with one TP | $d$-level single-particle state | $d$-level single-particle measurement | No                 | Unitary operation       | Yes        | Yes                           | 1                 |
4 Discussion and conclusion

Firstly, we compare the proposed MQPC protocols with the QPC protocols of Refs. [50–52] without considering the security check processes. Table 1 clearly shows that the performance of the proposed MQPC protocols has advantages over the protocols of Refs. [50–52]. For example, in the protocols of Refs. [50–52], in order to complete the whole size relation comparisons for \( n \) parties, TP has to execute the same protocol \( x \) times, where \( x = (n - 1) \) to \( \frac{n(n-1)}{2} \). Accordingly, in the optimal case, TP can complete the whole size relation comparisons within \( n - 1 \) times execution, and in the worst case, TP has to execute the protocol \( \frac{n(n-1)}{2} \) times. However, the proposed MQPC protocols can complete the whole size relation comparisons for \( n \) parties within one execution.

Secondly, we compare the proposed MQPC protocols with the MQPC protocol of Refs. [53–58] without considering the security check processes. Note that there are two MQPC protocols in Ref. [55], which are denoted as Ref. [55] -A and Ref. [55]-B, respectively. In the protocols of Refs. [53–56], TP can only compare all parties’ secrets for equality, while in the protocols of Refs. [57, 58] and the proposed MQPC protocols, TP can compare the size relation of all parties’ secrets. In addition, the proposed MQPC protocols just need \( d \)-level single-particle states as quantum resource, while all of other MQPC protocols listed in Table 2 employ \( d \)-level entangled states as quantum resource. As the preparation of \( d \)-level single-particle states is much easier than that of \( d \)-level entangled states, the proposed MQPC protocols exceed other MQPC protocols listed in Table 2 on the aspect of quantum resource.

In summary, in this paper, by using \( d \)-level single-particle states, we propose two novel MQPC protocols for size relation comparison with two semi-honest TPs and one semi-honest TP, respectively, where each TP may misbehave on her own but is not allowed to collude with anyone else. Each of the proposed MQPC protocol can compare the size relation of secret integers from \( n \) parties rather than just the equality within one time execution of the protocol. We validate in detail that the proposed MQPC protocols can resist both the outside attack and the participant attack. Specially, each party has no chance to know other parties’ secret integers, and the TPs also have no knowledge about each party’s secret integer. As there are no communication and no pre-shared key between each pair of party, the proposed MQPC protocol with two TPs is workable in a stranger environment, such as anonymous bidding and auction, where any two bidders are strange or want to keep their identities secret to each other. The proposed MQPC protocol with one TP is workable in an acquaintance environment, as all parties need to share a common private key beforehand.

Acknowledgments The authors would like to thank the anonymous reviewers for their valuable comments that help enhancing the quality of this paper. Funding by the National Natural Science Foundation of China (Grant No. 61402407) and the Natural Science Foundation of Zhejiang Province (Grant No. LY18F020007) is gratefully acknowledged.
References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, pp. 175–179 (1984)

2. Ekert, A.K.: Quantum cryptography based on bells theorem. Phys. Rev. Lett. 67(6), 661–663 (1991)

3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121–3124 (1992)

4. Cabello, A.: Quantum key distribution in the Holevo limit. Phys. Rev. Lett. 85(26), 5635 (2000)

5. Hwang, W.Y.: Quantum key distribution with high loss: toward global secure communication. Phys. Rev. Lett. 91(5), 057901 (2003)

6. Li, X.H., Deng, F.G., Zhou, H.Y.: Efficient quantum key distribution over a collective noise channel. Phys. Rev. A 78(2), 022321 (2008)

7. Zhang, C.M., Song, X.T., Treeviriyanupap, P., et al.: Delayed error verification in quantum key distribution. Chin. Sci. Bull. 59(23), 2825–2828 (2014)

8. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys. Rev. A 68(4), 042317 (2003)

9. Gu, B., Huang, Y.G., Fang, X., Zhang, C.Y.: A two-step quantum secure direct communication protocol with hyperentanglement. Chin. Phys. B 20(10), 100309 (2011)

10. Wang, J., Zhang, Q., Tang, C.J.: Quantum secure direct communication based on order rearrangement of single photons. Phys. Lett. A 358(4), 256–258 (2006)

11. Hillery, M., Buzek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59(3), 1829–1834 (1999)

12. Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys. Rev. A 59(1), 162–168 (1999)

13. Cleve, R., Gottesman, D., Lo, H.K.: How to share a quantum secret. Phys. Rev. Lett. 83(3), 648–651 (1999)

14. Gottesman, D.: Theory of quantum secret sharing. Phys. Rev. A 61(4), 042311 (2000)

15. Li, Y., Zhang, K., Peng, K.: Multiparty secret sharing of quantum information based on entanglement swapping. Phys. Lett. A 324(5), 420–424 (2004)

16. Xiao, L., Long, G.L., Deng, F.G., et al.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A 69(5), 052307 (2004)

17. Deng, F.G., Long, G.L., Zhou, H.Y.: An efficient quantum secret sharing scheme with Einstein–Podolsky–Rosen pair block. Phys. Lett. A 340(1–4), 43–50 (2005)

18. Wang, T.Y., Wen, Q.Y., Chen, X.B., et al.: An efficient and secure multiparty quantum secret sharing scheme based on single photons. Opt. Commun. 281(24), 6130–6134 (2008)

19. Guo, G.P., Guo, G.C.: Quantum secret sharing without entanglement. Phys. Lett. A 310(4), 247–251 (2003)

20. Markham, D., Sanders, B.C.: Graph states for quantum secret sharing. Phys. Rev. A 78(4), 042309 (2008)

21. Keet, A., Fortescue, B., Markham, D., et al.: Quantum secret sharing with qudit graph states. Phys. Rev. A 82(6), 062315 (2010)

22. Bouwmeester, D., Pan, J.W., Mattle, K., Eibl, M., Weinfurter, H., Zeilinger, A.: Experimental quantum teleportation. Nature 390(6660), 575–579 (1997)

23. Zhang, Z.J., Liu, Y.M., Zhang, Z.Y., Zhang, W., Zhang, Z.J.: Many-agent controlled teleportation of multi-qubit quantum information via quantum entanglement swapping. Commun. Theor. Phys. 44(5), 847–849 (2005)

24. Yin, X.F., Liu, Y.M., Man, Z.Y., Zhang, Z.J.: Perfect teleportation of an arbitrary three-qubit state with the highly entangled six-qubit genuine state. Sci. China Phys. Mech. Astron. 53(11), 2059–2063 (2010)

25. Jakobi, M., Simon, C., Gisin, N., et al.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A 83, 022301 (2011)

26. Gao, F., Liu, B., Huang, W., Wen, Q.Y.: Postprocessing of the oblivious key in quantum private query. IEEE J. Sel. Top. Quantum Electron. 21, 6600111 (2015)

27. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A 93, 042318 (2016)

28. Wei, C.Y., Cai, X.Q., Liu, B., et al.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. 67, 2–8 (2018)
29. Yao, A.C.: Protocols for secure computations. In: Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS’82), Washington, DC, p. 160 (1982)
30. Boudot, F., Schoenmakers, B., Traore, J.: A fair and efficient solution to the socialist billionaires’ problem. Discret Appl. Math. 111(1–2), 23–36 (2001)
31. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decay photons and two-photon entanglement. J. Phys. A: Math. Theor. 42, 055305 (2009)
32. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. 283, 1561 (2010)
33. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. 80, 065002 (2009)
34. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. 57, 583–588 (2012)
35. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. 11, 373–384 (2012)
36. Yang, Y.G., Xia, J., Jia, X., Shi, L., Zhang, H.: New quantum private comparison protocol without entanglement. Int. J. Quantum Inf. 10, 1250065 (2012)
37. Zi, W., Guo, F.Z., Luo, Y., Cao, S.H., Wen, Q.Y.: Quantum private comparison protocol with the random rotation. Int. J. Theor. Phys. 52, 3212–3219 (2013)
38. Liu, B., Gao, F., Jia, H.Y., Huang, W., Zhang, W.W., Wen, Q.Y.: Efficient quantum private comparison employing single photons and collective detection. Quantum Inf. Process. 12, 887–897 (2013)
39. Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int. J. Quantum Inf. 11, 1350039 (2013)
40. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semi-honest third party. Quantum Inf. Process. 12, 877–885 (2013)
41. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. 12, 1981–1990 (2013)
42. Chen, X.B., Su, Y., Niu, X.X., Yang, Y.X.: Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. Quantum Inf. Process. 13, 101–112 (2014)
43. Li, J., Zhou, H.F., Jia, L., Zhang, T.T.: An efficient protocol for the private comparison of equal information based on four-particle entangled W state and Bell entangled states swapping. Int. J. Theor. Phys. 53(7), 2167–2176 (2014)
44. Liu, X.T., Zhang, B., Wang, J., Tang, C.J., Zhao, J.J.: Differential phase shift quantum private comparison. Quantum Inf. Process. 13, 71–84 (2014)
45. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. 52, 212–218 (2013)
46. Lin, S., Guo, G.D., Liu, X.F.: Quantum private comparison of equality with $\chi$-type entangled states. Int. J. Theor. Phys. 52, 4185–4194 (2013)
47. Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W States. Int. J. Theor. Phys. 53(5), 1723–1729 (2014)
48. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. 65, 711–715 (2016)
49. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A 56(2), 1154–1162 (1997)
50. Lin, S., Sun, Y., Liu, X.F., Yao, Z.Q.: Quantum private comparison protocol with $d$-dimensional Bell states. Quantum Inf. Process. 12, 559–568 (2012)
51. Guo, F.Z., Gao, F., Qin, S.J., Zhang, J., Wen, Q.Y.: Quantum private comparison protocol based on entanglement swapping of $d$-level Bell states. Quantum Inf. Process. 12, 2793–2802 (2013)
52. Yu, C.H., Guo, G.D., Lin, S.: Quantum private comparison with $d$-level single-particle states. Phys. Scr. 88, 065013 (2013)
53. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. 12, 1077–1088 (2013)
54. Liu, W., Wang, Y.B., Wang, X.M.: Multi-party quantum private comparison protocol using $d$ dimensional basis states without entanglement swapping. Int. J. Theor. Phys. 53, 1085–1091 (2014)
55. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with $n$-level entangled states. Quantum Inf. Process. 13, 2375–2389 (2014)
56. Ji, Z.X., Ye, T.Y.: Multi-party quantum private comparison based on the entanglement swapping of $d$-level cat states and $d$-level Bell states. Quantum Inf. Process. 16(7), 177 (2017)
57. Luo, Q.B., Yang, G.W., She, K., Niu, W.N., Wang, Y.Q.: Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. 13, 2343–2352 (2014)
58. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum Inf. Process. 14(11), 4225–4235 (2015)
59. Hung, S.M., Hwang, S.L., Hwang, T., Kao, S.H.: Multiparty quantum private comparison with almost dishonest third parties for strangers. Quantum Inf. Process. 16(2), 36 (2017)
60. Li, C.Y., Zhou, H.Y., Wang, Y., Deng, F.G.: Secure quantum key distribution network with Bell states and local unitary operations. Chin. Phys. Lett. 22(5), 1049 (2005)
61. Li, C.Y., Li, X.H., Deng, F.G., Zhou, P., Liang, Y.J., Zhou, H.Y.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. 23(11), 2896 (2006)
62. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85(2), 441 (2000)
63. Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin. Phys. Lett. 24(1), 19 (2007)
64. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin. Phys. Lett. 30(4), 040305 (2013)
65. Cai, Q.Y.: Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys. Lett. A 351(1–2), 23–25 (2006)
66. Deng, F.G., Zhou, P., Li, X.H., Li, C.Y., Zhou, H.Y.: Robustness of two-way quantum communication protocols against Trojan horse attack. http://arxiv.org/abs/quant-ph/0508168 (2005)
67. Li, X.H., Deng, F.G., Zhou, H.Y.: Improving the security of secure direct communication based on the secret transmitting order of particles. Phys. Rev. A 74, 054302 (2006)
68. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145–195 (2002)
69. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. 7, 329 (2007)
70. Gao, F., Wen, Q.Y., Zhu, F.C.: Comment on: “quantum exam” [Phys. Lett. A 350 (2006) 174]. Phys. Lett. A 360(6), 748–750 (2007)
71. Guo, F.Z., Qin, S.J., Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: Participant attack on a kind of MQSS schemes based on entanglement swapping. Eur. Phys. J. D 56(3), 445–448 (2010)
72. Qin, S.J., Gao, F., Wen, Q.Y., Zhu, F.C.: Cryptanalysis of the Hillery–Buzek–Berthiaume quantum secret-sharing protocol. Phys. Rev. A 76(6), 062324 (2007)