Quantum Information Processing (2021) 20:178
https://doi.org/10.1007/s11128-021-03084-2

Novel two-party quantum private comparison via quantum walks on circle

Feng-Lin Chen[1] · Hai Zhang[1] · Su-Gen Chen[1] · Wen-Tao Cheng[1]

Received: 14 March 2020 / Accepted: 25 March 2021 / Published online: 8 May 2021

Abstract
The quantum private comparison aims to make the size comparison of two participants' private information without leaking the private data of their own with quantum mechanism. In this paper, different from the current method of using single particle or entangled state as the information carrier, a novel two-party quantum private comparison protocol is firstly proposed via quantum walks on circle. In the protocol, a third party is assumed to be semi-honest and allowed to misbehave on his own, but cannot conspire with either of the two dishonest participants and obtain the participants' private information. The protocol adopts the two-particle quantum walks state on circle rather than entangled state as the initial quantum resource and only needs measurement and quantum walks operator without the unitary operation and quantum entanglement swapping. The two-particle state is transferred as a whole among different parties, which reduces the protocol complexity and avoids the chance of being attacked. It can implement the equality comparison of private information, but also the size comparison. Security analyses show that this protocol is resistant to the external and internal malicious attacks, which can also determine the disputes over the judgment result of the third party. Compared with other quantum private comparison protocols, the proposed protocol has better flexibility and universality.

Keywords Quantum private comparison · Discrete-time quantum walks · Shift operator on circle · Security analysis

1 Introduction

The problem of secure multi-party computation (SMPC) was proposed by Yao [1] in 1982. The scenario is the millionaire problem: with the premise of not disclosing oneself's property status, how can the two millionaires compare who is richer without

✉ Feng-Lin Chen
chenfenglin@aqnu.edu.cn

[1] School of Mathematics and Physics, Anqing Normal University, Anqing 246133, China

a trusted third party. As a sub-field of cryptography, SMPC protocol allows multiple participants holding their own private data to perform collaborative computing under the condition of mutual distrust, cooperate to complete the function computing task (e.g., maximum computing), output the computing results, and ensure that no one can get any further information except the deserved computing results. Each involved party will not disclose its own data. SMPC plays an important role in electronic election, electronic voting, electronic auction, secret sharing, threshold signature and other scenarios. The theories and technologies of SMPC meet the needs of security computing in many cutting-edge fields, such as privacy protection, block-chain, machine learning.

Google researchers published the latest research results [2] in quantum computing and showed that its latest sycamore processor can accomplish the test computing in just 200 seconds, compared with the time of 10,000 years needed by the largest supercomputer in the world. The paper declared that Google has achieved the so-called quantum supremacy. It further warned that the classical cryptography algorithm based on difficult mathematical problem will be challenged by the threat of quantum computer technology. The quantum no-cloning theorem and Heisenberg uncertainty principle are the natural protective shields of quantum communication. Therefore, it is urgent to develop and study quantum cryptography based on quantum mechanism. Many scholars have since been devoted to the study of quantum SMPC. Quantum SMPC is the extension of classical one to quantum system. In 2017, Qiang et al. [3] proposed and implemented a quantum SMPC scheme based on the linear combination of unitary approach which was firstly proposed in [4]. The distributed secure quantum machine learning (DSQML) enables a classical client to delegate a remote quantum machine learning to the quantum server with the privacy data preserved. In 2017, Sheng and Zhou proposed a DSQML protocol which can be used to classify high-dimensional vectors and may provide a new viewpoint and application for future "big data."

As a branch of quantum SMPC protocol, quantum private comparison (QPC) has attracted extensive attentions in recent years. The so-called QPC aims to determine whether the two participants' private inputs are equal or not without disclosing each real secret contents. However, in 1997, Lo [5] pointed that it is impossible to construct a secure equality function in the two-party scenario, even in quantum methods. Therefore, some additional assumptions should be considered to make private comparison, and the existence of the third party (TP) is necessary. According to the reliability of the TP, there are three kinds of TP in the current QPC protocols, namely the completely honest, the dishonest and the semi-honest TP. In the real QPC environments, the first and second types are difficult, unreasonable or irrational to implement. For the semi-honest type, the TP is allowed to misbehave on its own. However, he cannot conspire with other participants. Without difficulty, this assumption of semi-honest TP is more reasonable in QPC protocols. As we know, it is the best assumption about the TP up to now.

In 2009, Yang and Wen [6] first presented an efficient two-party QPC protocol for comparing information of equality with decoy particles and Bell entanglement state. In the past decade, a large number of QPC protocols [6–58] using different technologies as private information carriers have emerged. If we distinguish by the number of participants in private comparison about these proposed protocols, we can divide them into two categories, namely two-party protocols and multi-party ones. Besides the two-party QPC protocols [6–42], many multi-party QPC protocols [43–58] have also been suggested. According to the number of carrier particles that transmit the private information of participants, the QPC protocols can be classified as single-particle ones and multi-particle entangled ones. The typical QPC protocols of single particle are mainly seen in [7–12,43–47]. Instead of using single particle to carry the private information, most QPC protocols use multi-particle entangled states as the message bridge, so as to achieve the private comparison of information. At present, most QPC protocols are of this type, such as protocols using Bell states [13–23,48–51], GHZ states [24–29,52–55], four-particle cluster states [30–32], four-particle χ-type entangled states [33–37], four-particle W states [38] and more than five particles entangled states [39–42,56–58]. The original concept of QPC is proposed to solve the wealth equality problem of the two millionaires without disclosing their real wealth. In fact, so far most of the proposed QPC protocols are about equality comparison ones. These protocols in [7–9,11–17,21–25,27–43,45,47–52,55–58] are typical examples of equality QPC protocols. If the private information of the participants is in a large range, the equality is an event with little probability. Thus, we think that the size comparison is more meaningful than the equality comparison. However, compared with the QPC protocols of the equality comparison, so far, the QPC protocols of the size comparison [10,18–20,26,44,46,53,54] are very few.

Random walks are introduced to describe the behavior of a walker over some path, such as a line, lattice, circle or graph. With a priori fixed probability, the walker can choose to follow one of the possible directions. Quantum walks (QWs) are the quantum mechanical analogs of classical random walks. In quantum scenario, the quantum state of the walker is given by a superposition of positions. In 1993, QWs were first introduced by Aharonov et al. [59]. There are two basic variants model of QWs: discrete-time [59] and continuous-time ones [60]. In recent years, QWs has provided some effective ideas in solving many practical problems, such as the element distinctness problem [61], the triangle finding in an undirected graph [62], the graph isomorphism problem [63], the quantum spatial search [64], the quantum network communication [65], the generalized quantum measurement [66], the perfect state transfer (PST) [67,68], the quantum lumped element router [69], the quantum cryptographic system [70,71], the quantum information splitting [72], and the quantum generalized teleportation [73,74].

From the above analysis, we can see that all the multi-particle QPC protocols adopted the quantum entangled states. For these protocols with the entangled states as private information carrier, the first important task is to distribute entangled particles among participants. In this process, it is a rather challenging task to ensure the reliable and safe transmission of distributed particles through quantum channels without attacks. Although the current level of quantum technology can achieve quantum entanglement in the laboratory to some extent, there are still many practical difficulties in large-scale realization, especially multi-particle quantum entanglement. As far as we know, QWs technology has not been used to implement the QPC. In this paper, we firstly propose an efficient two-party QPC protocol via QWs on circle. This protocol can fully meet the definition and security requirements about QPC. Because we do not prepare the entangled particles in advance, and the comparison of private information is one-time rather than bit-by-bit, our protocol is efficient. At the same time, our protocol can realize the size comparison of private information, not only the equality comparison, so it is more practical.

The rest of this paper is organized as follows: In Sect. 2, we introduce some basic notations and results about QWs on circle. In Sect. 3, the proposed QPC protocol is described in detail. In Sect. 4, we prove its correctness, analyze its security, and compare it with other QPC protocols. Finally, a brief concluding summary is given in Sect. 5.

2 QWs on circle

In discrete-time QWs system, the walker hops along discrete positions on a line, circle [70,71] or graph [75]. Here, we focus on the QWs on line and circle and review some basics on them. At each step, the walker particle moves to another position depending on the coin state. The QWs Hilbert space $\mathcal{H}$ is the tensor product of the walker's positions space $\mathcal{H}_p$ and the coin space $\mathcal{H}_c$, and is consequently defined as $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$. Each step evolution of the QWs is described by the unitary operator

$$U = S(I_p \otimes R_c), \tag{1}$$

where I_p is the identity operator on walker space $\mathcal{H}_p$, R_c is the coin operator on coin space $\mathcal{H}_c$, and S is the shift operator. In general, the R_c is

$$R_c = R_c(\theta, \xi, \zeta) = \begin{pmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ -e^{-i\zeta}\sin\theta & e^{-i\xi}\cos\theta \end{pmatrix}. \tag{2}$$

If we choose the parameters with $\xi = 0$, $\zeta = 0$ and $\theta = \frac{\pi}{4}$, the coin operator R_c will turn into the familiar Hadamard gate transformation $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{|0\rangle\langle 0|+|1\rangle\langle 0|+|0\rangle\langle 1|-|1\rangle\langle 1|}{\sqrt{2}}$.

In the case of QWs on line, the shift operator S can be written as:

$$S = \sum_{i\in Z}(|i+1\rangle\langle i| \otimes |0\rangle\langle 0| + |i-1\rangle\langle i| \otimes |1\rangle\langle 1|), \tag{3}$$

where the label i denotes the discrete position on line. When a line is joined end to end, it becomes a circle. For the q nodes of positions labeled from 0 to $q-1$ on circle, if we define the m-position operator

$$T_m = \sum_{i=0}^{q-1} |(i+m)mod\, q\rangle\langle i|, \tag{4}$$

then the general shift operator S of the QWs on circle can be expressed as:

$$S = T_1 \otimes |0\rangle\langle 0| + T_{-1} \otimes |1\rangle\langle 1|. \tag{5}$$

Suppose that the initial quantum state of the QWs is $|\phi_0\rangle = |w_0\rangle|c_0\rangle$, the final quantum state after l steps of QWs is

$$|\phi\rangle_l = U^l |w_0\rangle|c_0\rangle. \tag{6}$$

The probability at position $i \in [0, q-1]$ after l steps walks is

$$p(x, l) = \sum_{i \in \{0,1\}} |\langle i, x|\phi\rangle_l|^2. \tag{7}$$

The inverse evolution of the QWs is described by the unitary operator U^{-1}, i.e.,

$$U^{-1} = (S(I_p \otimes R_c))^{-1} = (I_p \otimes R_c^{-1})S^{-1}. \tag{8}$$

When the shift operator S refers to (5) on circle, its inverse shift operator is

$$S^{-1} = T_{-1}| \otimes |0\rangle\langle 0| + T_1| \otimes |1\rangle\langle 1|. \tag{9}$$

This conclusion can be deduced as follows:

$$\begin{aligned} SS^{-1} &= (T_1 \otimes |0\rangle\langle 0| + T_{-1} \otimes |1\rangle\langle 1|) \\ &\quad \times (T_{-1} \otimes |0\rangle\langle 0| + T_1 \otimes |1\rangle\langle 1|) \\ &= (T_1 T_{-1}) \otimes |0\rangle\langle 0| + (T_{-1} T_1) \otimes |1\rangle\langle 1| \\ &= I_q \otimes |0\rangle\langle 0| + I_q \otimes |1\rangle\langle 1| \\ &= I_q \otimes I_2 \\ &= I_{q+2}. \end{aligned}$$

According to the above definitions and conclusions, it is easy to prove that $U^{-1}|\phi\rangle_{l+1} = U^{-1}(U|\phi\rangle_l) = |\phi\rangle_l$. We can also generalize the conclusion

$$U^{-t}|\phi\rangle_{l+t} = |\phi\rangle_l \tag{10}$$

after t steps of the inverse QWs.

3 The proposed QPC protocol

In the proposed protocol, we give five assumptions. The first one is that the arbitrator TP is semi-honest. The second one is that all participants always adopt the coin operator R_c as H in the evolution of the QWs. The third one is that the number q of positions on circle must be an odd integer. This assumption ensures that there exists some

Table 1 Main symbols in the proposed protocol

Symbol	Meaning
q	Public odd integer of positions on circle
k	Copies number of quantum state, a predetermined security threshold
f	Secret steps of TP's QWs on circle
g	Secret steps of Alice's QWs on circle
m_1	Alice's private message, $m_1 \in [0, \frac{q-1}{2}]$
m_2	Bob's private message, $m_2 \in [0, \frac{q-1}{2}]$
m_3'	TP's measurement result with the basis $\{\|0\rangle, \|1\rangle, \ldots, \|q-1\rangle\}$, $m_3' \in [0, q-1]$
$\|\phi\rangle_f$	Quantum state after TP's f steps of QWs
$\|\varphi\rangle_{m_1}$	Quantum state after Alice's m_1 steps of position operator
$\|\chi\rangle_g$	Quantum state after Alice's g steps of QWs
$\|\psi\rangle_{m_2}$	Quantum state after Bob's m_2 steps of inverse position operator
$\|\omega\rangle_{f+g}$	Quantum state after TP's $f+g$ steps of inverse QWs

probability of the existence in every position for the walker after the $(q-1)$ steps walks on circle. If q is an even integer, then there are only $\frac{q}{2}$ possible positions on which the walker can hop. The fourth assumption is that the range of the participants' private information is from 0 to $\frac{q-1}{2}$. We assume that the quantum channel is in an ideal situation, so the influence of noise (such as the bit error and the phase error) on the channel will not be considered. This is the fifth assumption in the proposed QPC protocol.

In order to describe the proposed protocol clearly, we list the main symbols in Table 1.

3.1 The process of protocol

In short, a prepared two-particle QWs state is first prepared by TP and transformed to the participant Alice. After Alice's QWs evolution and her private information embedded, the QWs state is passed to participant Bob. Then, Bob embeds his private information in the QWs state and passes it to TP. With Alice's public parameter, TP final recovers the size comparison of the participants' private information with the QWs evolution and the measurement results on the two disentangled particles.

Step 1 TP's initialization

Suppose that the initial position state of walker in the QWs system is $|w_0\rangle \in \{|0\rangle, |1\rangle, \ldots |q-1\rangle\}$, and the initial state of coin is $|c_0\rangle \in \{|0\rangle, |1\rangle\}$, where the two parameters, $w_0 \in \{0, 1, \ldots, q-1\}$ and $c_0 \in \{0, 1\}$, are chosen by TP in secret in advance. Thus, the whole private initial state of the QWs system is product state $|\phi\rangle_0 = |w_0\rangle|c_0\rangle$. Then, TP chooses another secret parameter f, which represents his steps of QWs. After TP's f steps of QWs with the unitary evolution operator U on $|\phi\rangle_0$, he generates the whole QWs system

$$|\phi\rangle_f = U^f|\phi\rangle_0 = (S(I_p \otimes H)^f|\phi\rangle_0. \tag{11}$$

In the same way, TP prepares k copies of QWs state $|\phi\rangle_f$, denoted by $|\phi\rangle_f^{\otimes k}$, where k is a predetermined security threshold.

Step 2 TP's distribution

The secret quantum entangled state $|\phi\rangle_f$ consists of two particles, namely walker particle and coin particle. In order to accomplish the task of private comparison, $|\phi\rangle_f^{\otimes k}$ must be transmitted safely between communicators via quantum channel. In the process of transmission, these particles may be attacked by eavesdropper with interception, substitution, entanglement measurement and other destructions. TP randomly chooses d pairs of decoy particles from the set of EPR states $\{\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)\}$, where d is a predetermined security threshold. Then, the $2d$ decoy particles are inserted into the $2k$ particles $|\phi\rangle_f^{\otimes k}$ at random positions in turn to form a new sequence of $2k + 2d$ particles, denoted by $|\phi'\rangle_f^{\otimes k}$. Then, TP sends the $|\phi'\rangle_f^{\otimes k}$ to the first private information owner, Alice, via the TP-Alice quantum channel.

Step 3 Alice's position operator and QWs evolution

After receiving $|\phi'\rangle_f^{\otimes k}$ from TP, Alice promulgates the message to TP. Then, TP announces the concrete positions of the decoy particles in $|\phi'\rangle_f^{\otimes k}$ to Alice in turn. Afterward, Alice performs the corresponding quantum measurements with the horizontal basis or diagonal basis randomly on each pair of two neighboring particles in turn and tells TP the measurement results. Comparing the initial state of two-particle EPR decoy particles and Alice's measurement results, TP and Alice can judge the existence possibility of the eavesdropper in the TP-Alice quantum channel. If any inconsistent result is found between Alice's declaration and TP's original result, they will abort the protocol. Otherwise, they continue the process.

Alice removes the inserted decoy particles from $|\phi'\rangle_f^{\otimes k}$ and gets k copies of two-particle state $|\phi\rangle_f$. Suppose the Alice's private information is classical integer $m_1 \in [0, \frac{q-1}{2}]$. Alice performs the m_1-position operator T_{m_1} on the receiving $|\phi\rangle_f$ and obtains the new two-particle state

$$|\varphi\rangle_{m_1} = (T_{m_1} \otimes I)|\phi\rangle_f, \tag{12}$$

where the T_{m_1} refers to the position operator defined in (4).

For the quantum state $|\varphi\rangle_{m_1}$, Alice continues to choose randomly another secret parameter g of her steps of QWs evolution and then generates the QWs state

$$|\chi\rangle_g = U^g|\varphi\rangle_{m_1}. \tag{13}$$

Step 4 Alice's distribution

Afterward, Alice passes the $|\chi\rangle_g^{\otimes k}$ with the inserted decoy particles to the second private information owner, Bob, via the Alice-Bob quantum channel just as TP in Step 2.

Step 5 Bob's inverse position operator

If the security check passes between Alice and Bob, Bob performs his position operator on $|\chi\rangle_g$ with his private information $m_2 \in [0, \frac{q-1}{2}]$. Unlike Alice in Step 3, here Bob adopts the inverse position operator T_{-m_2}. Then, Bob generates his new two-particle state

$$|\psi\rangle_{m_2} = (T_{-m_2} \otimes I)|\chi\rangle_g. \tag{14}$$

Step 6 Bob's distribution

Similarly, Bob passes the $|\psi\rangle_{m_2}^{\otimes k}$ with the inserted decoy particles to TP via Bob-TP quantum channel.

Step 7 TP's inverse QWs evolution

If the security check passes between Bob and TP, TP will take up his further task. After TP announces that he has received Bob's quantum state, Alice publishes her secret parameter g generated in Step 3. Based on quantum state $|\psi\rangle_{m_2}$ from Bob, TP performs $f + g$ steps of inverse QWs evolution on circle and acquires

$$|\omega\rangle_{f+g} = (U^{-1})^{f+g}|\psi\rangle_{m_2} = U^{-f-g}|\psi\rangle_{m_2}. \tag{15}$$

Finally, TP generates k copies of $|\omega\rangle_{f+g}$, denoted by $|\omega\rangle_{f+g}^{\otimes k}$.

Step 8 TP's private comparison

TP first measures the k copies of coin particle with the measurement basis $\{|0\rangle, |1\rangle\}$. As long as the measurement result $|\overline{c_0}\rangle$ appears in one of k times measurements, the protocol will be stopped immediately. Otherwise, he goes on the following process. TP measures the k copies of walker particle with the measurement basis $\{|0\rangle, |1\rangle, \ldots, |q-1\rangle\}$ and gets k copies of $|m_3'\rangle$, where $m_3' \in [0, q-1]$. If each m_3' is the identical, TP continues the following judgment.

Denote $m_3 = (m_3' - w_0) mod\, q$. According to the m_3, TP can judge the size relationship of private information between Alice and Bob. The concrete result is as follows:

$$\begin{cases} m_1 = m_2 & (\text{if} \quad m_3 = 0) \\ m_1 > m_2 & (\text{if} \quad m_3 \in [1, \dfrac{q-1}{2}]) \\ m_1 < m_2 & (\text{if} \quad m_3 \in [\dfrac{q+1}{2}, q-1]). \end{cases} \tag{16}$$

From the formula, the private comparison between Alice and Bob is completed by TP.

3.2 A concrete example

Suppose the public odd number of positions on circle is $q = 5$. In this concrete example of QWs, suppose that TP chooses his secret initial state $|\phi\rangle_0 = |w_0\rangle|c_0\rangle = |2\rangle|1\rangle$ and his secret walks steps $f = 6$. Alice selects her private information $m_1 = 1 \in [0, 2]$ and her secret walks steps $g = 2$. Bob's private information is $m_2 = 2 \in [0, 2]$. We can demonstrate the protocol in each step as follows.

Firstly, with the secret parameter $f = 6$, TP generates successively his QWs state

$$\begin{aligned}
&|\phi\rangle_0 = |2\rangle|1\rangle \xrightarrow{I\otimes H} \frac{\sqrt{2}}{2}(|2\rangle|0\rangle - |2\rangle|1\rangle) \xrightarrow{S} |\phi\rangle_1 = \frac{\sqrt{2}}{2}(|3\rangle|0\rangle - |1\rangle|1\rangle),\\
&\ldots\\
&|\phi\rangle_6 = \frac{1}{8}(-3|0\rangle|0\rangle + 3|1\rangle|0\rangle + 2|2\rangle|0\rangle - 2|4\rangle|0\rangle + 2|0\rangle|1\rangle + 2|1\rangle|1\rangle - 2|2\rangle|1\rangle\\
&\qquad + 5|3\rangle|1\rangle + |4\rangle|1\rangle).
\end{aligned}$$

TP sends k copies of $|\phi\rangle_6$ with decoy particles to Alice. After the position operator on $|\phi\rangle_6$ with her private information $m_1 = 1$, Alice gets the quantum state $|\varphi\rangle_1 = (T_1 \otimes I)|\phi\rangle_6$, namely

$$\begin{aligned}
|\varphi\rangle_1 = &\frac{1}{8}(-3|1\rangle|0\rangle + 3|2\rangle|0\rangle + 2|3\rangle|0\rangle - 2|0\rangle|0\rangle + 2|1\rangle|1\rangle + 2|2\rangle|1\rangle - 2|3\rangle|1\rangle\\
&+ 5|4\rangle|1\rangle + |0\rangle|1\rangle).
\end{aligned}$$

Then, Alice implements the QWs evolution on $|\varphi\rangle_1$ with her secret steps $g = 2$ and obtains the quantum state $|\chi\rangle_2 = U^2|\varphi\rangle_1$, namely

$$|\chi\rangle_2 = \frac{1}{16}(-3|0\rangle|0\rangle + 3|3\rangle|0\rangle - 2|0\rangle|1\rangle - 5|1\rangle|1\rangle + 10|2\rangle|1\rangle + 3|3\rangle|1\rangle + 10|4\rangle|1\rangle).$$

After the inverse position operator on $|\chi\rangle_2$ with his private information m_2, Bob gets the quantum state $|\psi\rangle_2 = (T_{-2} \otimes I)|\chi\rangle_2$, namely

$$|\psi\rangle_2 = \frac{1}{16}(-3|3\rangle|0\rangle + 3|1\rangle|0\rangle - 2|3\rangle|1\rangle - 5|4\rangle|1\rangle + 10|0\rangle|1\rangle + 3|1\rangle|1\rangle + 10|2\rangle|1\rangle).$$

With the inverse quantum operator U^{-1}, TP applies the $f + g = 8$ steps of inverse QWs evolution on circle. The process is as follows:

$$\begin{aligned}
&|\psi\rangle_2 \xrightarrow{S^{-1}} \frac{1}{16}(-3|2\rangle|0\rangle + 3|0\rangle|0\rangle - 2|4\rangle|1\rangle - 5|0\rangle|1\rangle + 10|1\rangle|1\rangle + 3|2\rangle|1\rangle + 10|3\rangle|1\rangle)\\
&\quad \xrightarrow{I\otimes H} |\omega\rangle_1 = \frac{\sqrt{2}}{16}(-|0\rangle|0\rangle + 5|1\rangle|0\rangle + 5|3\rangle|0\rangle - |4\rangle|0\rangle + 4|0\rangle|1\rangle - 5|1\rangle|1\rangle\\
&\quad - 3|2\rangle|1\rangle - 5|3\rangle|1\rangle + |4\rangle|1\rangle),\\
&\ldots\\
&|\omega\rangle_7 = \frac{\sqrt{2}}{2}(|2\rangle|0\rangle - |0\rangle|1\rangle),\\
&|\omega\rangle_8 = |1\rangle|1\rangle.
\end{aligned}$$

Finally, TP measures the walks particle with the basis $\{|0\rangle, |1\rangle, \ldots, |4\rangle\}$ and gets the result $m_3' = 1$. TP gets $m_3 = (m_3' - w_0) mod\, q = (1-2) mod\, 5 = 4$. Because of $m_3 \in [3, 4]$, TP comes to the conclusion that Alice's private information is smaller than Bob's, namely $m_1 < m_2$. Obviously, this conclusion is in line with the fact.

4 Analysis of the protocol

In this section, we will analyze the proposed protocol from three aspects including the correctness, security and comparison with other QPC protocols.

4.1 Correctness

It is a basic requirement for the correctness of the proposed protocol. The following three lemmas lead to the final correctness of the proposed QPC protocol.

Lemma 1 *In QWs on circle, the position operator T_m satisfies the relation $T_u T_v = T_{u+v}$, where $u, v \in [-(q-1), q-1]$.*

Proof According to the definition of T_m in (4), the product of two position operator can be expressed as:

$$\begin{aligned}
T_u T_v &= \left(\sum_{i=0}^{q-1} |(i+u) mod\, q\rangle\langle i|\right)\left(\sum_{j=0}^{q-1} |(j+v) mod\, q\rangle\langle j|\right) \\
&= \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} |(i+u) mod\, q\rangle\langle i|(j+v) mod\, q\rangle\langle j| \\
&= \sum_{j=0}^{q-1} |(((j+v) mod\, q)+u) mod\, q\rangle\langle j| \\
&= \sum_{j=0}^{q-1} |(j+(u+v) mod\, q\rangle\langle j| \\
&= T_{u+v}.
\end{aligned}$$

The lemma follows.

Lemma 2 *The operators $T_m \otimes I$ and U satisfy commutative law, i.e., $(T_m \otimes I)U = U(T_m \otimes I)$.*

Proof On the one hand, the $(T_m \otimes I)U$ can be expressed as:

$$\begin{aligned}
(T_m \otimes I)U &= (T_m \otimes I)(S(I \otimes R_c)) \\
&= (T_m \otimes I)(T_1 \otimes |0\rangle\langle 0| + T_{-1} \otimes |1\rangle\langle 1|)(I \otimes R_c) \\
&= (T_m T_1 \otimes |0\rangle\langle 0| + T_m T_{-1} \otimes |1\rangle\langle 1|)(I \otimes R_c) \\
&= T_{m+1} \otimes |0\rangle\langle 0| R_c + T_{m-1} \otimes |1\rangle\langle 1| R_c.
\end{aligned}$$

On the other hand, the $U(T_m \otimes I)$ can be expressed as:

$$\begin{aligned} U(T_m \otimes I) &= (S(I \otimes R_c))(T_m \otimes I) \\ &= (T_1 \otimes |0\rangle\langle 0| + T_{-1} \otimes |1\rangle\langle 1|)(I \otimes R_c)(T_m \otimes I) \\ &= (T_1 T_m \otimes |0\rangle\langle 0| + T_{-1} T_m \otimes |1\rangle\langle 1|)(I \otimes R_c) \\ &= T_{m+1} \otimes |0\rangle\langle 0| R_c + T_{m-1} \otimes |1\rangle\langle 1| R_c. \end{aligned}$$

Thus, the commutative law holds and the lemma follows.

Lemma 3 *Suppose that the initial state of QWs is $|\phi_0\rangle = |w_0\rangle|c_0\rangle$. The final quantum state $|\omega\rangle_{f+g}$ is disentangled and satisfies $|\omega\rangle_{f+g} = |(m_1 - m_2 + w_0) mod\, q\rangle|c_0\rangle$, where m_1 and m_2 are the private information of Alice and Bob, respectively.*

Proof After the operations of the three participants, the final quantum state $|\omega\rangle_{f+g}$ can be expressed as:

$$\begin{aligned} |\omega\rangle_{f+g} &= U^{-f-g}|\psi\rangle_{m_2} \\ &= U^{-f-g}(T_{-m_2} \otimes I)|\chi\rangle_g \\ &= U^{-f-g}(T_{-m_2} \otimes I)U^g|\varphi\rangle_{m_1} \\ &= U^{-f-g}(T_{-m_2} \otimes I)U^g(T_{m_1} \otimes I)|\phi\rangle_f \\ &= U^{-f-g}(T_{-m_2} \otimes I)U^g(T_{m_1} \otimes I)U^f|w_0\rangle|c_0\rangle \end{aligned}$$

According to Lemmas 1 and 2, the following formula can be deduced

$$\begin{aligned} |\omega\rangle_{f+g} &= U^{-f-g}(T_{-m_2} \otimes I)U^g(T_{m_1} \otimes I)U^f|w_0\rangle|c_0\rangle \\ &= U^{-f-g}(T_{-m_2} \otimes I)(T_{m_1} \otimes I)U^g U^f|w_0\rangle|c_0\rangle \\ &= U^{-f-g}(T_{m_1-m_2} \otimes I)U^{f+g}|w_0\rangle|c_0\rangle \\ &= U^{-f-g}U^{f+g}(T_{m_1-m_2} \otimes I)|w_0\rangle|c_0\rangle \\ &= I(T_{m_1-m_2} \otimes I)|w_0\rangle|c_0\rangle \\ &= |(m_1 - m_2 + w_0) mod\, q\rangle|c_0\rangle. \end{aligned}$$

It completes the proof.

Proposition 1 *The proposed QPC protocol is correct.*

Proof From Lemma 3, the final quantum state $|\omega\rangle_f$ is disentangled $|(m_1 - m_2 + w_0) mod\, q\rangle|c_0\rangle$. In the stage of TP's private comparison, TP should acquire the walker particle state $|m_3'\rangle = |(m_1 - m_2 + w_0) mod\, q\rangle$ and the coin particle state $|c_0\rangle$, respectively. Then, TP obtains the walker parameter $m_3 = (m_3' - w_0) mod\, q = (m_1 - m_2) mod\, q$.

Since the private m_1 and m_2 are limited to the range $[0, \frac{q-1}{2}]$, we can obtain $m_1 - m_2 \in [-\frac{q-1}{2}, \frac{q-1}{2}]$.

If $m_1 = m_2$, it is easy to get $m_3 = (m_1 - m_2) mod\, q = 0$.

If $m_1 > m_2$, we get the relations $m_1 - m_2 \in [1, \frac{q-1}{2}]$ and $m_3 = (m_1 - m_2) mod\, q \in [1, \frac{q-1}{2}]$.

If $m_1 < m_2$, we get the relations $m_1 - m_2 \in [-\frac{q-1}{2}, -1]$ and $m_3 = (m_1 - m_2) mod\, q \in [\frac{q+1}{2}, q-1]$.

With the TP's measurement results of the two particles, TP can conclude the size comparison between Alice's private m_1 and Bob's private m_2. Thus, the proposed QPC protocol is correct.

Thus, the proof is completed.

4.2 Security

We first show that the external attacks are invalid to the proposed QPC protocol. Then, it is clearly shown that the protocol is immune to internal attacks. More specifically, one participant cannot obtain other participant's private information. Meanwhile, the semi-honest TP, who announces the participants' size comparison result, cannot know both participants' secrets either. At last, we analyze the TP's judgment when there is a dispute in the protocol.

4.2.1 External attacks

We know that some well-known external attacks, such as intercept-resend attack [76], correlation-elicitation attack [77] and entanglement-measure attack [78], are frequently mentioned in the quantum channel. The decoy particles technique [79,80] can be regarded as a security check variant of the effective eavesdropping method of the BB84 protocol. Actually, the effectiveness of decoy particles technology has been explicitly validated in detail in some literature, such as Refs. [42,46,81–84].

In the subsection, we analyze the external attacks according to each step of the protocol. In this protocol, since TP only performs QWs operations without transmission of the quantum particles in Step 1, 7 and 8, Alice in Step 3, Bob in Step 5, respectively, thus there is no chance for the outside eavesdropper to attack the quantum states in these steps. Therefore, regarding external attacks, we only need to analyze the Step2, 4 and 6 in the quantum channel.

In Step 2, TP transmits k copies of two-particle QWs states $|\phi\rangle_f^{\otimes k}$ with random $2d$ decoy particles to Alice via the TP-Alice quantum channel. In the $2d$ decoy particles, each of the two adjacent particles randomly comes from the set of EPR states $\{\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle)\}$ and inserted into $|\phi\rangle_f^{\otimes k}$ at random positions to form a new sequence of particles $|\phi'\rangle_f^{\otimes k}$. After TP sends $|\phi'\rangle_f^{\otimes k}$ to the first participant Alice and then Alice declares her receiving quantum particles, TP announces the positions of all $2d$ decoy particles. Later, Alice randomly measures each pair of the corresponding decoy particles with the horizontal basis or diagonal basis and then announces the results to TP. Afterward, TP can judge the existence of the outside eavesdropper Eve by checking Alice's measurement results. Suppose that Eve randomly selects e positions of $2k + 2d$ to do the outside attacks in order to obtain private information, where we take the case of $2k \le e \le 2d$ to illustrate TP's detection probability. It is easy to know that Alice gets the correct result with probability $\frac{1}{2}$ if she measures the decoy particle destroyed by Eve with TP's claiming position. We can obtain the TP's detection probability against the Eve's external attack through decoy technology as follows:

$$p = 1 - \sum_{x=0}^{2k} \Big(\frac{C_{2k}^{x} C_{2d}^{e-x}}{C_{2k+2d}^{e}} \cdot (\frac{1}{2})^{e-x} \Big). \tag{17}$$

The detection probability p is close to 1 if d is large enough. Therefore, an outside eavesdropper cannot steal any secret without being detected in Step 2.

As for the Step 4 and 6, the analogous security analyses can also be made because of their same communication principles as the Step 2. Thus, the external attacks are invalid to our proposed protocol.

4.2.2 Internal attacks

There are three internal participants (the semi-honest TP, the dishonest Alice and Bob) in the two-party QPC protocol, and thus exist two cases of participants' attacks from the dishonest two parties and the semi-honest TP. The semi-honest TP executes loyally the protocol and records the intermediate data. The limitation of behavior for TP is that he cannot conspire with one dishonest participant to steal the other private information. However, he might try to reveal the participants' private information from the open records or the protocol loophole. Obviously, compared with the malicious Eve's external attacks, the internal ones are generally more powerful, and thus should be paid more attention to.

In Steps 1 and 2, the sequence of $2k + 2d$ particles $|\phi'\rangle_f^{\otimes k}$, consisting of k copies of two-particle QWs states $|\phi\rangle_f^{\otimes k}$ and $2d$ decoy particles, is transmitted via the TP-Alice quantum channel. If the dishonest participant Bob wants to obtain TP's secret, he has to face the sequence with decoy detection particles. As we have analyzed before, the participant Bob, whose identity is an external attacker at this time, would be detected by TP and Alice with the decoy technology, so this attack will not work. Even if Bob has gained the QWs state $|\phi\rangle_f^{\otimes k}$ from TP to Alice, which have been stripped the decoy detection particles, he still has to face the two entangled particles of QWs. The participants, Alice and Bob, cannot infer the secret parameters $w_0 \in \{0, 1, \ldots, q-1\}$ and $c_0 \in \{0, 1\}$ in initial QWs state and the secret steps $f \in S_f$ of QWs selected by TP in Step 1. The probability that the participant Bob correctly guesses the three parameters is $\frac{1}{2q\| S_f \|}$, where $\| \ S_f \ \|$ represents the number of elements in the set S_f. Obviously, the probability is almost negligible, and thus, the participants' internal attacks are impossible.

In Steps 3 and 4, with the position operator of the QWs, Alice embeds her private classical information $m_1 \in [0, \frac{q-1}{2}]$ into the two-particle QWs state $|\phi\rangle_f$ from TP and obtains $|\varphi\rangle_{m_1}$. Afterward, Alice selects randomly another secret parameter $g \in S_g$ of her steps of QWs and then generates a new QWs state $|\chi\rangle_g$. In Step 4, Alice transmits $|\chi\rangle_g$ to Bob via Alice-Bob quantum channel. The probability that the semi-honest TP and dishonest Bob correctly obtain the two parameters is $\frac{2}{(q+1)\| S_g \|}$, where $\| \ S_g \ \|$

represents the number of elements in the set S_g. Thus, the attacks of the internal TP and Bob are impractical.

In Steps 5 and 6, with the private information $m_2 \in [0, \frac{q-1}{2}]$, Bob performs the inverse position operator T_{-m_2} of the QWs on $|\chi\rangle_g$ and generates his new two-particle state $|\psi\rangle_{m_2}$, and then passes it to TP in the Bob-TP quantum channel. Similarly, it is impossible for Alice and TP to guess the Bob's private information m_2 with the small probability $\frac{2}{q+1}$.

In Steps 7 and 8, after TP informs Alice to disclose her secret parameter g, TP performs $f+g$ steps of inverse QWs evolution on the quantum state $|\psi\rangle_{m_2}$, and then acquires $|\omega\rangle_{f+g}$. TP measures the walk particle in $|\omega\rangle_{f+g}$ and gets m_3. According to the proof of Proposition 1, the $m_3 = (m_1 - m_2) mod\, q$ holds. Thus, the semi-honest TP cannot separate conversely Alice's private information m_1 and Bob's m_2 from m_3, respectively. TP can only judge the size between m_1 and m_2, which is the expected result of the proposed protocol.

4.2.3 Dispute

Different from the mentioned internal and external attacks for obtaining the participant's private information, there is another kind of destructive attack. This kind of attack usually manifests itself as the malicious destruction of the external Eve or internal participants, which may cause that TP cannot correctly judge the protocol result. There are two cases of dispute attacks on QWs particles in this protocol.

The first case is the dispute caused by two kinds of destructions on the QWs particles. One destruction is implemented by the external Eve, and the other is done by the participant Alice or Bob. In the above subsection about external attacks, we show that the decoy technology can be used to find the destructive attack on quantum particles by Eve. The technology can be used only to judge whether the decoy particles are destructive or not, but the QWs particles cannot. Meanwhile, it is also possible for the internal participants to destroy deliberately the QWs particles just for malicious destruction. In fact, the two destructions can be found once we find that the measurement result of the first QWs particle is not c_0 or one of the measurement value of the second QWs particle is different from m'_3. For simplicity, suppose that one of the k copies of QWs states is destroyed. The probability that this QWs state is found not to be the same as other $k-1$ QWs states is

$$p = 1 - |\langle c_0, m'_3|\omega'\rangle_{f+g}|^2, \tag{18}$$

where $|\omega'\rangle_{f+g}$ is the entangled two-particle QWs state. This probability is close to 1.

The second case is the dispute caused by the deliberate lie of participant Alice. In Step 3, Alice chooses a randomly secret parameter g to operate on $|\varphi\rangle_{m_1}$ and then generates the QWs state $|\chi\rangle_g$. In Step 7, at TP's request, Alice publicly announces her secret parameter g generated in Step 3. In Step 7, TP performs inverse QWs evolution and gets $|\omega\rangle_{f+g}$. In Step 8, TP measures the two particles of $|\omega\rangle_{f+g}$, respectively. Then, he obtains the private comparison between Alice and Bob. In this process, maybe it is just a hoax, participant Alice would declare deliberately a different parameter, see g', in Step 3. In fact, this strategy can be found by TP. According to Lemma 3, the final QWs state $|\omega\rangle_{f+g'}$ is not product state, but entangled state. Suppose TP's measurement result of the entangled state $|\omega\rangle_{f+g'}$ is $\{m_3', c_0\}$ for the first time, which has the probability $|\langle c_0, m_3'|\omega\rangle_{f+g'}|^2$. In order for TP not to detect Alice's dishonesty, it must ensure that the result $\{m_3', c_0\}$ must be obtained in each of the remaining $k-1$ measurements. It is easy to know that the probability of not finding Alice's behavior is at most $|\langle c_0, m_3'|\omega\rangle_{f+g'}|^{2k}$. As a matter of fact, the probability of TP's discovery is at least

$$p = 1 - |\langle c_0, m_3'|\omega\rangle_{f+g'}|^{2k}. \tag{19}$$

With the increase in k, the limit of probability is 1. Thus, the dispute arising from Alice's dishonesty will be discovered by TP.

4.3 Comparison

Compared with the previous QPC protocols, the proposed two-party QPC one has its unique characteristics in terms of mechanism, implementation mode, security, etc. In the following, we give the comparisons from the essential aspects, rather than specific details.

4.3.1 Basic technology

Except the single-particle protocols, the current ones use the entangled states to realize the private information transmission and comparison. Unlike the entanglement technology, our protocol is based on QWs technology.

4.3.2 Number of particles

According to the analysis in Introduction, there are single-particle and multi-particle carriers embodying the participants' private information. The truth of the matter is that most of the QPC protocols adopt multi-particle entangled states. For our protocol, the private information carrier is the two-particle QWs state.

4.3.3 Entanglement

In the current multi-particle entanglement protocols, the entangled particles are distributed among the participants, and the participants' private information is compared by entanglement swapping, unitary operation and measurement. Unlike the particles being always entangled before measurement, the two particles in our protocol are product state and do not exist entanglement at the beginning of QWs. They emerge the entanglement during the process of QWs, and then disentangle and form the product state at the end of the protocol.

4.3.4 Particles distribution

In the current multi-particle entanglement protocols, each particle must be distributed to each different participant at the beginning via quantum channel. In our protocol, the two-particle QWs state is transferred as a whole among different participants. In fact, there are only three times of transmissions in total via quantum channel. This reduces the protocol complexity and avoids the chance of being attacked.

4.3.5 Dispute resolution

It is normal for participants to dispute the result of the protocol. However, most of the current protocols seldom mention basically the dispute over the judgment result of the semi-honest TP. Our protocol takes into account the dispute and is more in line with the actual situation.

Therefore, compared with the traditional protocols, our protocol has its unique advantages in principle, implementation efficiency and security.

5 Conclusion

To sum up, in this paper, we propose a novel two-party QPC protocol with a semi-honest TP via QWs on circle. Here, the TP is allowed to misbehave on his own, while not able to conspire with either of the two dishonest participants. Our protocol adopts the two-particle QWs state rather than entangled state as the initial quantum resource, and involves only QWs operators for participants. It does not need the quantum entanglement swapping. It can not only compare the equality of private information, but also the size between them, which is in line with the actual situation. Meanwhile, the semi-honest TP cannot obtain the participants' private information. Our protocol only employs the QWs on circle and quantum measurement, both of which can be realized by current quantum information technology. We have proved the correctness of the proposed protocol through mathematical deduction and proof. As for the security, the protocol can resist the external and internal malicious attacks, but also can give the judgment results in case of dispute.

Of course, the proposed protocol is two-party size comparison of private information. If it can be extended to multi-party size comparison, it will be more significant in practicability and universality. At the same time, some security issues of this protocol, such as the generalized scenarios involving noise and Eve's various strategies, are worthy of further rigorous study in the future. These directions deserve further investigation.

Acknowledgements This work was supported in part by University Natural Science Research Project of Anhui Province of China (Grant Nos. KJ2019A0580, KJ2019A0562), National Natural Science Foundation of China (Grant Nos. 11975025, 11701009) and Natural Science Foundation of Anhui Province of China (Grant No. 1708085MA10).

References

1. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), Chicago, IL, USA, 1982, pp. 160–164
2. Arute, F., Arya, K., Babbush, R., et al.: Quantum supremacy using a programmable superconducting processor. Nature **574**, 505–511 (2019)

3. Qiang, X.G., Zhou, X.Q., Aungskunsiri, K., et al.: Quantum processing by remote quantum control. Quantum Sci. Technol. **2**, 045002 (2017)
4. Long, G.L.: General quantum interference principle and duality computer. Commun. Theor. Phys. **45**(5), 825–844 (2006)
5. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154–1162 (1997)
6. 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. **42**(5), 055305 (2009)
7. Yang, Y.G., Gao, W.F., Wen, Q.Y.: Secure quantum private comparison. Phys. Scr. **80**(6), 065002 (2009)
8. Yang, Y.G., Xia, J., Jia, X., et al.: New quantum private comparison protocol without entanglement. Int. J. Quantum Inf. **10**(06), 1250065 (2012)
9. Huang, W., Wen, Q.Y., Lin, B., et al.: Robust and efficient quantum private comparison of equality with collective detection over collective-noise channels. Sci. China-Phys. Mech. **56**(9), 1670–1678 (2013)
10. Yu, C.H., Guo, G.D., Lin, S.: Quantum private comparison with d-level single-particle states. Phys. Scr. **88**(6), 065013 (2013)
11. Liu, B., Xiao, D., Huang, W., et al.: Quantum private comparison employing single-photon interference. Quantum Inf. Process. **16**(7), 180 (2017)
12. Pan, H.M.: Two-party quantum private comparison using single photons. Int. J. Theor. Phys. **57**, 3389–3395 (2018)
13. Liu, W., Wang, Y.B., Cui, W.: Quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **57**(4), 583–588 (2012)
14. Tseng, H.Y., Lin, J., Hwang, T.: New quantum private comparison protocol using EPR pairs. Quantum Inf. Process. **11**(2), 373–384 (2012)
15. Wang, C., Xu, G., Yang, Y.X.: Cryptanalysis and improvements for the quantum private comparison protocol using EPR pairs. Int. J. Quantum Inf. **11**(04), 1350039 (2013)
16. Yang, Y.G., Xia, J., Jia, X., Zhang, H.: Comment on quantum private comparison protocols with a semihonest third party. Quantum Inf. Process. **12**(2), 877–885 (2013)
17. Zhang, W.W., Zhang, K.J.: Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf. Process. **12**(5), 1981–1990 (2013)
18. Lin, S., Sun, Y., Liu, X.F., Yao, Z.Q.: Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf. Process. **12**(1), 559–568 (2013)
19. Guo, F.Z., Gao, F., Qin, S.J., et al.: Quantum private comparison protocol based on entanglement swapping of d-level Bell states. Quantum Inf. Process. **12**(8), 2793–2802 (2013)
20. Zhang, W.W., Li, D., Zhang, K.J., Zuo, H.J.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **13**(6), 2241–2249 (2013)
21. Liu, W.J., Liu, C., Chen, H.W., et al.: Cryptanalysis and improvement of quantum private comparison protocol based on Bell entangled states. Commun. Theor. Phys. **62**(2), 210–214 (2014)
22. Tan, X.Q., Zhang, X.Q., Li, J.: Big data quantum private comparison with the intelligent third party. J. Ambient Intell. Hum. Comput. **6**(6), 797–806 (2015)
23. Wang, F., Luo, M., Li, H., et al.: Quantum private comparison based on quantum dense coding. Sci. China-Inf. Sci. **59**(11), 112501 (2016)
24. Chen, X.B., Xu, G., Niu, X.X., et al.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. **283**(7), 1561–1565 (2010)
25. Lin, J., Tseng, H.Y., Hwang, T.: Intercept-resend attacks on Chen et al.'s quantum private comparison protocol and the improvements. Opt. Commun. **284**(9), 2412–2414 (2011)
26. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. **284**(1), 545–549 (2011)
27. Liu, W., Wang, Y.B.: Quantum private comparison based on GHZ entangled states. Int. J. Theor. Phys. **51**(11), 3596–3604 (2012)
28. Liu, W., Wang, Y.B., Jiang, Z.T.: An efficient protocol for the quantum private comparison of equality with W state. Opt. Commun. **284**, 3160–3163 (2011)
29. Zhang, W.W., Li, D., Li, Y.B.: Quantum private comparison protocol with W States. Int. J. Theor. Phys. **53**(5), 1723–1729 (2014)
30. Xu, G.A., Chen, X.B., Wei, Z.H., et al.: An efficient protocol for the quantum private comparison of equality with a four-qubit cluster state. Int. J. Quantum Inf. **10**(4), 1250045 (2012)

31. Sun, Z.W., Long, D.Y.: Quantum private comparison protocol based on cluster states. Int. J. Theor. Phys. **52**(1), 212–218 (2013)
32. Li, C.Y., Chen, X.B., Li, H., et al.: Efficient quantum private comparison protocol based on the entanglement swapping between four-qubit cluster state and extended Bell state. Quantum Inf. Process. **18**(5), 158 (2019)
33. Liu, W., Wang, Y.B., Jiang, Z.T., et al.: A protocol for the quantum private comparison of equality with χ-type state. Int. J. Theor. Phys. **51**(1), 69–77 (2012)
34. Jia, H.Y., Wen, Q.Y., Li, Y.B., Cao, F.: Quantum private comparison using genuine four-particle entangled states. Int. J. Theor. Phys. **51**(4), 1187–1194 (2012)
35. Liu, W., Wang, Y.B., Jiang, Z.T., et al.: New quantum private comparison protocol using χ-type state. Int. J. Theor. Phys. **51**(6), 1953–1960 (2012)
36. Lin, S., Guo, G.D., Liu, X.F.: Quantum private comparison of equality with χ-type entangled states. Int. J. Theor. Phys. **52**(11), 4185–4194 (2013)
37. Pan, H.M.: Quantum private comparison based on χ-type entangled states. Int. J. Theor. Phys. **56**(10), 3340–3347 (2017)
38. 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)
39. Ji, Z.X., Fan, P.R., Zhang, H.G., Wang, H.Z.: Several two-party protocols for quantum private comparison using entanglement and dense coding. Opt. Commun. **459**(15), 124911 (2020)
40. Ye, T.Y., Ji, Z.X.: Two-party quantum private comparison with five-qubit entangled states. Int. J. Theor. Phys. **56**(5), 1517–1529 (2017)
41. Ji, Z.X., Ye, T.Y.: Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun. Theor. Phys. **65**(6), 711–715 (2016)
42. Ji, Z.X., Zhang, H.G., Wang, H.Z.: Quantum private comparison protocols with a number of multi-particle entangled states. IEEE Access **7**, 44613–44621 (2019)
43. Liu, W., Wang, Y.B.: Dynamic multi-party quantum private comparison protocol with single photons in both polarization and spatial-mode degrees of freedom. Int. J. Theor. Phys. **55**(12), 5307–5317 (2016)
44. Ye, C.Q., Ye, T.Y.: Multi-party quantum private comparison of size relation with d-level single-particle states. Quantum Inf. Process. **17**(10), 252 (2018)
45. Du, G., Zhang, F., Ma, C.G.: A new multi-party quantum private comparison protocol based on circle model. Int. J. Theor. Phys. **58**, 3225–3233 (2019)
46. Song, X.L., Wen, A.J., Gou, R.: Multiparty quantum private comparison of size relation based on single-particle states. IEEE Access **7**, 142507–142514 (2019)
47. Abulkasim, H., Alsuqaih, H.N., Hamdan, W.F., Hamad, S., et al.: Improved dynamic multi-party quantum private comparison for next-generation mobile network. IEEE Access **7**, 17917–17926 (2019)
48. Liu, W., Wang, Y.B., Wang, X.M.: Quantum multi-party private comparison protocol using d-dimensional Bell states. Int. J. Theor. Phys. **54**(6), 1830–1839 (2015)
49. Ye, T.Y.: Multi-party quantum private comparison protocol based on entanglement swapping of Bell entangled states. Commun. Theor. Phys. **66**(3), 280–290 (2016)
50. 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)
51. Ye, T.Y., Ji, Z.X.: Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci. China-Phys. Mech. Astron. **60**(9), 090312 (2017)
52. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process. **12**(2), 1077–1088 (2013)
53. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison protocol with an almost-dishonest third party using GHZ states. Int. J. Theor. Phys. **55**(6), 2969–2976 (2016)
54. Huang, S.L., Hwang, T., Gope, P.: Multi-party quantum private comparison with an almost-dishonest third party. Quantum Inf. Process. **14**, 4225–4235 (2015)
55. 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)
56. Wang, Q.L., Sun, H.X., Huang, W.: Multi-party quantum private comparison protocol with n-level entangled states. Quantum Inf. Process. **13**(11), 2375–2389 (2014)
57. Luo, Q.B., Yang, G.W., She, K., et al.: Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. **13**(10), 2343–2352 (2014)

58. 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**(4), 1085–1091 (2014)
59. Aharonov, Y., Davidovich, L., Zagury, N.: Quantum random walks. Phys. Rev. A **48**(2), 1687–1690 (1993)
60. Farhi, E., Gutmann, S.: Quantum computation and decision trees. Phys. Rev. A **58**(2), 915–928 (1998)
61. Ambainis, A.: Quantum walk algorithm for element distinctness. In: 45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, pp. 22–31 (2004)
62. Magniez, F., Santha, M., Szegedy, M.: Quantum algorithms for the triangle problem. SIAM J. Comput. **37**(2), 413–424 (2007)
63. Tamascelli, D., Zanetti, L.: A quantum-walk-inspired adiabatic algorithm for solving graph isomorphism problems. J. Phys. A-Math. Theor. **47**(32), 3025302 (2014)
64. Chakraborty, S., Novo, L., Giorgio, S.D., Omar, Y.: Optimal quantum spatial search on random temporal networks. Phys. Rev. Lett. **119**(22), 220503 (2017)
65. Yang, Y.G., Yang, J.J., Zhou, Y.H., et al.: Quantum network communication: a discrete-time quantum-walk approach. Sci. China-Inf. Sci. **61**(4), 042501 (2018)
66. Kurzyński, P., Wójcik, A.: Quantum walk as a generalized measuring device. Phys. Rev. Lett. **110**(20), 200404 (2013)
67. Zhan, X., Qin, H., Bian, Z.H., et al.: Perfect state transfer and efficient quantum routing: a discrete-time quantum-walk approach. Phys. Rev. A **90**(1), 012331 (2014)
68. Yalccinkaya, I., Gedik, Z.: Qubit state transfer via discrete-time quantum walks. J. Phys. A: Math. Theor. **48**(22), 225302 (2015)
69. Babatunde, A.M., Cresser, J., Twamley, J.: Using a biased quantum random walk as a quantum lumped element router. Phys. Rev. A **90**(1), 124–129 (2014)
70. Vlachou, C., Rodrigues, J., Mateus, P., et al.: Quantum walk public-key cryptographic system. Int. J. Quantum Inf. **13**(07), 1550050 (2015)
71. Vlachou, C., Krawec, W., Mateus, P., et al.: Quantum key distribution with quantum walks. Quantum Inf. Process. **17**(11), 288 (2018)
72. Li, H.J., Jian, J., Xiang, N., et al.: A new kind of universal and flexible quantum information splitting scheme with multi-coin quantum walks. Quantum Inf. Process. **18**(10), 316 (2019)
73. Wang, Y., Shang, Y., Xue, P.: Generalized teleportation by quantum walks. Quantum Inf. Process. **16**(9), 221 (2017)
74. Yang, Y.G., Cao, S.N., Chao, W.F., et al.: Generalized teleportation by means of discrete-time quantum walks on N-lines and N-cycles. Mod. Phys. Lett. B **33**(06), 1950070 (2019)
75. Gnutzmann, S., Smilansky, U.: Quantum graphs: applications to quantum chaos and universal spectral statistics. Adv. Phys. **55**(5–6), 527–625 (2006)
76. Gao, F., Gao, F.Z., Wen, Q.Y., Zhu, F.C.: Comment on "experimental demonstration of a quantum protocol for byzantine agreement and liar detection". Phys. Rev. Lett. **101**(20), 208901 (2008)
77. Gao, F., Lin, S., Wen, Q.Y., Zhu, F.C.: A special eavesdropping on one-sender versus n-receiver QSDC protocol. Chin. Phys. Lett. **25**(5), 1561–1563 (2008)
78. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the brádler-dušek protocol. Quantum Inf. Comput. **7**(4), 329–334 (2007)
79. 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), 1049–1052 (2005)
80. Li, C.Y., Li, X.H., Deng, F.G., et al.: Efficient quantum cryptography network without entanglement and quantum memory. Chin. Phys. Lett. **23**(11), 2896–2899 (2006)
81. Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin. Phys. Lett. **24**(1), 19 (2007)
82. Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin. Phys. Lett. **30**(04), 040305 (2013)
83. Gao, G., Wang, L.P.: A protocol for bidirectional quantum secure communication based on genuine four-particle entangled states. Commun. Theor. Phys. **54**(3), 447–451 (2010)
84. Xiu, X.M., Dong, H.K., Dong, L., et al.: Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. Opt. Commun. **282**(12), 2457–2459 (2009)

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