SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Multi-party quantum private comparison of size relationship based on one-direction quantum walks on a circle

Jintao WANG, Jiangyuan LIAN & Tianyu YE*

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, *China*

Appendix A Introduction

In 1982, Yao [1] proposed the classical private comparison problem for the first time. i.e., two millionaires wish to know which one is richer without leaking their properties. In 1984, Bennett and Brassard [2] proposed the famous BB84 protocol on quantum key distribution (QKD) by combining quantum mechanics with classical cryptography and set a precedent for quantum cryptography. In 2009, by combining quantum cryptography and classical private comparison, in order to compare the equality of private information from two players, Yang and Wen [3] firstly proposed the brand-new concept of quantum private comparison (QPC) protocol. From then on, various QPC protocols which exploit different quantum resources and quantum technologies [4–12] have been put forward.

In 2013, Chang *et al.* [13] put forward the first multi-party quantum private comparison (MQPC) protocol for equality comparison among more than two users by using GHZ class states. Later, a number of MQPC protocols of equality with different quantum technologies [14–18] were presented. However, those protocols of Refs. [13–18] are limited to evaluate the equality of privacies instead of size relationship comparison, which may restrict their scope of practical applications.

In 2013, Lin *et al.* [19] put forward the first QPC protocol of size relationship through d-dimensional Bell states. In 2014, Luo *et al.* [20] proposed a novel MQPC protocol of size relationship to accomplish the size comparison of privacies among more than two users by using d-dimensional entangled states. Subsequently, numerous MQPC protocols of size relationship were constructed, such as the one based on d-dimensional single-particle [21], d-dimensional Bell states [22], d-dimensional GHZ states [23].

Quantum walks (QW) are the quantum counterpart of classical random walks, and portray a natural stochastic process when the walker randomly wanders around. In 2018, Vlachou *et al.* [24] firstly introduced QW into QKD to design the QW-based quantum cryptography protocol. In 2020, Srikara and Chandrashekar [25] put forward the novel quantum secure direct communication (QSDC) protocols based on QW. Afterward, Chen *et al.* [26] and Wang *et al.* [27] proposed different two-party QPC protocols based on QW, respectively; and Wang *et al.* [28] constructed a novel verifiable multi-dimensional (t, n) threshold quantum secret sharing (QSS) protocol based on QW. In 2024, Wang *et al.* [29] proposed a quantum secure multi-party summation (QSMS) protocol based on QW.

Based on the above analysis, in this paper, in order to accomplish the size relationship comparison of privacies between one user and the remaining users, we present a novel MQPC protocol of size relationship based on one-direction quantum walks on a circle (ODQWC) with two semi-honest third parties (TPs), TP_1 and TP_2, where each TP is allowed to perform all kinds of attacks but cannot conspire with others. To be specific, TP_1 prepares initial QW states, distributes initial QW states to users, decrypts the encrypted QW states, measures the walker particles to get the comparison result and publishes the comparison result, while TP_2 helps encrypt the QW states and transfers them to TP_1. On the other hand, TP_1 and TP_2 can supervise each other mutually, and successfully accomplish the goal of this protocol under their controls. The proposed protocol adopts the QW states as the initial quantum resource, which are actually a kind of two-particle product states rather than quantum entangled states. Different from the QW-based two-party QPC protocols in Ref. [26] and Ref. [27], the proposed protocol can accomplish the size relationship comparison of privacies from users more than two within one execution of protocol, and only needs d-dimensional single particle measurements. In addition, we construct the quantum circuits of ODQWC and validate the output correctness of the proposed protocol through simulation by using IBM Qiskit.

Appendix B Preliminaries

A discrete-time QW system on a line is composed of a walker system, which describes the walker particle's position, and a coin system, which determines the coin particle's direction [30]. The tensor product of walker particle space $\mathcal{H}_p$ and coin particle space $\mathcal{H}_c$ spans the Hilbert space $\mathcal{H} = \mathcal{H}_p \otimes \mathcal{H}_c$ where QW state lies in. Here, the QW state is represented by

$$|\psi\rangle = |position\rangle_p \otimes |coin\rangle_c , \tag{B1}$$

where $position \in (-d, d) \cap \mathbb{Z}$, $coin \in \{0, 1\}$ and $\mathbb{Z}$ is the integer set. The evolution operator, which is used to make the QW state evolve, is defined as

$$U = S \cdot \big(I_p \otimes C\big), \tag{B2}$$

where C is the coin operator of $\mathcal{H}_c$, I_p is the identity operator of $\mathcal{H}_p$, and S is the global shifting operator. Here, C is generally defined as [31]

$$C_{\xi,\theta,\zeta} = \begin{pmatrix} e^{i\xi}\cos\theta & e^{i\zeta}\sin\theta \\ e^{-i\zeta}\sin\theta & -e^{-i\xi}\cos\theta \end{pmatrix}. \tag{B3}$$

* Corresponding author (email: yetianyu@zjgsu.edu.cn)

According to the definition, $C_{0,\pi/4,0}$ is the Hadamard gate $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ [32]. The effect of C applying on the coin particle is as follows:

$$|i\rangle_p |0\rangle_c \xrightarrow{C} |i\rangle_p \otimes \frac{1}{\sqrt{2}}\big(|0\rangle_c + |1\rangle_c\big), \tag{B4}$$

$$|i\rangle_p |1\rangle_c \xrightarrow{C} |i\rangle_p \otimes \frac{1}{\sqrt{2}}\big(|0\rangle_c - |1\rangle_c\big). \tag{B5}$$

Here, $|0\rangle_c$ means that the walker particle steps forward, while $|1\rangle_c$ means that the walker particle steps backward. In this paper, we always make C be H. In addition, as for two-direction quantum walks on a line (TDQWL), S is defined as

$$S = \sum\nolimits_i |i+1\rangle_p \langle i| \otimes |0\rangle_c \langle 0| + \sum\nolimits_i |i-1\rangle_p \langle i| \otimes |1\rangle_c \langle 1| . \tag{B6}$$

As a result, it has

$$|i\rangle_p |0\rangle_c \xrightarrow{S} |i+1\rangle_p |0\rangle_c , \tag{B7}$$

$$|i\rangle_p |1\rangle_c \xrightarrow{S} |i-1\rangle_p |1\rangle_c . \tag{B8}$$

Suppose that the initial QW state is $|\psi_0\rangle = |0\rangle_p|0\rangle_c$. Then, three-step evolution with U performed on $|\psi_0\rangle$ can be depicted as

$$\begin{aligned} |\psi_0\rangle = |0\rangle_p |0\rangle_c &\xrightarrow{U} |\psi_1\rangle = \frac{1}{\sqrt{2}}\big(|1\rangle_p |0\rangle_c + |-1\rangle_p |1\rangle_c\big) \\ &\xrightarrow{U} |\psi_2\rangle = \frac{1}{2}\big(|2\rangle_p |0\rangle_c + |0\rangle_p |1\rangle_c + |0\rangle_p |0\rangle_c - |-2\rangle_p |1\rangle_c\big) \\ &\xrightarrow{U} |\psi_3\rangle = \frac{1}{2\sqrt{2}}\big(|3\rangle_p |0\rangle_c + |1\rangle_p |1\rangle_c + 2|1\rangle_p |0\rangle_c - |-1\rangle_p |0\rangle_c + |-3\rangle_p |1\rangle_c\big). \end{aligned} \tag{B9}$$

Clearly, if the walker particle is measured with the $\{|-(d-1)\rangle, \cdots, |-2\rangle, |-1\rangle, |0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis, the walker particle of $|\psi_1\rangle$ will fall on positions 1 and -1 each with the probability of 1/2; the walker particle of $|\psi_2\rangle$ will fall on positions 2, 0, -2 with the possibility of 1/4, 1/2, 1/4, respectively; and the walker particle of $|\psi_3\rangle$ will fall on positions 3, 1, -1, -3 with the possibility of 1/8, 5/8, 1/8, 1/8, respectively.

Define the T_k operator as

$$T_k = \sum_{i=0}^{d-1} |i \oplus k\rangle\langle i|, \tag{B10}$$

where the symbol '$\oplus$' denotes the modulo d addition. As a result, the global shifting operator corresponding to T_k is

$$S^k = T_k \otimes |0\rangle\langle 0| + T_{-k} \otimes |1\rangle\langle 1|. \tag{B11}$$

The inverse evolution operator corresponding to U is

$$U^{-1} = \big[S \cdot (I_p \otimes C)\big]^{-1} = \big(I_p \otimes C^{-1}\big) \cdot S^{-1}, \tag{B12}$$

where the inverse coin operator $C^{-1} = H^{-1} = H$, and the inverse global shifting operator

$$S^{-1} = T_{-1} \otimes |0\rangle\langle 0| + T_1 \otimes |1\rangle\langle 1|. \tag{B13}$$

Define the one-direction global shifting operator S_{od} and its inverse S_{od}^{-1} as

$$S_{od} = T_1 \otimes |0\rangle\langle 0| + T_0 \otimes |1\rangle\langle 1|, \tag{B14}$$

$$S_{od}^{-1} = T_{-1} \otimes |0\rangle\langle 0| + T_0 \otimes |1\rangle\langle 1|. \tag{B15}$$

Consequently, the one-direction evolution operator U_{od} and its inverse U_{od}^{-1} are respectively

$$U_{od} = S_{od} \cdot \big(I_p \otimes C\big), \tag{B16}$$

$$U_{od}^{-1} = \big(I_p \otimes C^{-1}\big) \cdot S_{od}^{-1}. \tag{B17}$$

By using U_{od} instead of U, TDQWL can be converted into one-direction quantum walks on a circle (ODQWC). In this paper, U_{od}^k means applying k times U_{od} on the QW state, while U_{od}^{-k} means applying k times U_{od}^{-1} on the QW state.

Wang *et al.* have proved in Ref. [27] that when U_{od}^k is performed on the initial QW state $|0\rangle|0\rangle$, where $k \in [1, d)$, the walker particle's position may be collapsed into the position equal to or bigger than 0 after being performed with the $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis measurement; when U_{od}^{-k} is performed on the initial QW state $|0\rangle|0\rangle$, where $k \in [1, d)$, the walker particle's position is never collapsed into the position 0 after being performed with the $\{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis measurement.

Here, we give a concrete example to demonstrate how U_{od}^k affects the QW state. Suppose that the initial QW state is $|3\rangle|0\rangle$, $d = 8$, and $k \in [-3, 5)$. After theoretical calculation, we can easily obtain the probability distribution of positions of walker particle from $|3\rangle|0\rangle$ in first k steps of ODQWC, which is shown in Table B1 for clarity. Here, p denotes the position where the walker particle is located. According to Table B1, when $k \in [0, 5)$, the position of the walker particle is equal to or bigger than 3; and when $k \in [-3, 0)$, the position of the walker particle is smaller than 3.

Table B1 Probability distribution of positions of walker particle from $|3\rangle|0\rangle$ in first k steps of ODQWC derived from theoretical calculation

k \ p	0	1	2	3	4	5	6	7
−3	1/4	1/2	1/4	–	–	–	–	–
−2	–	1/2	1/2	–	–	–	–	–
−1	–	–	1	–	–	–	–	–
0	–	–	–	1	–	–	–	–
1	–	–	–	1/2	1/2	–	–	–
2	–	–	–	1/4	1/2	1/4	–	–
3	–	–	–	1/8	1/8	5/8	1/8	–
4	–	–	–	1/16	1/8	1/8	5/8	1/16

Appendix C The proposed MQPC protocol with two TPs based on ODQWC

Assume that there are n users $P_1, P_2, \cdots, P_n$, and the private integer of P_i can be represented as p_i, where $p_i \in [0, p_0]$, p_0 is an integer located in the range $\left[1, \left\lfloor \frac{d-1}{2} \right\rfloor\right]$ and $i \in \{1, 2, \cdots, n\}$. Suppose that P_i desires to finish comparing the size relationship between her private integer and the ones from the remaining users within one execution of the protocol on the basis of not leaking out them, with the help of two semi-honest TPs, TP_1 and TP_2. Here, either TP is permitted to perform any possible attacks but cannot conspire with others. We put forward a novel MQPC protocol with two TPs based on ODQWC to accomplish this task, which is made up of the following steps.

Step 1: By virtue of a secure QKD protocol [24], P_i pre-shares a private key k_i with TP_1, where $k_i \in [0, d)$ and $i \in \{1, 2, \cdots, n\}$. Moreover, $P_1, P_2, \cdots, P_n$ pre-share a private integer q among them through a secure multi-party QKD protocol, where $q \in [0, d)$.

Step 2: TP_1 prepares m copies initial QW states all in the state of $|\psi_0\rangle = |p_0\rangle|0\rangle$. TP_1 needs to keep the value of p_0 in mind. In order to disguise the particles of m copies $|\psi_0\rangle$, TP_1 generates λ decoy particles randomly within the $Z_d = \{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$ basis or the $X_d = \{\mathcal{F}|0\rangle, \mathcal{F}|1\rangle, \cdots, \mathcal{F}|d-1\rangle\}$ basis, where $\mathcal{F}$ means the quantum Fourier transform defined as

$$\mathcal{F}|l\rangle = \frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l \varphi}{d}} |\varphi\rangle \tag{C1}$$

and $l \in \{0, 1, \cdots, d-1\}$. After that, TP_1 randomly inserts λ decoy particles in m copies $|\psi_0\rangle$ to form a new sequence of $2m + \lambda$ particles. Lastly, TP_1 distributes this particle sequence to P_i via a quantum channel. Here, $i \in \{1, 2, \cdots, n\}$.

Step 3: TP_1 declares the concrete positions and the preparing basis of λ decoy particles. P_i measures the corresponding decoy particles with the preparing basis TP_1 told and returns the measurement results to TP_1. TP_1 calculates the error rate by comparing P_i's measurement results on decoy particles and their initial prepared states. If the error rate is acceptable, the communication will be continued; otherwise, the communication will be terminated.

Step 4: P_i calculates an encrypted integer

$$v_i = k_i + p_i + q, \tag{C2}$$

and applies $U_{od}^{v_i}$ on $|\psi_0\rangle$ to get

$$|\psi_1^i\rangle = U_{od}^{v_i} |\psi_0\rangle. \tag{C3}$$

Then, P_i generates λ decoy particles randomly within the Z_d basis or the X_d basis and randomly inserts them into m copies $|\psi_1^i\rangle$ to form a new sequence of $2m + \lambda$ particles. Finally, P_i sends this particle sequence to TP_2 via a quantum channel, and conveys v_i through a classical channel. Here, $i \in \{1, 2, \cdots, n\}$.

Step 5: P_i and TP_2 implement the security check process in the way same to Step 3. When the quantum channel is secure, TP_2 normally acquires m copies $|\psi_1^i\rangle$ and v_i from P_i, where $i \in \{1, 2, \cdots, n\}$. TP_2 imposes $U_{od}^{-v_i}$ on $|\psi_1^j\rangle$ to gain

$$|\psi_2^{ij}\rangle = U_{od}^{-v_i} |\psi_1^j\rangle, \tag{C4}$$

where $j \in \{1, 2, \cdots, n\}$ and $j \neq i$. Then, TP_2 generates λ decoy particles randomly within the Z_d basis or the X_d basis, and randomly inserts them into m copies $|\psi_2^{ij}\rangle$ to form a new sequence of $2m + \lambda$ particles. Finally, TP_2 transfers this particle sequence to TP_1 via a quantum channel.

Step 6: TP_1 and TP_2 implement the security check process in the way same to Step 3. When the quantum channel is secure, TP_1 normally acquires m copies $|\psi_2^{ij}\rangle$ from TP_2, where $i, j \in \{1, 2, \cdots, n\}$ and $j \neq i$. TP_1 imposes $U_{od}^{k_i}$ and $U_{od}^{-k_j}$ on $|\psi_2^{ij}\rangle$, and gets

$$|\psi_3^{ij}\rangle = U_{od}^{-k_j} U_{od}^{k_i} |\psi_2^{ij}\rangle. \tag{C5}$$

Here, $i, j \in \{1, 2, \cdots, n\}$ and $j \neq i$. Afterwards, TP_1 measures the walker particles of m copies $|\psi_3^{ij}\rangle$ within the Z_d basis. There are three cases that may happen:

1) After the Z_d basis measurements of TP_1, all walker particles' positions are collapsed into the original position p_0. In this case, it has $p_j = p_i$;

2) After the Z_d basis measurements of TP_1, a number of walker particles' positions are collapsed into the positions bigger than p_0, while the remaining walker particles' positions are collapsed into the original position p_0. In this case, it has $p_j > p_i$;

3) After the Z_d basis measurements of TP_1, all walker particles' positions are collapsed into the positions smaller than p_0. In this case, it has $p_j < p_i$.

TP_1 publishes the comparison result of p_j and p_i to P_i and P_j, respectively.

For clarity, the flow chart of the above protocol is shown schematically as Fig. C1 after the security check processes are omitted. Within one execution of protocol, the proposed protocol can achieve the size relationship comparison between P_i ($i \in \{1, 2, \cdots, n\}$) and the remaining users. After we execute the proposed protocol framework for n times, we can realize the size comparison for arbitrary two users among $P_1, P_2, \cdots, P_n$.

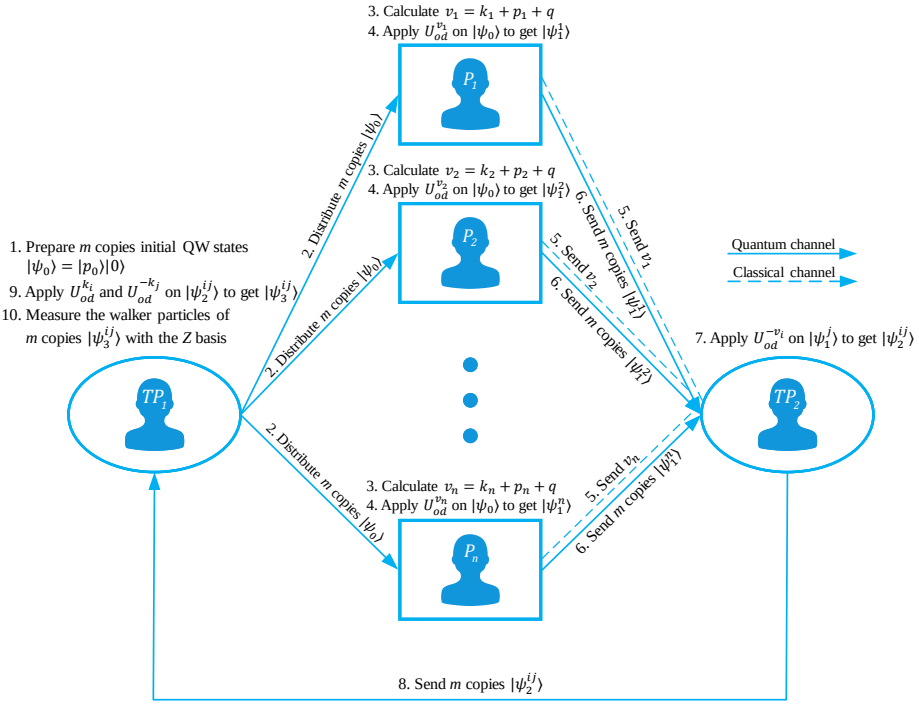

Figure C1 Procedure of the proposed MQPC protocol without the security check processes

Appendix D Concrete examples

Here we give a specific example to further demonstrate the correctness of the proposed protocol.

Suppose that $d = 8$ and $p_0 = \left\lfloor \frac{d-1}{2} \right\rfloor = 3$; P_1's private integer is $p_1 = 2$, while P_2's private integer is $p_2 = 1$; P_1 pre-shares $k_1 = 1$ with TP_1, while P_2 pre-shares $k_2 = 2$ with TP_1; and moreover, P_1 and P_2 pre-share $q = 1$.

TP_1 prepares $2m$ copies initial QW states all in the state of $|\psi_0\rangle = |p_0\rangle|0\rangle = |3\rangle|0\rangle$. Then, TP_1 distributes m copies $|\psi_0\rangle$ to P_1 and m copies $|\psi_0\rangle$ to P_2.

Afterward, P_1 calculates

$$v_1 = k_1 + p_1 + q = 1 + 2 + 1 = 4, \tag{D1}$$

applies $U_{od}^{v_1}$ on $|\psi_0\rangle$ to get

$$|\psi_1^1\rangle = U_{od}^{v_1}|\psi_0\rangle = U_{od}^{4}|\psi_0\rangle, \tag{D2}$$

and then transmits m copies $|\psi_1^1\rangle$ and v_1 to TP_2. In the meanwhile, P_2 calculates

$$v_2 = k_2 + p_2 + q = 2 + 1 + 1 = 4, \tag{D3}$$

applies $U_{od}^{v_2}$ on $|\psi_0\rangle$ to get

$$|\psi_1^2\rangle = U_{od}^{v_2}|\psi_0\rangle = U_{od}^{4}|\psi_0\rangle, \tag{D4}$$

and then transmits m copies $|\psi_1^2\rangle$ and v_2 to TP_2.

TP_2 receives m copies $|\psi_1^1\rangle$ and v_1 from P_1, as well as m copies $|\psi_1^2\rangle$ and v_2 from P_2. Without loss of generality, in order to obtain the comparison result of p_1 and p_2, assume that TP_2 applies $U_{od}^{-v_1}$ on $|\psi_1^2\rangle$ to get

$$|\psi_2^{12}\rangle = U_{od}^{-v_1}|\psi_1^2\rangle = U_{od}^{-4}|\psi_1^2\rangle = |\psi_0\rangle, \tag{D5}$$

and transmits m copies $|\psi_2^{12}\rangle$ to TP_1.

TP_1 receives m copies $|\psi_2^{12}\rangle$ from TP_2. TP_1 applies $U_{od}^{k_1}$ and $U_{od}^{-k_2}$ on $|\psi_2^{12}\rangle$ to obtain

$$\begin{aligned} |\psi_3^{12}\rangle &= U_{od}^{-2}U_{od}^{1}|\psi_2^{12}\rangle = U_{od}^{-1}|\psi_0\rangle \\ &= U_{od}^{-1}|3\rangle|0\rangle = \frac{1}{\sqrt{2}}\big(|2\rangle|0\rangle + |2\rangle|1\rangle\big). \end{aligned} \tag{D6}$$

In the end, TP_1 measures the walker particles of m copies $|\psi_3^{12}\rangle$ within the Z_d basis. Apparently, TP_1 obtains the measurement results $|2\rangle$ with a probability of 100%. Hence, TP_1 can concludes that $p_2 < p_1$.

Appendix E Correctness analysis

Appendix E.1 Proof of Lemma 1

Lemma 1. In an ODQWC system, it has $U_{od}^{-a}U_{od}^{b}=U_{od}^{b-a}$. Specially, when $a=b$, it has $U_{od}^{-a}U_{od}^{b}=I_{2d}$. Here, I_{2d} is the identity matrix of size $2d\times 2d$, $a,b\in\mathbb{Z}^{+}\cup\{0\}$ and $\mathbb{Z}^{+}$ is the positive integer set.

Proof. Ref. [26] has proved that $T_xT_y=T_{x+y}$ for $x,y\in(-d,d)$. According to this proof, it is easy to derive that $T_xT_y=T_{x+y}$ for $\forall x,y\in\mathbb{Z}$. As a result, it has

$$\begin{aligned}S_{od}^{-1}S_{od}&=\big(T_{-1}\otimes|0\rangle\langle 0|+T_0\otimes|1\rangle\langle 1|\big)\cdot\big(T_1\otimes|0\rangle\langle 0|+T_0\otimes|1\rangle\langle 1|\big)\\&=T_0\otimes\big(|0\rangle\langle 0|+|1\rangle\langle 1|\big)=T_0\otimes I_2.\end{aligned}\tag{E.1-1}$$

According to Eq. (E.1-1), it has

$$\begin{aligned}U_{od}^{-1}U_{od}&=\big(I_d\otimes H^{-1}\big)S_{od}^{-1}\cdot S_{od}\big(I_d\otimes H\big)\\&=\big(I_d\otimes H\big)\big(T_0\otimes I_2\big)\big(I_d\otimes H\big)\\&=\big(T_0\otimes H\big)\big(I_d\otimes H\big)=T_0\otimes I_2\\&=\sum_{i=0}^{d-1}|i\rangle\langle i|\otimes I_2=I_d\otimes I_2.\end{aligned}\tag{E.1-2}$$

According to Eq. (E.1-2), it has

$$\begin{aligned}U_{od}^{-a}U_{od}^{b}&=U_{od}^{-(a-1)}\big(U_{od}^{-1}U_{od}\big)U_{od}^{b-1}\\&=U_{od}^{-(a-1)}\big(I_d\otimes I_2\big)U_{od}^{b-1}.\end{aligned}\tag{E.1-3}$$

There are three cases needed to be discussed:

1) When $a=b$, Eq. (E.1-3) can be rewritten into

$$\begin{aligned}U_{od}^{-a}U_{od}^{b}&=U_{od}^{-(a-1)}\big(I_d\otimes I_2\big)U_{od}^{b-1}\\&=U_{od}^{-(a-2)}\big(U_{od}^{-1}U_{od}\big)U_{od}^{b-2}\\&=U_{od}^{-(a-2)}\big(I_d\otimes I_2\big)U_{od}^{b-2}\\&\ \ \vdots\\&=I_d\otimes I_2=I_{2d}.\end{aligned}\tag{E.1-4}$$

2) When $a>b$, Eq. (E.1-3) can be rewritten into

$$U_{od}^{-a}U_{od}^{b}=U_{od}^{-(a-1)}(I_d\otimes I_2)U_{od}^{b-1}=U_{od}^{-(a-2)}\big(I_d\otimes I_2\big)U_{od}^{b-2}=\cdots=U_{od}^{-(a-b)}.\tag{E.1-5}$$

3) When $a<b$, Eq. (E.1-3) can be rewritten into

$$U_{od}^{-a}U_{od}^{b}=U_{od}^{-(a-1)}\big(I_d\otimes I_2\big)U_{od}^{b-1}=U_{od}^{-(a-2)}\big(I_d\otimes I_2\big)U_{od}^{b-2}=\cdots=U_{od}^{b-a}.\tag{E.1-6}$$

Until now, the proof of Lemma 1 has been completed.

Appendix E.2 Proof of Lemma 2

Lemma 2. In ODQWC, when U_{od}^{k} is performed on the initial QW state $|p_0\rangle|0\rangle$, where $k\in[1,d-p_0)\cap\mathbb{Z}$ and p_0 is an integer located in the range $\left[1,\left\lfloor\frac{d-1}{2}\right\rfloor\right]$, the walker particle's position is collapsed into the position equal to or bigger than p_0 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position p_0+k is $\left(\frac{1}{2}\right)^k$.

Proof. This proof is developed from Lemma 1 in Ref. [27].

1) When $k=1$, it has

$$\begin{aligned}U_{od}\,|p_0\rangle|0\rangle&=S_{od}\cdot\big(I_d\otimes C\big)\,|p_0\rangle|0\rangle\\&=\frac{1}{\sqrt{2}}S_{od}\cdot\big(|p_0\rangle|0\rangle+|p_0\rangle|1\rangle\big)\\&=\frac{1}{\sqrt{2}}\big(|p_0+1\rangle|0\rangle+|p_0\rangle|1\rangle\big).\end{aligned}\tag{E.2-1}$$

According to Eq. (E.2-1), when U_{od} is performed on the initial QW state $|p_0\rangle|0\rangle$, the walker particle's position may be collapsed into the position p_0 or p_0+1 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position p_0+1 is $\frac{1}{2}$.

2) Suppose that as for $1<j<d-p_0-1$ and $j\in\mathbb{Z}$, when $k=j$, it has

$$U_{od}^{j}\,|p_0\rangle|0\rangle=\sum_{i=0}^{j}\big(\alpha_i\,|p_0+i\rangle|0\rangle+\beta_i\,|p_0+i\rangle|1\rangle\big),\tag{E.2-2}$$

where $\alpha_0 = 0 \neq \beta_0$, $|\alpha_i|^2 + |\beta_i|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j-1$, $\beta_j = 0$ and $|\alpha_j|^2 = \left(\frac{1}{2}\right)^j$. In other words, when U_{od}^j is performed on the initial QW state $|p_0\rangle|0\rangle$, the walker particle's position may be collapsed into the position equal to or bigger than p_0 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position $p_0 + j$ is $\left(\frac{1}{2}\right)^j$.

When $k = j+1$, according to Eq. (E.2-2), it has

$$\begin{aligned}
&U_{od}^{j+1}|p_0\rangle|0\rangle = U_{od}U_{od}^j|p_0\rangle|0\rangle \\
&= S_{od}\cdot\left(I_d\otimes C\right)\sum_{i=0}^{j}\left(\alpha_i|p_0+i\rangle|0\rangle + \beta_i|p_0+i\rangle|1\rangle\right) \\
&= \sum_{i=0}^{j}\Big[\frac{\alpha_i}{\sqrt{2}}\left(|p_0+i+1\rangle|0\rangle + |p_0+i\rangle|1\rangle\right) + \frac{\beta_i}{\sqrt{2}}\left(|p_0+i+1\rangle|0\rangle - |p_0+i\rangle|1\rangle\right)\Big] \\
&= \sum_{i=0}^{j}\Big(\frac{\alpha_i+\beta_i}{\sqrt{2}}|p_0+i+1\rangle|0\rangle + \frac{\alpha_i-\beta_i}{\sqrt{2}}|p_0+i\rangle|1\rangle\Big) \\
&= \frac{\alpha_0-\beta_0}{\sqrt{2}}|p_0\rangle|1\rangle + \sum_{i=1}^{j}\Big(\frac{\alpha_{i-1}+\beta_{i-1}}{\sqrt{2}}|p_0+i\rangle|0\rangle + \frac{\alpha_i-\beta_i}{\sqrt{2}}|p_0+i\rangle|1\rangle\Big) + \frac{\alpha_j+\beta_j}{\sqrt{2}}|p_0+j+1\rangle|0\rangle.
\end{aligned} \tag{E.2-3}$$

Let

$$\alpha_i' = \begin{cases} 0, & i = 0 \\ \dfrac{\alpha_i - 1 + \beta_{i-1}}{\sqrt{2}}, & 1 \leqslant i \leqslant j+1 \end{cases} \tag{E.2-4}$$

and

$$\beta_i' = \begin{cases} \dfrac{\alpha_i - \beta_i}{\sqrt{2}}, & 0 \leqslant i \leqslant j \\ 0, & i = j+1 \end{cases}, \tag{E.2-5}$$

thus Eq. (E.2-3) can be rewritten as

$$U_{od}^{j+1}|p_0\rangle|0\rangle = \sum_{i=0}^{j+1}\left(\alpha_i'|p_0+i\rangle|0\rangle + \beta_i'|p_0+i\rangle|1\rangle\right). \tag{E.2-6}$$

Due to $\alpha_0 = 0 \neq \beta_0$, $\alpha_0' = 0$ and $\beta_0' = \frac{\alpha_0-\beta_0}{\sqrt{2}}$, it has

$$\alpha_0' = 0 \neq \beta_0'. \tag{E.2-7}$$

According to Eq. (E.2-7), when U_{od}^{j+1} is performed on the initial QW state $|p_0\rangle|0\rangle$, the walker particle's position may be collapsed into the position p_0 after the walker particle is performed with the Z_d basis measurement.

Due to $\beta_j = 0$, $|\alpha_j|^2 = \left(\frac{1}{2}\right)^j$ and $\alpha_{j+1}' = \frac{\alpha_j+\beta_j}{\sqrt{2}}$, it has

$$|\alpha_{j+1}'|^2 = \left|\frac{\alpha_j+\beta_j}{\sqrt{2}}\right|^2 = \left(\frac{1}{2}\right)^{j+1}. \tag{E.2-8}$$

According to Eq. (E.2-8) and $\beta_{j+1}' = 0$, when U_{od}^{j+1} is performed on the initial QW state $|p_0\rangle|0\rangle$, after the walker particle is performed with the Z_d basis measurement, the probability of the walker particle's position being collapsed into the position $p_0 + j + 1$ is $\left(\frac{1}{2}\right)^{j+1}$.

On the basis of Eq. (E.2-4) and Eq. (E.2-5), it has

$$|\alpha_i'|^2 + |\beta_i'|^2 = \begin{cases} \left|\dfrac{\alpha_i-\beta_i}{\sqrt{2}}\right|^2, & i = 0 \\ \left|\dfrac{\alpha_{i-1}+\beta_{i-1}}{\sqrt{2}}\right|^2 + \left|\dfrac{\alpha_i-\beta_i}{\sqrt{2}}\right|^2, & 1 \leqslant i \leqslant j \\ \left|\dfrac{\alpha_{i-1}+\beta_{i-1}}{\sqrt{2}}\right|^2, & i = j+1 \end{cases}. \tag{E.2-9}$$

Then, it can be proved by contradiction that $|\alpha_i'|^2 + |\beta_i'|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j$. To make $|\alpha_i'|^2 + |\beta_i'|^2 = 0$ be true for all $1 \leqslant i \leqslant j$, both $\alpha_{i-1} = -\beta_{i-1}$ and $\alpha_i = \beta_i$ must be satisfied. In other words, it has to be simultaneously satisfied that $\alpha_0 = -\beta_0$, $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = \cdots = \alpha_{j-1} = \beta_{j-1} = 0$ and $\alpha_j = \beta_j$, which violate $\alpha_0 = 0 \neq \beta_0$, $|\alpha_i'|^2 + |\beta_i'|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j-1$, as well as $\beta_j = 0$ and $|\alpha_j|^2 = \left(\frac{1}{2}\right)^j$. As a result, $|\alpha_i'|^2 + |\beta_i'|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j$.

Until now, the proof of Lemma 2 has been completed.

Appendix E.3 Proof of Lemma 3

Lemma 3. In ODQWC, when U_{od}^{-k} is performed on the initial QW state $|p_0\rangle|0\rangle$, where $k \in [1, p_0] \cap \mathbb{Z}$ and p_0 is an integer located in the range $\left[1, \left\lfloor\frac{d-1}{2}\right\rfloor\right]$, the walker particle's position is collapsed into the position smaller than p_0 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position $p_0 - k$ is $\left(\frac{1}{2}\right)^{k-1}$.

Proof. This proof is developed from Lemma 2 in Ref. [27].

1) When $k=1$, it has

$$\begin{aligned} U_{od}^{-1}\,|p_0\rangle|0\rangle &= \left(I_d\otimes C^{-1}\right)\cdot S_{od}^{-1}\,|p_0\rangle|0\rangle \\ &= \left(I_d\otimes C^{-1}\right)|p_0-1\rangle|0\rangle \\ &= |p_0-1\rangle\otimes\frac{1}{\sqrt{2}}\big(|0\rangle+|1\rangle\big). \end{aligned} \tag{E.3-1}$$

According to Eq. (E.3-1), when U_{od}^{-1} is performed on the initial QW state $|p_0\rangle|0\rangle$, the walker particle's position may be collapsed into the position p_0-1 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position p_0-1 is 1.

2) Suppose that as for $1<j<p_0$ and $j\in\mathbb{Z}$, when $k=j$, it has

$$U_{od}^{-j}\,|p_0\rangle|0\rangle=\sum_{i=1}^{j}|p_0-i\rangle\otimes\left(\gamma_i\,|0\rangle+\delta_i\,|1\rangle\right), \tag{E.3-2}$$

where $|\gamma_i|^2+|\delta_i|^2=0$ is not necessarily true for all $1\leqslant i\leqslant j-1$ and $|\gamma_j|^2=|\delta_j|^2=\left(\frac{1}{2}\right)^j$. In other words, when U_{od}^{-j} is performed on the initial QW state $|p_0\rangle|0\rangle$, the walker particle's position is collapsed into the position smaller than p_0 after the walker particle is performed with the Z_d basis measurement; moreover, the probability of the walker particle's position being collapsed into the position p_0-j is $\left(\frac{1}{2}\right)^{j-1}$.

When $k=j+1$, according to Eq. (E.3-2), it has

$$\begin{aligned} &U_{od}^{-(j+1)}\,|p_0\rangle|0\rangle = U_{od}^{-1}U_{od}^{-j}\,|p_0\rangle|0\rangle \\ &=\left(I_d\otimes C^{-1}\right)\cdot S_{od}^{-1}\sum_{i=1}^{j}|p_0-i\rangle\otimes\left(\gamma_i\,|0\rangle+\delta_i\,|1\rangle\right) \\ &=\left(I_d\otimes C^{-1}\right)\cdot\sum_{i=1}^{j}\left(\gamma_i\,|p_0-i-1\rangle|0\rangle+\delta_i\,|p_0-i\rangle|1\rangle\right) \\ &=\sum_{i=1}^{j}\Big[|p_0-i-1\rangle\otimes\frac{\gamma_i}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)+|p_0-i\rangle\otimes\frac{\delta_i}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)\Big] \\ &=|p_0-1\rangle\otimes\frac{\delta_1}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)+\sum_{i=2}^{j}|p_0-i\rangle\otimes\Big[\frac{\gamma_{i-1}}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)+\frac{\delta_i}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)\Big]+|p_0-j-1\rangle\otimes\frac{\gamma_i}{\sqrt{2}}\big(|0\rangle+|1\rangle\big). \end{aligned} \tag{E.3-3}$$

Let

$$\gamma_i'=\begin{cases}\dfrac{\delta_i}{\sqrt{2}}, & i=1\\ \dfrac{\gamma_{i-1}+\delta_i}{\sqrt{2}}, & 2\leqslant i\leqslant j\\ \dfrac{\gamma_{i-1}}{\sqrt{2}}, & i=j+1\end{cases} \tag{E.3-4}$$

and

$$\delta_i'=\begin{cases}-\dfrac{\delta_i}{\sqrt{2}}, & i=1\\ \dfrac{\gamma_{i-1}-\delta_i}{\sqrt{2}}, & 2\leqslant i\leqslant j\\ \dfrac{\gamma_{i-1}}{\sqrt{2}}, & i=j+1\end{cases}, \tag{E.3-5}$$

thus Eq. (E.3-3) can be rewritten as

$$U_{od}^{-(j+1)}\,|p_0\rangle|0\rangle=\sum_{i=1}^{j+1}|p_0-i\rangle\otimes\left(\gamma_i'\,|0\rangle+\delta_i'\,|1\rangle\right). \tag{E.3-6}$$

Due to $|\gamma_j|^2=|\delta_j|^2=\left(\frac{1}{2}\right)^j$, $\gamma_{j+1}'=\frac{\gamma_j}{\sqrt{2}}$ and $\delta_{j+1}'=\frac{\gamma_j}{\sqrt{2}}$, it has

$$\left|\gamma_{j+1}'\right|^2=\left|\delta_{j+1}'\right|^2=\left(\frac{1}{2}\right)^{j+1}. \tag{E.3-7}$$

According to Eq. (E.3-7), when $U_{od}^{-(j+1)}$ is performed on the initial QW state $|p_0\rangle|0\rangle$, after the walker particle is performed with the Z_d basis measurement, the probability of the walker particle's position being collapsed into the position $p_0-(j+1)$ is $\left(\frac{1}{2}\right)^j$.

On the basis of Eq. (E.3-4) and Eq. (E.3-5), it has

$$\left|\gamma_i'\right|^2+\left|\delta_i'\right|^2=\begin{cases}|\delta_i|^2, & i=1\\ \dfrac{1}{2}|\gamma_{i-1}+\delta_i|^2+\dfrac{1}{2}|\gamma_{i-1}-\delta_i|^2, & 2\leqslant i\leqslant j\\ |\gamma_{i-1}|^2, & i=j+1\end{cases}. \tag{E.3-8}$$

Then, it can be proved by contradiction that $\left|\gamma_i'\right|^2+\left|\delta_i'\right|^2=0$ is not necessarily true for all $1\leqslant i\leqslant j$. To make $\left|\gamma_i'\right|^2+\left|\delta_i'\right|^2=0$ be true for all $1\leqslant i\leqslant j$, both $\delta_1=0$ and $\gamma_{i-1}=-\delta_i=\delta_i$ for $2\leqslant i\leqslant j-1$ must be satisfied. In other words, it has to be

simultaneously satisfied that $\delta_j = \gamma_{j-1} = ... = \delta_3 = \gamma_2 = \delta_2 = \gamma_1 = \delta_1 = 0$, which violate $|\gamma_i|^2 + |\delta_i|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j-1$ and $|\gamma_j|^2 = |\delta_j|^2 = \left(\frac{1}{2}\right)^j$. As a result, $\left|\gamma_i'\right|^2 + \left|\delta_i'\right|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j$.

Because $1 < j < p_0$ and $j \in \mathbb{Z}$, according to Eq. (E.3-6), Eq. (E.3-7) and the conclusion that $\left|\gamma_i'\right|^2 + \left|\delta_i'\right|^2 = 0$ is not necessarily true for all $1 \leqslant i \leqslant j$, the walker particle's position is collapsed into the position smaller than p_0 after the walker particle is performed with the Z_d basis measurement.

Until now, the proof of Lemma 3 has been completed.

Appendix F Security analysis

Appendix F.1 Outside attack

In the proposed protocol, there are three times quantum state transmissions, i.e., TP_1 distributes a particle sequence including m copies $|\psi_0\rangle$ to P_i, where $i \in \{1, 2, \cdots, n\}$; P_i distributes a particle sequence including m copies $\left|\psi_1^i\right\rangle$ to TP_2; and TP_2 transfers a particle sequence including m copies $\left|\psi_2^{ij}\right\rangle$ to TP_1, where $j \in \{1, 2, \cdots, n\}$ and $j \neq i$. During each quantum state transmission, decoy particles randomly within the Z_d basis or the X_d basis are adopted to guarantee the security against the attacks from an outside eavesdropper, Eve. In other words, the decoy particle technology within the d-dimensional quantum system is used to ensure the security for each quantum state transmission. Note that the effectiveness of decoy particle technology within the two-dimensional quantum system against Eve has been validated in detail in Ref. [33]. In the following, we will take TP_1 distributing a particle sequence including m copies $|\psi_0\rangle$ to P_i for example to illustrate the effectiveness of decoy particle technology within the d-dimensional quantum system against Eve.

(1) Intercept-resend attack

Eve may perform the intercept-resend attack as follows: she intercepts the particle sequence sent out from P_i and sends the fake particles prepared beforehand by herself to P_i. According to Ref. [22], with respect to one decoy particle, the probability that Eve's intercept-resend attack on one decoy particle can be discovered by TP_1 and P_i is $\frac{d-1}{d}$. As a result, Eve's intercept-resend attack on λ decoy particles can be discovered by TP_1 and P_i with the probability of $1 - \left(\frac{1}{d}\right)^\lambda$, which will converge to 1 if λ is large enough.

(2) Measure-resend attack

Eve may perform the measure-resend attack as follows: after intercepting the particle sequence sent out from TP_1, she measures its particles randomly with the Z_d basis or the X_d basis, and resends the measured states to P_i. According to Ref. [22], with respect to one decoy particle, the probability that Eve's measure-resend attack on one decoy particle can be discovered by TP_1 and P_i is $\frac{d-1}{2d}$. As a result, Eve's measure-resend attack on λ decoy particles can be discovered by TP_1 and P_i with the probability of $1 - \left(\frac{d+1}{2d}\right)^\lambda$, which will be also near to 1 if λ is large enough.

(3) Entangle-measure attack

Eve may lunch her entangle-measure attack as follows: Eve entangles her auxiliary particle $|\vartheta\rangle$ with the particle sent out from TP_1 through the unitary operation $\mathcal{U}_\mathcal{E}$, and then tries to measure her auxiliary particle to acquire useful information.

Proposition F1. Eve launches her entangle-measure attack as above. In order to incur no error during the security check between TP_1 and P_i, where $i \in \{1, 2, \cdots, n\}$, Eve's final probe state should be independent from the particle sent out from TP_1.

Proof. 1) The particle sent out from TP_1 within the Z_d basis is represented as $|l\rangle$. On the ground of Ref. [22], after Eve imposes $\mathcal{U}_\mathcal{E}$, the global state of the composite system becomes

$$\mathcal{U}_\mathcal{E}\left(|l\rangle|\vartheta\rangle\right) = \sum_{l'=0}^{d-1} \xi_{ll'} |l'\rangle|\vartheta_{ll'}\rangle, \tag{F1}$$

where $|\vartheta_{ll'}\rangle$ $(l, l' \in \{0, 1, \cdots, d-1\})$ is Eve's probe state and

$$\sum_{l'=0}^{d-1} \left|\xi_{ll'}\right|^2 = 1. \tag{F2}$$

In order to incur no error during the security check between TP_1 and P_i, it should satisfy

$$\xi_{ll'} = \begin{cases} \xi_{ll'}, & if \quad l' = l; \\ 0, & if \quad l' \neq l. \end{cases} \tag{F3}$$

As a result, Eq. (F1) is degenerated into

$$\mathcal{U}_\mathcal{E}\left(|l\rangle|\vartheta\rangle\right) = \xi_{ll} |l\rangle|\vartheta_{ll}\rangle. \tag{F4}$$

2) The particle sent out from TP_1 within the X_d basis is represented as $|\mathcal{F}_l\rangle$, where $|\mathcal{F}_l\rangle = \mathcal{F}|l\rangle = \frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l\varphi}{d}} |\varphi\rangle$ and $l \in \{0, 1, \cdots, d-1\}$. On the ground of Ref. [22], after Eve imposes $\mathcal{U}_\mathcal{E}$, the global state of the composite system becomes

$$\begin{aligned} \mathcal{U}_\mathcal{E}\left(|\mathcal{F}_l\rangle|\vartheta\rangle\right) &= \mathcal{U}_\mathcal{E}\left[\left(\frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l\varphi}{d}} |\varphi\rangle\right)|\vartheta\rangle\right] \\ &= \frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l\varphi}{d}} \mathcal{U}_\mathcal{E}\left(|\varphi\rangle|\vartheta\rangle\right). \end{aligned} \tag{F5}$$

Inserting Eq. (F4) into Eq. (F5) generates

$$\mathcal{U}_\mathcal{E}\left(|\mathcal{F}_l\rangle|\vartheta\rangle\right) = \frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l\varphi}{d}} \xi_{\varphi\varphi} |\varphi\rangle|\vartheta_{\varphi\varphi}\rangle. \tag{F6}$$

In the light of the inverse discrete quantum Fourier transform, it has

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{\partial=0}^{d-1} e^{-\frac{2\pi i \partial \varphi}{d}} |\mathcal{F}_\partial\rangle. \tag{F7}$$

Inserting Eq. (F7) into Eq. (F6) generates

$$\begin{aligned} \mathcal{U}_{\mathcal{E}}\left(|\mathcal{F}_l\rangle|\vartheta\rangle\right) &= \frac{1}{\sqrt{d}} \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i l \varphi}{d}} \xi_{\varphi\varphi} \left(\frac{1}{\sqrt{d}} \sum_{\partial=0}^{d-1} e^{-\frac{2\pi i \partial \varphi}{d}} |\mathcal{F}_\partial\rangle \right) |\vartheta_{\varphi\varphi}\rangle \\ &= \frac{1}{d} \sum_{\partial=0}^{d-1} |\mathcal{F}_\partial\rangle \sum_{\varphi=0}^{d-1} e^{\frac{2\pi i (l-\partial) \varphi}{d}} \xi_{\varphi\varphi} |\vartheta_{\varphi\varphi}\rangle. \end{aligned} \tag{F8}$$

In order to incur no error during the security check between TP_1 and P_i, it should satisfy

$$\sum_{\varphi=0}^{d-1} e^{\frac{2\pi i (l-\partial) \varphi}{d}} \xi_{\varphi\varphi} |\vartheta_{\varphi\varphi}\rangle = \begin{cases} \sum_{\varphi=0}^{d-1} \xi_{\varphi\varphi} |\vartheta_{\varphi\varphi}\rangle, & if \quad \partial = l; \\ 0, & if \quad \partial \neq l. \end{cases} \tag{F9}$$

When $\partial \neq l$, it has

$$\sum_{\varphi=0}^{d-1} e^{\frac{2\pi i (l-\partial) \varphi}{d}} = 0. \tag{F10}$$

In light of Eq. (F9) and Eq. (F10), it has

$$\xi_{00} |\vartheta_{00}\rangle = \xi_{11} |\vartheta_{11}\rangle = \cdots = \xi_{(d-1)(d-1)} \left|\vartheta_{(d-1)(d-1)}\right\rangle = \xi' |\vartheta'\rangle. \tag{F11}$$

3) Inserting Eq. (F11) into Eq. (F4) generates

$$\mathcal{U}_{\mathcal{E}}\left(|l\rangle|\vartheta\rangle\right) = \xi' |l\rangle|\vartheta'\rangle. \tag{F12}$$

Inserting Eq. (F11) into Eq. (F8) generates

$$\mathcal{U}_{\mathcal{E}}\left(|\mathcal{F}_l\rangle|\vartheta\rangle\right) = \xi' |\mathcal{F}_l\rangle|\vartheta'\rangle. \tag{F13}$$

In light of Eq. (F12) and Eq. (F13), in order to incur no error during the security check between TP_1 and P_i, Eve's final probe state should be independent from the particle sent out from TP_1. Hence, Eve gets nothing useful at all.

(4) Trojan horse attacks

To disable Eve's invisible photon eavesdropping attacks, the receiver can install a wavelength filter in front of her devices to filter out illegal photon signals [34, 35]. To disable Eve's delay-photon Trojan horse attacks, the receiver can install a 50:50 beam splitter to split each sample signal into two parts, measure them via the appropriate measurement bases, and judge whether the multi-photon rate is reasonable or not [34, 35].

Appendix F.2 Inside attack

In 2007, Gao *et al.* [36] indicated that attacks from disloyal participants are always more serious than those by outside eavesdroppers. In this subsection, the security of the proposed protocol against internal attacks is analyzed in detail.

(1) The participant attack from one dishonest user

In the proposed protocol, $P_1, P_2, \cdots, P_n$ are independent and play the similar roles. Without loss of generality, suppose that P_a is the dishonest user who tries her best to obtain p_b, where $a, b \in \{1, 2, \cdots, n\}$ and $a \neq b$. P_a may perform her attacks on the particle sequences sent out from TP_1 to P_b, from P_b to TP_2, and from TP_2 to TP_1, respectively. Since P_a doesn't know the genuine positions and the prepared basis of decoy particles in each particle sequence, she is inevitably detected as an external eavesdropper, just as analyzed in Appendix F.1.

To say the least, even though P_a happens to pass eavesdropper detection and uses the Z basis to measure the walker particles of $\left|\psi_1^b\right\rangle$ she intercepted; however, she still cannot get p_b, due to lack of k_b. Similarly, even though P_a happens to pass eavesdropper detection and uses the Z basis to measure the walker particles of $\left|\psi_2^{cb}\right\rangle$ she intercepted, where $c \in \{1, 2, \cdots, n\}$ and $c \neq b$, she still cannot get p_b, due to lack of k_b and k_c. In addition, P_a may hear of v_b sent out from P_b to TP_2, which is encrypted by k_b; however, due to lack of k_b, P_a still has no opportunity to get p_b.

(2) The participant attack from two or more dishonest users

Here, we consider the extreme situation that $n-1$ dishonest users $P_1, P_2, \cdots, P_{b-1}, P_{b+1}, P_{b+2}, \cdots, P_n$ conspire together to steal p_b, where $b \in \{1, 2, \cdots, n\}$. Even though $P_1, P_2, \cdots, P_{b-1}, P_{b+1}, P_{b+2}, \cdots, P_n$ conspire together, they essentially act as one dishonest user, since $P_1, P_2, \cdots, P_n$ are independent and play the similar roles. According to the analysis in Part (1) of Appendix F.1, the participant attack from $P_1, P_2, \cdots, P_{b-1}, P_{b+1}, P_{b+2}, \cdots, P_n$ is invalid.

(3) The participant attack from semi-honest TP_1

In the proposed protocol, TP_1 may hear of v_i sent out from P_i to TP_2, where $i \in \{1, 2, \cdots, n\}$; however, due to lack of q, TP_1 still has no way to decode out p_i from v_i. TP_1 may also launch her attacks on the particle sequence sent out from P_i to TP_2; however, because of not knowing the genuine positions and the prepared basis of decoy particles, TP_1 is inevitably detected as an outside attacker, just as analyzed in Appendix F.1. TP_1 can receive m copies $\left|\psi_2^{ij}\right\rangle$ from TP_2 and may measure their walker particles with the Z basis, where $i, j \in \{1, 2, \cdots, n\}$ and $j \neq i$; however, TP_1 still cannot know p_i or p_j, due to lack of q. In addition, TP_1 knows the comparison result of p_i and p_j; however, TP_1 still has no way to obtain the genuine value of p_i or p_j.

(4)The participant attack from semi-honest TP_2

In the proposed protocol, TP_2 can acquire $\left|\psi_1^i\right\rangle$ and v_i from P_i, where $i \in \{1, 2, \cdots, n\}$. But TP_2 doesn't know k_i or q. Firstly, TP_2 has no way to deduce p_i from v_i, as p_i is encrypted by k_i and q. Secondly, TP_2 may measure the walker particles of m copies $\left|\psi_1^i\right\rangle$ with the Z basis; however, TP_2 still cannot know p_i, due to lack of k_i, q and p_0. Thirdly, TP_2 may calculate

$$\begin{aligned} v_i - v_j &= \big(k_i + p_i + q\big) - \big(k_j + p_j + q\big) \\ &= \big(k_i - k_j\big) + \big(p_i - p_j\big), \end{aligned} \tag{F14}$$

where $i, j \in \{1, 2, \cdots, n\}$ and $j \neq i$; however, TP_2 still has no way to get p_i or p_j from Eq. (F14). Fourthly, even though TP_2 may hear of the comparison result of p_j and p_i from TP_1, she still has no knowledge about the genuine value of p_i or p_j.

Appendix G Simulation of ODQWC

Suppose that the dimension of $\mathcal{H}_p$ is $d = 2^n$. As a result, it needs n bits to represent a walker particle. Since the dimension of $\mathcal{H}_c$ is 2, it only requires one bit to denote a coin particle. The controlled addition is made up of the standard controlled-not (CNOT) gate, Toffoli gate and generalized Toffoli gates, which can achieve the modulo 2 addition for the target bit of two-qubit, three-qubit, and n-qubit systems, respectively. When all controlling bits from low positions are activated, the target bit adds one. According to Ref. [37], the quantum circuit of controlled addition can be shown as Fig. G1(a), whose function is to calculate the modulo d addition under controls; the quantum circuit of controlled subtraction can be shown as Fig. G1(b), whose function is to calculate the modulo d subtraction under controls; and the quantum circuit of controlled subtraction is the inverse version of controlled addition with the order of gates reversed. There are $n + 1$ qubit registers in each subfigure; and in each subfigure, the first qubit denotes the coin particle, while the n remainders are mapped to the walker particle. Note that the coin qubit always plays the role of a control qubit acting on n walker qubits.

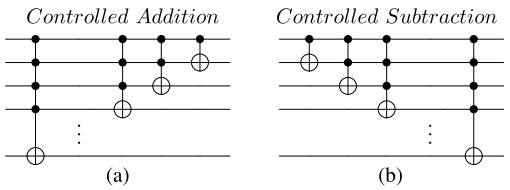

Figure G1 Quantum circuits of controlled addition and controlled subtraction

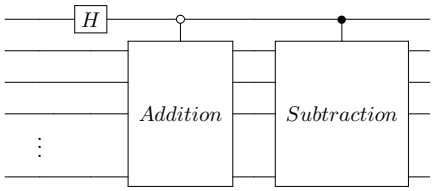

Figure G2 Schematic diagram of two-direction evolution operator for QW on a circle

The schematic diagram of two-direction evolution operator for QW on a circle is presented as Fig. G2, which is composed of a Hadamard gate implemented on the coin qubit, a controlled addition triggered by $|0\rangle$ and a controlled subtraction triggered by $|1\rangle$ according to Ref. [38]. The quantum circuit of two-direction evolution operator for QW on a circle is shown in Fig. G3. Here, the symbol X denotes the NOT gate; the $|0\rangle$ trigger is achieved by the first X gate; and after two X gates, the coming qubit can be restored to its initial state. The quantum circuit of U_{od} in ODQWC is shown in Fig. G4(a), while the quantum circuit of U_{od}^{-1} in ODQWC is shown in Fig. G4(b).

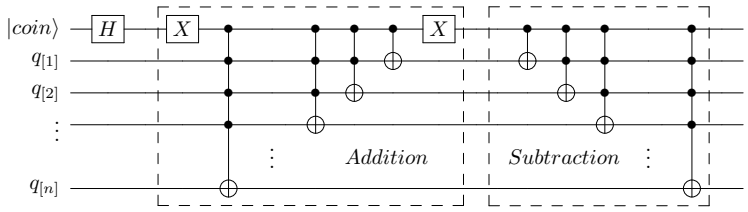

Figure G3 Quantum circuit of two-direction evolution operator for QW on a circle

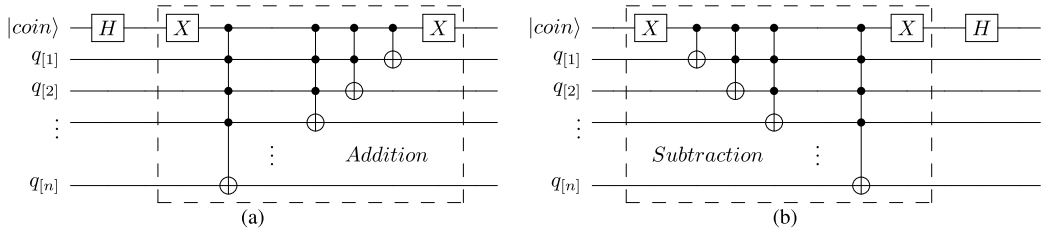

Figure G4 Quantum circuit of U_{od} and U_{od}^{-1} in ODQWC. (a) Quantum circuit of U_{od}. (b) Quantum circuit of U_{od}^{-1}.

Now we verify the correctness of Table B1 by simulating with Qiskit of IBM. Firstly, we construct the simulation circuits of U_{od} and its controlled addition as Fig. G5, and design the simulation circuits of U_{od}^{-1} and its controlled subtraction as Fig. G6. Secondly, we construct the simulation circuits of continuously implementing U_{od} one, two, three and four times on $|3\rangle|0\rangle$, respectively. Thirdly, we construct the simulation circuits of continuously implementing U_{od}^{-1} one, two and three times on $|3\rangle|0\rangle$, respectively. The simulation circuit of continuously implementing U_{od} four times is shown as Fig. G7. Here, the inputs of quantum

registers are on the left of the first barrier; the circuit of implementing U_{od} four times is on the left of the second barrier; and quantum measurement gates on three walker qubits are at the end. The simulation circuit of continuously implementing U_{od}^{-1} three times is shown as Fig. G8, where the circuit of implementing U_{od}^{-1} three times is on the left of the second barrier.

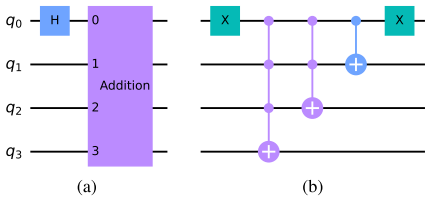

Figure G5 Simulation circuits of U_{od} and its controlled addition. (a) Simulation circuit of U_{od}. (b) Simulation circuit of controlled addition in U_{od}.

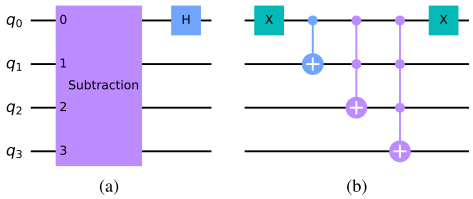

Figure G6 Simulation circuits of U_{od}^{-1} and its controlled subtraction. (a) Simulation circuit of U_{od}^{-1}. (b) Simulation circuit of controlled subtraction in U_{od}^{-1}.

The frequency distribution of positions of walker particle from $|3\rangle|0\rangle$ in first k steps of ODQWC derived from simulation with executing 10,000 shots is shown as Fig. G9(a)-(h). For clarity, Fig. G9 can be further turned into Table G1. Apparently, Table G1 is nearly consistent to Table B1, which implies the correctness of B1. Table G1 also validates Proposition 1 when $d = 8$ and $p_0 = 3$.

In addition, it is easy to find out that when $d \in \left(2^{n-1}, 2^n\right)$, we can use a similar method with $n+1$ qubit registers to obtain the corresponding simulation result.

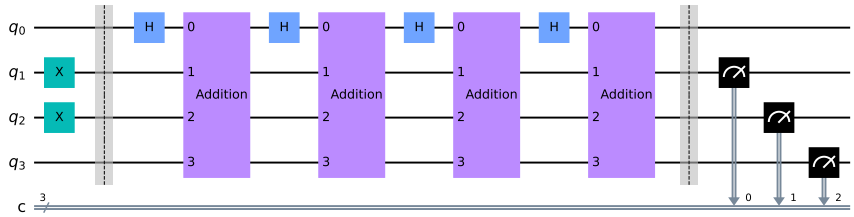

Figure G7 Simulation circuit of continuously implementing U_{od} four times on $|3\rangle|0\rangle$ in ODQWC

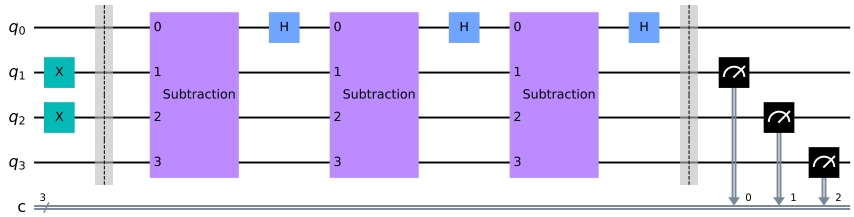

Figure G8 Simulation circuit of continuously implementing U_{od}^{-1} three times on $|3\rangle|0\rangle$ in ODQWC

Appendix H Discussion

In order to evaluate the efficiency performance of a quantum communication protocol within the d-dimensional quantum system, Ref. [39] generalizes qubit efficiency proposed by Ref. [40] to qudit efficiency, which is defined as

$$\eta = \frac{\varepsilon_s}{\varepsilon_q + \varepsilon_c}, \tag{H1}$$

where ε_s is the length of private information compared, ε_q is the number of consumed qudits, and ε_c is the length of classical information used during classical communication.

Here, we compute the qudit efficiency for the proposed protocol after neglecting the resources consumed by the generation of pre-shared QKD keys and security check processes. In the proposed protocol, P_i only has one private integer, thus it has $\varepsilon_s = 1$; TP_1 prepares m copies initial QW states all in the state of $|\psi_0\rangle = |p_0\rangle|0\rangle$ and sends them to P_i, where $i \in \{1, 2, \cdots, n\}$, thus it has $\varepsilon_q = 2mn$; P_i distributes v_i to TP_2, thus it has $\varepsilon_c = n$. Therefore, the qudit efficiency of the proposed protocol is equal to $\eta = \frac{1}{2mn+n}$.

We compare the proposed protocol with previous two QPC protocols based on QW and show the comparison results in Table H1. In light of Table H1, it can be concluded that: (1) only the proposed protocol can accomplish the size relationship comparison of privacies from users more than two within one execution of the protocol; (2) only the proposed protocol is adaptive for the circumstance where there are two TPs; (3) the QW system used in the proposed protocol is different from that of Ref. [26]. Specifically, Ref. [26] adopts two-direction quantum walks on a circle (TDQWC) system; and the participants in Ref. [26] embed their private information with $T_k \otimes I_2$, and perform the two-direction evolution operator with secret steps for encryption. Both Ref. [27] and the proposed protocol adopt the ODQWC system, and directly apply U_{od}^k to embed and encrypt the private information; (4) the particle transmission mode of the proposed protocol is different from that of Ref. [26]; (5) the proposed protocol exceeds the protocols of Ref. [26] and Ref. [27] in quantum measurement, as it doesn't employ two-dimensional single particle measurements.

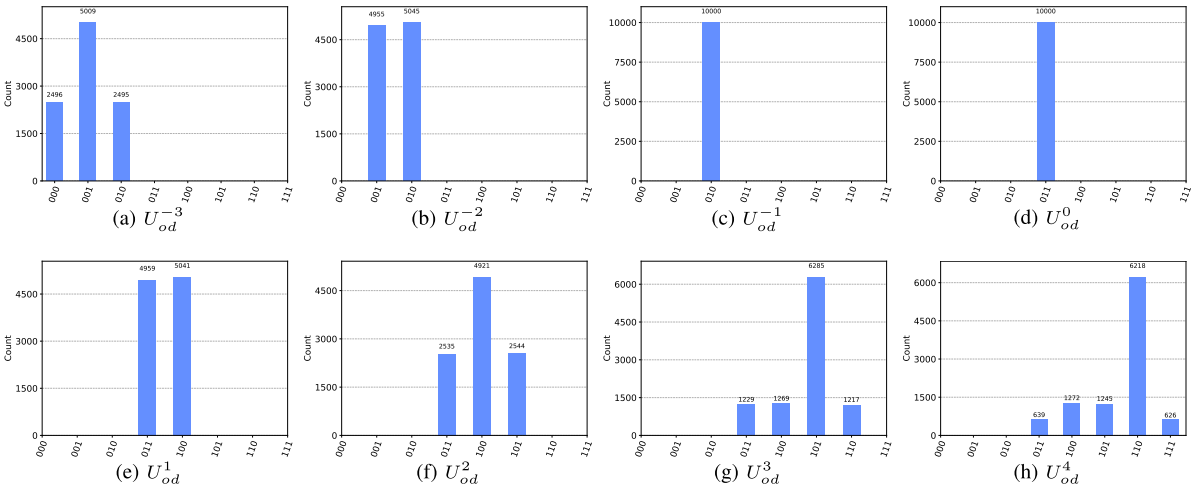

Figure G9 Frequency distribution of positions of walker particle from $|3\rangle|0\rangle$ in first k steps of ODQWC derived from simulation

Table G1 Probability distribution of positions of walker particle from $|3\rangle|0\rangle$ in first k steps of ODQWC derived from simulation

k \ p	000	001	010	011	100	101	110	111
−3	0.2496	0.5009	0.2495	–	–	–	–	–
−2	–	0.4955	0.5045	–	–	–	–	–
−1	–	–	1	–	–	–	–	–
0	–	–	–	1	–	–	–	–
1	–	–	–	0.4959	0.5041	–	–	–
2	–	–	–	0.2535	0.4921	0.2544	–	–
3	–	–	–	0.1229	0.1269	0.6285	0.1217	–
4	–	–	–	0.0639	0.1272	0.1245	0.6218	0.0626

Table H1 Comparison results of different QPC protocols based on QW

	Ref. [26]	Ref. [27]	This protocol
Number of users	Two	Two	n
Number of TPs	One	One	Two
Type of comparison	Size relationship comparison	Size relationship comparison	Size relationship comparison
QW system	TDQWC	ODQWC	ODQWC
Initial quantum states	Two-particle product states	Two-particle product states	Two-particle product states
Particle transmission mode	Circular type	Tree type	Tree type
Quantum measurement	d-dimensional single particle measurements and two-dimensional single particle measurements	d-dimensional single particle measurements and two-dimensional single particle measurements	d-dimensional single particle measurements
Usage of pre-shared QKD keys	No	Yes	Yes
Usage of unitary operations	Yes	Yes	Yes
Usage of quantum entanglement swapping	No	No	No

Appendix I Conclusion

In this paper, in order to accomplish the size relationship comparison of privacies between one user and the remaining users, we suggest a novel MQPC protocol of size relationship based on ODQWC with two semi-honest TPs. This protocol only uses two-particle product states as the initial quantum resource, only adopts d-dimensional single particle measurements and doesn't employ quantum entanglement swapping operations. This protocol is proved to be secure against both the outside attacks and the participant attacks. In addition, its output correctness is validated through both the theoretical analysis and the quantum circuits of ODQWC constructed and simulated on IBM Qiskit. In the QW-based QPC protocols, how to make full use of the natural characteristics of QW and reduce the consumption of initial QW states deserves further studies.

References

1 Yao A C. Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), 1982, 160.
2 Bennett C H and Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the International Conference on Computers, Systems and Signal Processing, 1984, 175.
3 Yang Y G and Wen Q Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A-math Theor, 2009, 42: 055305.
4 Yang Y G, Cao W F, and Wen Q Y. Secure quantum private comparison. Phys Scr, 2009, 80: 065002.
5 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, 2010, 283: 1561.
6 Liu W, Wang Y B, and Cui W. Quantum private comparison protocol based on Bell entangled states. Commun Theor Phys, 2012, 57: 583.
7 Tseng H Y, Lin J, and Hwang T. New quantum private comparison protocol using EPR pairs. Quantum Inf Process, 2012, 11: 373.
8 Sun Z W and Long D Y. Quantum private comparison protocol based on cluster states. Int J Theor Phys, 2013, 52: 212.
9 Zhang W W and Zhang K J. Cryptanalysis and improvement of the quantum private comparison protocol with semi-honest third party. Quantum Inf Process, 2013, 12: 1981.
10 Li J, Zhou H F, Jia L, et al. 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, 2014, 53: 2167.
11 Ye T Y and Ji Z X. Two-party quantum private comparison with five-qubit entangled states. Int J Theor Phys, 2017, 56: 1517.
12 Ji Z X and Ye T Y. Quantum private comparison of equal information based on highly entangled six-qubit genuine state. Commun Theor Phys, 2016, 65: 711.
13 Chang Y J, Tsai C W, and Hwang T. Multi-user private comparison protocol using GHZ class states. Quantum Inf Process, 2013, 12: 1077.
14 Wang Q L, Sun H X, and Huang W. Multi-party quantum private comparison protocol with n-level entangled states. Quantum Inf Process, 2014, 13: 2375.
15 Ye T Y and Ji Z X. Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states. Sci China Phys Mech, 2017, 60: 1.
16 Ji Z X and 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, 2017, 16: 1.
17 Ye C Q and Ye T Y. Circular multi-party quantum private comparison with n-level single-particle states. Int J Theor Phys, 2019, 58: 1282.
18 Ye T Y and Hu J L. Multi-party quantum private comparison based on entanglement swapping of Bell entangled states within d-level quantum system. Int J Theor Phys, 2021, 60: 1471.
19 Lin S, Sun Y, Liu X F, et al. Quantum private comparison protocol with d-dimensional Bell states. Quantum Inf Process, 2013, 12: 559.
20 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, 2014, 13: 2343.
21 Ye C Q and Ye T Y. Multi-party quantum private comparison of size relation with d-level single-particle states. Quantum Inf Process, 2018, 17: 1.
22 Lian J Y, Li X, and Ye T Y. Multi-party quantum private comparison of size relationship with two third parties based on d-dimensional Bell states. Phys Scr, 2023, 98: 035011.
23 Cao H, Ma W P, Lü L D, et al. Multi-party quantum privacy comparison of size based on d-level GHZ states. Quantum Inf Process, 2019, 18: 1.
24 Vlachou C, Krawec W, Mateus P, et al. Quantum key distribution with quantum walks. Quantum Inf Process, 2018, 17: 288.
25 Srikara S and Chandrashekar C M. Quantum direct communication protocols using discrete-time quantum walk. Quantum Inf Process, 2020, 19: 1.
26 Chen F L, Zhang H, Chen S G, et al. Novel two-party quantum private comparison via quantum walks on circle. Quantum Inf Process, 2021, 20: 178.
27 Wang J J, Dou Z, Chen X B, et al. Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle. Chinese Phys B, 2022, 31: 050308.
28 Wang Y, Lou X P, Fan Z, et al. Verifiable multi-dimensional (t, n) threshold quantum secret sharing based on quantum walk. Int J Theor Phys, 2022, 61: 24.
29 Wang J T, Li X, and Ye T Y. A quantum secure multi-party summation protocol based on one-direction quantum walks on a circle. Sci Sin-Phys Mech Astron, 2024, 54: 240311.
30 Vlachou C, Rodrigues J, Mateus P, et al. Quantum walk public-key cryptographic system. Int J Quantum Inf, 2015, 13: 1550050.
31 Chandrashekar C M, Srikanth R, and Laflamme R. Optimizing the discrete time quantum walk using a SU(2) coin. Phys Rev A, 2008, 77: 032326.
32 Kadian K, Garhwal S, and Kumar A. Quantum walk and its application domains: A systematic review. Comput Sci Rev, 2021, 41: 100419.
33 Ye T Y and Jiang L Z. Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chinese Phys Lett, 2013, 30: 040305.

34 Deng F G, Zhou P, Li X H, et al. Robustness of two-way quantum communication protocols againstTrojan horse attack. arXiv preprint quant-ph/0508168, 2005.
35 Li X H, Deng F G, and Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. Phys Rev A, 2006, 74: 054302.
36 Gao Fei, Qin S J, Wen Q Y, et al. A simple participant attack on the brádler-dušek protocol. Quantum Inf Comput, 2007, 7: 329.
37 Fujiwara S, Osaki H, Buluta I M, et al. Scalable networks for discrete quantum random walks. Phys Rev A, 2005, 72: 032329.
38 Douglas B L and Wang J B. Efficient quantum circuit implementation of quantum walks. Phys Rev A, 2009, 79: 052335.
39 Geng M J, Xu T J, Chen Y, et al. Semiquantum private comparison of size relationship based on d-level single-particle states. Sci Sin-Phys Mech Astron, 2022, 52: 290311.
40 Cabello A. Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85: 5635.