SCIENCE CHINA
Information Sciences

• **LETTER** •

February 2025, Vol. 68, Iss. 2, 129502:1–129502:2
https://doi.org/10.1007/s11432-024-4188-6

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

Received 21 May 2024/Revised 3 July 2024/Accepted 10 October 2024/Published online 14 January 2025

Citation Wang J T, Lian J Y, Ye T Y. Multi-party quantum private comparison of size relationship based on one-direction quantum walks on a circle. Sci China Inf Sci, 2025, 68(2): 129502, https://doi.org/10.1007/s11432-024-4188-6

Quantum walks (QW) are the quantum counterpart of classical random walks, and portray a natural stochastic process when the walker randomly wanders around. In a discrete-time QW system on a circle, when the walker particle generally steps towards two directions, i.e., clockwise and anti-clockwise, this kind of QW is called two-direction quantum walks on a circle (TDQWC); and the walker particle always steps towards one direction or stays stationary, this kind of QW is called as one-direction quantum walks on a circle (ODQWC). ODQWC exhibits some different properties, and may induce potential applications in the field of quantum secure multi-party computation.

In 2021, Chen et al. [1] proposed a novel two-party quantum private comparison (QPC) based on TDQWC. In 2022, Wang et al. [2] proposed an efficient two-party QPC protocol based on ODQWC. In the same year, Joseph and Ali [3] proposed a multi-party quantum private comparison (MQPC) protocol based on TDQWC to achieve bit equality comparison. And in 2024, Wang et al. [4] proposed a quantum secure multi-party summation (QSMS) protocol based on ODQWC.

In this letter, 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 ODQWC with two semi-honest third parties (TPs), TP_1 and TP_2. Here, each TP is permitted 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 control.

ODQWC. In a discrete-time QW system, the QW state is composed of a walker particle and a coin particle, which can be represented by $|\psi\rangle = |p\rangle \otimes |c\rangle$. Here, $p \in \{0, 1, \ldots, d-1\}$ and $c \in \{0, 1\}$. The one-direction evolution operator, which is used to make the QW state evolve towards one direction, is defined as

$$U_{\rm od} = S_{\rm od} \cdot \left(I_d \otimes C\right). \tag{1}$$

Here, C is the coin operator and can be generally chosen as the Hadamard operator $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix}1 & 1\\ 1 & -1\end{smallmatrix}\right)$, I_d is the identity operator of size $d \times d$, and $S_{\rm od}$ is the one-direction shifting operator, which is defined as

$$S_{\rm od} = \sum\nolimits_i |i \oplus 1\rangle \langle i| \otimes |0\rangle \langle 0| + \sum\nolimits_i |i\rangle \langle i| \otimes |1\rangle \langle 1|. \tag{2}$$

Here, the symbol '$\oplus$' denotes the modulo d addition.

The inverse evolution operator corresponding to $U_{\rm od}$ is

$$U_{\rm od}^{-1} = \left(I_d \otimes C^{-1}\right) \cdot S_{\rm od}^{-1}, \tag{3}$$

where $C^{-1} = H^{-1} = H$, and the inverse operator of $S_{\rm od}$ is

$$S_{\rm od}^{-1} = \sum\nolimits_i |i \ominus 1\rangle \langle i| \otimes |0\rangle \langle 0| + \sum\nolimits_i |i\rangle \langle i| \otimes |1\rangle \langle 1|. \tag{4}$$

Here, the symbol '$\ominus$' denotes the modulo d subtraction.

Suppose that $d = 2^n$, thus there are n qubits needed to represent a walker particle, and another qubit to denote a coin particle. On the ground of [5], the quantum circuits of $U_{\rm od}$ and $U_{\rm od}^{-1}$ in ODQWC are shown in Figure 1. It is worth noting that $U_{\rm od}^{k}$ means applying k times $U_{\rm od}$ on the QW state, while $U_{\rm od}^{-k}$ means applying k times $U_{\rm od}^{-1}$ on the QW state.

Protocol description. Assume that there are n users $P_1, P_2, \ldots, P_n$ and two semi-honest TPs, TP_1 and TP_2; 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 $[1, \lfloor \frac{d-1}{2} \rfloor]$ and $i \in \{1, 2, \ldots, n\}$. The MQPC protocol omitting the security check processes is made up of the following steps.

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

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

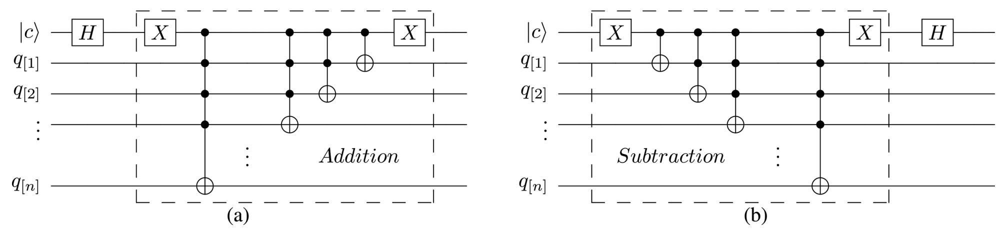

Figure 1 Quantum circuits of (a) $U_{\rm od}$ and (b) $U_{\rm od}^{-1}$ in ODQWC.

Step 2. TP_1 prepares m copies of 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. After that, TP_1 distributes m copies $|\psi_0\rangle$ to P_i via a quantum channel. Here, $i \in \{1, 2, \ldots, n\}$.

Step 3. P_i calculates an encrypted integer $v_i = k_i + p_i + q$, and applies $U_{\rm od}^{v_i}$ on $|\psi_0\rangle$ to get $|\psi_1^i\rangle = U_{\rm od}^{v_i}|\psi_0\rangle$. Then, P_i sends m copies $|\psi_1^i\rangle$ to TP_2 via a quantum channel, and conveys v_i through a classical channel. Here, $i \in \{1, 2, \ldots, n\}$.

Step 4. TP_2 acquires m copies $|\psi_1^i\rangle$ and v_i from P_i, where $i \in \{1, 2, \ldots, n\}$. TP_2 imposes $U_{\rm od}^{-v_i}$ on $|\psi_1^j\rangle$ to gain $|\psi_2^{ij}\rangle = U_{\rm od}^{-v_i}|\psi_1^j\rangle$, where $j \in \{1, 2, \ldots, n\}$ and $j \neq i$. Then, TP_2 transfers m copies $|\psi_2^{ij}\rangle$ to TP_1 via a quantum channel.

Step 5. TP_1 acquires m copies $|\psi_2^{ij}\rangle$ from TP_2, where $i, j \in \{1, 2, \ldots, n\}$ and $j \neq i$. TP_1 imposes $U_{\rm od}^{k_i}$ and $U_{\rm od}^{-k_j}$ on $|\psi_2^{ij}\rangle$, and gets $|\psi_3^{ij}\rangle = U_{\rm od}^{-k_j}U_{\rm od}^{k_i}|\psi_2^{ij}\rangle$. Afterwards, TP_1 measures the walker particles of m copies $|\psi_3^{ij}\rangle$ within the $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ basis. There are three cases that may happen after the $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ basis measurements of TP_1.

(1) All walker particles' positions are collapsed into the original position p_0. In this case, it has $p_j = p_i$.

(2) 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) 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.

Within one execution of the protocol, the proposed protocol can achieve the size relationship comparison between P_i ($i \in \{1, 2, \ldots, n\}$) and the remaining users. After executing the framework for n times, we can realize the size comparison for arbitrary two users among $P_1, P_2, \ldots, P_n$.

Correctness. In the following, we illustrate the output correctness of the proposed protocol through Lemmas 1–3.

Lemma 1. In an ODQWC system, it has $U_{\rm od}^{-a}U_{\rm od}^{b} = U_{\rm od}^{b-a}$. Specially, when $a = b$, it has $U_{\rm od}^{-a}U_{\rm od}^{b} = I_{2d}$. 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.

In ODQWC, when $U_{\rm od}^{k}$ is performed on the initial QW state $|p_0\rangle|0\rangle$, where $k \in \mathbb{Z}$ and p_0 is an integer located in the range $[1, \lfloor\frac{d-1}{2}\rfloor]$, after the walker particle is performed with the $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ basis measurement, it has Lemmas 2 and 3.

Lemma 2. When $k \in [1, d - p_0)$, the walker particle's position is collapsed into the position bigger than or equal to p_0; moreover, the probability of the walker particle's position being collapsed into the position $p_0 + k$ is $(\frac{1}{2})^k$.

Lemma 3. When $k \in [-p_0, -1]$, the walker particle's position is collapsed into the position smaller than p_0; moreover, the probability of the walker particle's position being collapsed into the position $p_0 - |k|$ is $(\frac{1}{2})^{|k|-1}$.

Proposition 1. The output of the proposed MQPC protocol is correct.

Proof. According to Lemma 1 and the protocol, it has

$$\begin{aligned}
|\psi_3^{ij}\rangle &= U_{\rm od}^{-k_j}U_{\rm od}^{k_i}|\psi_2^{ij}\rangle = U_{\rm od}^{-(k_j-k_i)}U_{\rm od}^{-v_i}|\psi_1^j\rangle \\
&= U_{\rm od}^{-(k_j-k_i)}U_{\rm od}^{-v_i}U_{\rm od}^{v_j}|\psi_0\rangle \\
&= U_{\rm od}^{-(k_j-k_i)}U_{\rm od}^{-(k_i+p_i+q)}U_{\rm od}^{k_j+p_j+q}|\psi_0\rangle \\
&= U_{\rm od}^{-(k_j-k_i)}U_{\rm od}^{k_j-k_i}U_{\rm od}^{p_j-p_i}|\psi_0\rangle \\
&= U_{\rm od}^{p_j-p_i}|\psi_0\rangle \\
&= U_{\rm od}^{p_j-p_i}|p_0\rangle|0\rangle. \qquad (5)
\end{aligned}$$

In terms of Lemmas 2 and 3, after the $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ basis measurements of TP_1 on the walker particles of m copies $|\psi_3^{ij}\rangle$, it can be obtained that

(1) when $p_j = p_i$, all walker particles' positions are collapsed into the original position p_0;

(2) when $p_j > p_i$, 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;

(3) when $p_j < p_i$, all walker particles' positions are collapsed into the positions smaller than p_0.

Conclusion. In this study, we put forward a novel MQPC protocol of size relationship based on ODQWC with two semi-honest TPs, which can achieve the size relationship comparison of privacies between one user and the remaining users. This protocol only adopts two-particle product states as the initial quantum resource, only uses d-dimensional single particle measurements and does not employ quantum entanglement swapping operations.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 62071430) and Scientific Research Fund of Zhejiang Provincial Education Department (Grant No. Y202352615).

Supporting information Appendixes A–I. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 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
2 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. Chin Phys B, 2022, 31: 050308
3 Joseph J, Ali S T. Multiparty quantum private comparison based on quantum walks. Quantum Inf Process, 2022, 22: 17
4 Wang J T, Li X, 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
5 Douglas B L, Wang J B. Efficient quantum circuit implementation of quantum walks. Phys Rev A, 2009, 79: 052335