

Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle

Jv-Jie Wang(王苣杰), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Citation: Chin. Phys. B, 2022, 31 (**5**): 050308. DOI: 10.1088/1674-1056/ac5a3f
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Self-error-rejecting multipartite entanglement purification for electron systems assisted by quantum-dot spins in optical microcavities

Yong-Ting Liu(刘永婷), Yi-Ming Wu(吴一鸣), and Fang-Fang Du(杜芳芳)
Chin. Phys. B, 2022, 31 (**5**): 050303. DOI: 10.1088/1674-1056/ac4489

Channel parameters-independent multi-hop nondestructive teleportation

Hua-Yang Li(李华阳), Yu-Zhen Wei(魏玉震), Yi Ding(丁祎), and Min Jiang(姜敏)
Chin. Phys. B, 2022, 31 (**2**): 020302. DOI: 10.1088/1674-1056/ac1330

Efficient and stable wireless power transfer based on the non-Hermitian physics

Chao Zeng(曾超), Zhiwei Guo(郭志伟), Kejia Zhu(祝可嘉), Caifu Fan(范才富), Guo Li(李果), Jun Jiang(江俊), Yunhui Li(李云辉), Haitao Jiang(江海涛), Yaping Yang(羊亚平), Yong Sun(孙勇), and Hong Chen(陈鸿)
Chin. Phys. B, 2022, 31 (**1**): 010307. DOI: 10.1088/1674-1056/ac3815

Low-loss belief propagation decoder with Tanner graph in quantum error-correction codes

Dan-Dan Yan(颜丹丹), Xing-Kui Fan(范兴奎), Zhen-Yu Chen(陈祯羽), and Hong-Yang Ma(马鸿洋)
Chin. Phys. B, 2022, 31 (**1**): 010304. DOI: 10.1088/1674-1056/ac11cf

Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states

Bing Wang(王冰), San-Qiu Liu(刘三秋), and Li-Hua Gong(龚黎华)
Chin. Phys. B, 2022, 31 (**1**): 010302. DOI: 10.1088/1674-1056/ac1413

Efficient quantum private comparison protocol based on one direction discrete quantum walks on the circle

Jv-Jie Wang(王莒杰)[1], Zhao Dou(窦钊)[1,†], Xiu-Bo Chen(陈秀波)[1], Yu-Ping Lai(赖裕平)[2], and Jian Li(李剑)[2]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[2] *Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 17 December 2021; revised manuscript received 17 February 2022; accepted manuscript online 3 March 2022)

We propose an efficient quantum private comparison protocol firstly based on one direction quantum walks. With the help of one direction quantum walk, we develop a novel method that allows the semi-honest third party to set a flag to judge the comparing result, which improves the qubit efficiency and the maximum quantity of the participants' secret messages. Besides, our protocol can judge the size of the secret messages, not only equality. Furthermore, the quantum walks particle is disentangled in the initial state. It only requires a quantum walks operator to move, making our proposed protocol easy to implement and reducing the quantum resources. Through security analysis, we prove that our protocol can withstand well-known attacks and brute-force attacks. Analyses also reveal that our protocol is correct and practical.

Keywords: quantum private comparison protocol, one direction quantum walks, efficiency, brute-force attack

PACS: 03.67.Dd 03.67.Hk 03.67.Ac **DOI:** 10.1088/1674-1056/ac5a3f

1. Introduction

In 1982, Yao introduced the millionaire problem.[1] The millionaire problem describes a circumstance in which two millionaires desire to know who is wealthier without divulging their property. Since then, secure multi-party computation (SMPC), as a new branch of cryptography, has been established. Nowadays, SMPC is a cryptographic primitive that can be used for many tasks, such as electronic election[2–4] and secret sharing.[5–7]

However, with the rapid development of quantum technology, classical cryptography has been substantially challenged because of the quantum parallelism.[8] Therefore, the security of SMPC is worth discussing. With more and more researchers turning to the quantum cryptography protocols' study, plenty of efforts have been made, such as quantum key distribution (QKD),[9–13] quantum secret sharing (QSS),[14–18] quantum secure direct communication (QSDC).[19–22] In 2009, Yang and Wen proposed the first quantum private comparison (QPC) protocol,[23] which is the extension area of the SMPC. The QPC seeks to compare the size of the two participants' private input without revealing the true values. Most QPC protocols require a semi-honest third party (TP) to assist the mutually distrustful participants in completing the protocols, while some of the QPC protocol only needs an untrusted third party. So far, several protocols for QPC have been presented. There are protocols based on Bell states,[24–29] GHZ entangled states,[30–34] entanglement swapping,[35–38] superdense coding,[39] etc. To take more participants into comparison, the multi-party quantum private comparison (MQPC) has been firstly proposed by Chang *et al.* in 2013.[40]

The participants constantly try to obtain others' secret information, on which is the most severe hazard we concentrate. The QPC protocols can be divided into two categories according to the type of the particles. They are protocols based on the single-particle[41–46] and protocols based on the multi-particle.[26–31] Most of the multi-particle-based protocols are using entangled states. In 2012, Wen *et al.* proposed the QPC protocol based on Bell states.[24] In 2013, Guo *et al.*[35] proposed a protocol based on GHZ state, which solves the feasibility to expand in network service. In 2021, Zhou *et al.*[29] put forward a new semi-quantum QPC protocol based on d-dimensional Bell states. As for the protocols based on the single-particle, in 2012, Yang *et al.* proposed the first QPC protocol without entanglement.[41] In 2018, Lang proposed a QPC protocol using single photons,[45] delivering a new direction of single-particle protocols. In 2019, Lin *et al.*[46] came up with a practical and efficient semi-quantum QPC protocol using single photons.

The protocol based on single-particle has several advantages. Firstly, it has fewer potential security risks than the multi-particle-based protocols. There are multiple attacks on entangled states. For example, Gao *et al.* proposed the correlation-elicitation attack for entanglement states.[47] Besides, the entanglement states pervasively require pre-distribution before the execution of the protocol. That is another potential security risk. Secondly, the single-particle can be easily prepared under the circumstance of nowadays quan-

†Corresponding author. E-mail: dou@bupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

tum technology. Therefore, the utilization of single-particle has the potential to minimize costs and equipment requirements.

Recently, Chen *et al.* firstly proposed a novel QPC protocol based on discrete quantum walks (QWs) on circle (DQWC),[48] which also has the advantages of the protocols based on single-particle. The QWs are the extension of classical random walk. It has a coin state within 2-dimension and a d-dimensional walker state. The QWs state is made up of the tensor product of those two states. It is simple to prepare because it is a product state, does not have entanglement in its initial state. The QWs states move by applying the unitary evolution operator. Recent studies suggest that the QWs has been divided into two main categories, which are one-dimensional QWs[49,50] and high-dimensional QWs.[51] The one-dimensional QWs is performed on an infinite line, and high-dimensional QWs can be performed on the graph or cube, etc. The QWs is widely used in quantum communication and computation. It can be applied in speeding up the quantum algorithm,[52] enhancing the efficiency, and also simulating the quantum systems.[53] In Chen *et al.*'s protocol,[48] the QWs particles are encrypted by the evolution operator and the secret messages are encoded into the QWs particles by the shift operator. The participants' secret messages are in $\{0,1,\ldots,\lfloor\frac{d-1}{2}\rfloor\}$.

Inspired by Chen *et al.*'s protocol,[48] we propose a QPC protocol based on one-direction quantum walks on the circle (ODQWC). Our protocol can compare the size between the two participants, not only the equality. With the ODQWC, TP can set the walker state $|0\rangle_{\rm p}$ as a flag to judge the comparison result. In our proposed protocol, the participants' secret messages are in $\{0,1,\ldots,d-1\}$ which improves the qubit efficiency. Besides, we analyze various attacks such as the intercept-resend attack, entangle-measure attack and brute-force attack.[54] Moreover, Alice and Bob's operations are symmetric in our protocol, which means they are equivalent. That reduces the security risk from the participants. Our protocol also has the advantages of the protocols based on the single-particle, because QWs particle is easy to prepare.

In Section 2, we introduce the basic knowledge of quantum walks and the property of the ODQWC. In Section 3, we give a detailed illustration of our proposed protocol. In Section 4, the correctness and security of our protocol are proved. Subsequently, we demonstrate the advantages of our protocol in Section 5. In the last part of our paper, we make a conclusion.

2. Preliminaries

We introduce some fundamental quantum walks knowledge and properties in this section, which will be used in our proposed protocol. We mention the discrete quantum walks on a line (DQWL) because the ODQWC is evolved from it.

2.1. Discrete quantum walks on a line

Quantum walks are a variation of the traditional random walk. It consists of two quantum systems: the walker system, which describes the particle's position, and the coin system, which determines the particle's direction. The Hilbert space H where QWs is located is composed of the tensor product of the coin's Hilbert space and the walker's Hilbert space. Hence, H could be presented as $H = H_{\rm c} \otimes H_{\rm p}$. We denote the quantum state of the walker as $|\text{position}\rangle_{\rm p}$ and the coin as $|c\rangle_{\rm c}$, where position $\in (-d,+d)$ and $c \in \{0,1\}$. Therefore, we can write a QWs state as $|\psi\rangle = |c\rangle_{\rm c} \otimes |\text{position}\rangle_{\rm p}$.

2.2. Evolution operator

Subsequently, we will go over a crucial operator called the evolution operator, which plays an important role in our protocol. The evolution operator, also known as the step operator, is used to regulate the movement of particles. The quantum walks, like the classical random walk, start by flipping a coin to select the particle's walking direction. The shift operator is then used to move one step. We specify that the $|0\rangle$ state of the coin represents the particle going right, while the $|1\rangle$ goes left. Generally, we use the Hadamard gate for the coin toss, which is also called the Hadamard walk.[55] That is

$$C = H = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\right). \tag{1}$$

The Hadamard gate acts on $|0\rangle$ and $|1\rangle$ as follows:

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right), \tag{2}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \tag{3}$$

The shift operator should be used after the coin tossing. It is denoted as

$$S = |0\rangle_{\rm c}\langle 0| \otimes \sum_i |i+1\rangle_{\rm p}\langle i| + |1\rangle_{\rm c}\langle 1| \otimes \sum_i |i-1\rangle_{\rm p}\langle i|. \tag{4}$$

The shift operator converts $|0\rangle_{\rm c}|x\rangle_{\rm p}$ to $|0\rangle_{\rm c}|x+1\rangle_{\rm p}$ and $|1\rangle_{\rm c}|x\rangle_{\rm p}$ to $|1\rangle_{\rm c}|x-1\rangle_{\rm p}$. The evolution operator, also a unitary operator, is defined as follows by combining the two states of the quantum walks:

$$U = S \cdot \left(C \otimes I_{\rm p}\right). \tag{5}$$

Reference [48] provides proofs that U and S have inverse operators. We show their inverse operators below:

$$U^{-1} = \left(C^{-1} \otimes I_{\rm p}\right) \cdot S^{-1}, \tag{6}$$

$$S^{-1} = |0\rangle_{\rm c}\langle 0| \otimes \sum_i |i-1\rangle_{\rm p}\langle i| + |1\rangle_{\rm c}\langle 1| \otimes \sum_i |i+1\rangle_{\rm p}\langle i|. \tag{7}$$

If the QWs particles desire to move k steps, then k evolution operators should be applied. We denote the k evolution operators as U^k and its inverse operator as U^{-k}.

2.3. Measurement and properties of QWs

In the protocols based on QWs, one of the foremost tasks is measurement. The distinction between classical random walks and quantum walks resides in the quantum state's superposition. Of course, it is no different from a traditional random walk if we measure the particles after each step and let the particles collapse into a specific state.

We measure the coin state by utilizing the operator

$$M_{\mathrm{c}} = \alpha_0 |0\rangle_{\mathrm{c}} \langle 0| + \alpha_1 |1\rangle_{\mathrm{c}} \langle 1|, \quad (|\alpha_0|^2 + |\alpha_1|^2 = 1).$$
$$M_{\mathrm{p}} = \sum_{i=0}^{d-1} \alpha_i |i\rangle_{\mathrm{p}} \langle i|, \quad \left(\sum_i |\alpha_i|^2 = 1\right)$$

is used to measure the position state. Note that all the measurement bases are orthogonal. Generally, we let $\alpha_i = 1/\sqrt{d}$.

Table 1 suggests that the QWs particle with an initial state $|1\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$ is more likely to move along the left side. However, we can still obtain the measurement result on the other side, demonstrating that the QWs particles can move on both sides simultaneously. Here T represents the moving steps, P is the position of the QWs particles and the initial state is $|1\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$.

Table 1. Probability distribution of $|1\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$ in first 3 step.

T \ P	–4	–3	–2	–1	0	1	2	3	4
0					1				
1				1/2		1/2			
2			1/4		1/2		1/4		
3		1/8		5/8		1/8		1/8	
4	1/16		5/8		1/8		1/8		1/16

2.4. One direction discrete quantum walks on circle

If the endpoints of the DQWL are linked, it is called discrete quantum walks on circle.

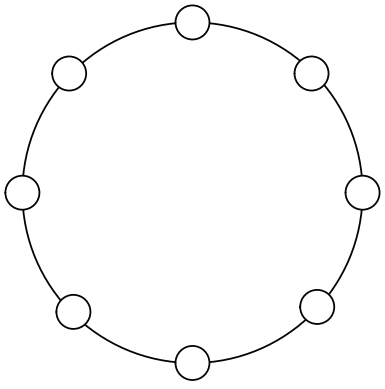


Fig. 1. Schematic diagram of DQWC.

The following shift operator should be used if we want the particle to go in one direction:

$$S_{\mathrm{o}} = |0\rangle_{\mathrm{c}} \langle 0| \otimes \sum_i |(i+1) \bmod d\rangle_{\mathrm{p}} \langle i| + |1\rangle_{\mathrm{c}} \langle 1| \otimes \sum_i |i \bmod d\rangle_{\mathrm{p}} \langle i|. \tag{8}$$

This slight change makes the QWs particle move in one direction. We denote the one direction evolution operator as

$$U_{\mathrm{o}} = S_{\mathrm{o}} \left(C \otimes I_{\mathrm{p}}\right), \tag{9}$$

and the inverse operators of the shift and evolution operators are

$$S_{\mathrm{o}}^{-1} = |0\rangle_{\mathrm{c}} \langle 0| \otimes \sum_i |(i-1) \bmod d\rangle_{\mathrm{p}} \langle i| + |1\rangle_{\mathrm{c}} \langle 1| \otimes \sum_i |i \bmod d\rangle_{\mathrm{p}} \langle i|, \tag{10}$$

$$U_{\mathrm{o}}^{-1} = (C^{-1} \otimes I_{\mathrm{p}}) \cdot S_{\mathrm{o}}^{-1}. \tag{11}$$

We list the particle's probability distribution of the first 3 steps ODQWC in Table 2 (T is steps, P is position, and the initial state is $|0\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$).

Table 2. Probability distribution of $|0\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$ in ODQWC in first 3 step.

T \ P	0	1	2	3	4
0	1				
1	1/2	1/2			
2	1/4	1/2	1/4		
3	1/8	1/8	5/8	1/8	

We can find that the furthest position of the particle is equal to the moving steps.

3. The proposed QPC protocol based on one direction discrete quantum walks on circle

The following work illustrates our proposed protocol based on the one-direction discrete quantum walks on circle. We assume that the proposed protocol runs in ideal conditions, in which there are no technical errors and the transmission channels are lossless and noiseless. The proposed protocol requires a semi-honest third party and can judge the size of two parties' secret messages.

Step 1 The protocol begins with semi-honest TP, who prepares k copies of QWs particles $|0\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$. The parameter k is a safety threshold value that is sufficient for measurements. TP owns two secret keys P_{k1} and P_{k2}. Alice and Bob share a private key P_{k3} through some secure QKD protocols, such as BB84.[9] TP applies $U_{\mathrm{o}}^{P_{k1}}$ on the k $|0\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}$ to form the initial sequence S_0. We denote the initial particles as

$$|\xi\rangle = U_{\mathrm{o}}^{P_{k1}} |0\rangle_{\mathrm{c}} |0\rangle_{\mathrm{p}}. \tag{12}$$

Step 2 To prevent the divulge of the secret messages, the eavesdropping must be detected. Therefore, TP randomly chooses 2λ decoy particles from the assemble $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$ and inserts them into S_0 at random to generate S_0'. F is the Fourier transform of d-dimensional quantum particles,

$$F|j\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} jk}{d}} |k\rangle. \tag{13}$$

The measurement bases of $|i\rangle$ and $F|i\rangle$ are $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ and $\{F|0\rangle, F|1\rangle, \ldots, F|d-1\rangle\}$. Then TP sends S_0' to Alice.

Step 3 Alice will report to TP after receiving the particles. Then TP will announce the position of the decoy particles and the measurement basis to Alice. After that, Alice performs the measurements on the decoy particle using the corresponding measurement bases, and reports the measurement results to TP. By comparing the measurement results from Alice and the initial states of the particles, TP can check the error rate of the measurement results to determine whether there is an eavesdropper. If the error rate is higher than the safety threshold, they will abandon the particles and restart the protocol. Otherwise, Alice will remove the decoy particles and continue the protocol.

Step 4 After Alice removes the decoy particles, she applies the evolution operator $U_o^{P_{k3}}$ on S_0. Then she encodes his secret message $m_1\,(m_1 \le d-1)$ into S_0 by applying operator $U_o^{m_1}$. Then she sends his new generated sequence S_A to TP through the quantum channel, using the method in Step 2 and Step 3.

Step 5 After the security verification process passes between Alice and TP, TP will apply the evolution operator $U_o^{P_{k2}}$ on S_A. We denote the new sequence as S_T. Then TP inserts some new decoy particles into S_T and sends them to Bob.

Step 6 Bob removes the decoy particles in S_T and checks whether there is an eavesdropper. If the transmission is safe, Bob will apply the evolution operator $U_o^{-P_{k3}}$ and $U_o^{-m_2}\,(m_2 \le d-1)$ on S_T to generate S_B. Then he adopts the methods in Step 2 and Step 3 to send the sequence S_B to TP.

Step 7 TP checks and removes the decoy particles in S_B. Then he inverses the keys P_{k1}, P_{k2} by applying the operator $U_o^{-P_{k1}}$, $U_o^{-P_{k2}}$. In the end, he gets the sequence S_F. He measures all the particles using the operator $M_c \otimes M_p$. As a result, he can get the probability of the location where the particle might appear. According to the measurement result, we can divide it into three situations.

(1) If all the walker states are $|0\rangle_p$, then $m_1 = m_2$.

(2) If there exists at least one walker state but not all of them in $|0\rangle_p$, then $m_1 > m_2$.

(3) If there is no walker state in $|0\rangle_p$, then $m_1 < m_2$.

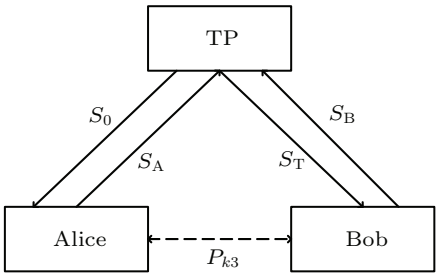


Fig. 2. Flow graph of our proposed protocol.

4. Analyses

We will analyze our proposed protocol from two perspectives in this section: correctness and security.

4.1. Correctness

In this subsection, we will prove the correctness of our proposed protocol.

Lemma 1 In ODQWC the operator U_o satisfies that the walker's measurement result of $U_o^k|0\rangle_c|0\rangle_p$ might appear $|0\rangle_p$, for $\forall k$, $k \in [0,1,\ldots,d-1]$.

Proof When $k=1$, the QWs state is

$$\begin{aligned} U|0\rangle_c|0\rangle_p &= S\cdot(C\otimes I_p)|0\rangle_c|0\rangle_p \\ &= \frac{1}{\sqrt{2}}S\left(|0\rangle_c|0\rangle_p + |1\rangle_c|0\rangle_p\right) \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle_c|1\rangle_p + |1\rangle_c|0\rangle_p\right). \end{aligned} \tag{14}$$

We suppose the QWs state after $k=j$ $(0<j\le d-2)$ steps is

$$\begin{aligned} &U_o^j|0\rangle_c|0\rangle_p = \sum_{i=0}^{j}\left(\alpha_i|0\rangle_c|i\rangle_p + \beta_i|1\rangle_c|i\rangle_p\right), \\ &\left(|\alpha_i|^2+|\beta_i|^2\neq 0\right), \end{aligned} \tag{15}$$

where $|\alpha_i|^2+|\beta_i|^2\neq 0$, for $\forall i$. Then the QWs state after $k=j+1$ steps is

$$\begin{aligned} &U_o\otimes U_o^j|0\rangle_c|0\rangle_p \\ &= S_o(C\otimes I)\left[\sum_{i=0}^{j}\left(\alpha_i|0\rangle_c|i\rangle_p + \beta_i|1\rangle_c|i\rangle_p\right)\right] \\ &= \sum_{i=0}^{j}\left[\frac{\alpha_i}{\sqrt{2}}\left(|0\rangle_c|i+1\rangle_p + |1\rangle_c|i\rangle_p\right)\right. \\ &\quad \left.+\frac{\beta_i}{\sqrt{2}}\left(|0\rangle_c|i+1\rangle_p - |1\rangle_c|i\rangle_p\right)\right] \\ &= \sum_{i=0}^{j+1}\left(\alpha_i'|0\rangle_c|i\rangle_p + \beta_i'|1\rangle_c|i\rangle_p\right). \end{aligned} \tag{16}$$

Therefore, the measurement result of the walker after k steps is $|\xi\rangle_p$, where $\xi\in[0,k]\cap\mathbb{Z}$. Because the $|\alpha_i|^2+|\beta_i|^2\neq 0$, we have $|\alpha_i'|^2+|\beta_i'|^2\neq 0$. Therefore, the probability of the walker's measurement results $|i\rangle_p$ will not be 0, for $i\in[0,1,2,\ldots,k]$. As a result when $k\in[0,1,\ldots,d-1]$, TP still has a chance of obtaining the measurement result $|0\rangle_p$, and not all the measurement results are $|0\rangle_p$. Thus, Lemma 1 follows.

Lemma 2 When $-(d-1)\le k<0$ the walker's measurement results of $U_o^k|0\rangle_c|0\rangle_p$ will not appear $|0\rangle_p$.

Proof Equation (11) shows the inverse operator of the evolution operator in ODQWC. When $k=-1$, the evolution operator U_o^{-1} acting on $|0\rangle_c|0\rangle_p$ is

$$\begin{aligned} U_o^{-1}|0\rangle_c|0\rangle_p &= (C^{-1}\otimes I_p)\cdot S_o^{-1}|0\rangle_c|0\rangle_p \\ &= (H\otimes I_p)\cdot\left(|0\rangle_c\langle 0|\otimes\sum_i|(i-1)\bmod d\rangle_p\langle i|\right. \end{aligned}$$

$$
\begin{aligned}
&+|1\rangle_{\mathrm{c}}\langle 1|\otimes\sum_{i}|i \bmod d\rangle_{\mathrm{p}}\langle i|\Big)|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}\\
&=(H\otimes I_{\mathrm{p}})\cdot|0\rangle_{\mathrm{c}}|-1 \bmod d\rangle_{\mathrm{p}}\\
&=\frac{1}{\sqrt{2}}\left(|0\rangle_{\mathrm{c}}|d-1\rangle_{\mathrm{p}}+|1\rangle_{\mathrm{c}}|d-1\rangle_{\mathrm{p}}\right). \qquad (17)
\end{aligned}
$$

When $k=-2$, the evolution operator U_{o}^{-2} acting on $|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}$ is

$$
\begin{aligned}
&U_{\mathrm{o}}^{-2}|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}\\
&=\frac{1}{\sqrt{2}}U_{\mathrm{o}}^{-1}\left(|0\rangle_{\mathrm{c}}|-1 \bmod d\rangle_{\mathrm{p}}+|1\rangle_{\mathrm{c}}|-1 \bmod d\rangle_{\mathrm{p}}\right)\\
&=\frac{1}{2}\Big(|0\rangle_{\mathrm{c}}|-2 \bmod d\rangle_{\mathrm{p}}+|1\rangle_{\mathrm{c}}|-2 \bmod d\rangle\\
&\quad+|0\rangle_{\mathrm{c}}|-1 \bmod d\rangle_{\mathrm{p}}-|1\rangle_{\mathrm{c}}|-1 \bmod d\rangle_{\mathrm{p}}\Big)\\
&=\sum_{i=-2}^{-1}\left(\alpha_i|0\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}+\beta_i|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right), \qquad (18)
\end{aligned}
$$

where $|\alpha_i|^2+|\beta_i|^2\neq 0$. Therefore, we can assume that when $k=-j$ $(1<j\leq d-2)$ the QWs state after k steps is

$$
U_{\mathrm{o}}^{k}|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}=\sum_{i=-j}^{-1}\left(\alpha_i|0\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}+\beta_i|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right). \qquad (19)
$$

The QWs state after $k=-(j+1)$ steps is

$$
\begin{aligned}
&U_{\mathrm{o}}^{-1}\otimes U_{\mathrm{o}}^{-j}|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}\\
&=(H\otimes I_{\mathrm{p}})\cdot S\left[\sum_{i=-j}^{-1}\left(\alpha_i|0\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}+\beta_i|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right)\right]\\
&=(H\otimes I_{\mathrm{p}})\sum_{i=-j}^{-1}\left(\alpha_i|0\rangle_{\mathrm{c}}|(i-1) \bmod d\rangle_{\mathrm{p}}+\beta_i|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right)\\
&=\sum_{i=-j}^{-1}\left[\frac{\alpha_i}{\sqrt{2}}\left(|0\rangle_{\mathrm{c}}|(i-1) \bmod d\rangle_{\mathrm{p}}+|1\rangle_{\mathrm{c}}|(i-1) \bmod d\rangle_{\mathrm{p}}\right)\right.\\
&\quad\left.+\frac{\beta_i}{\sqrt{2}}\left(|0\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}-|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right)\right]\\
&=\sum_{i=-(j+1)}^{-1}\left(\alpha_i'|0\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}+\beta_i'|1\rangle_{\mathrm{c}}|i \bmod d\rangle_{\mathrm{p}}\right). \qquad (20)
\end{aligned}
$$

Because $2<j+1\leq d-1$, the measurement result of walker will not appear $|0\rangle_{\mathrm{p}}$. The Lemma 2 holds.

Proposition 1 The result of our proposed protocol is correct.

Proof The final QWs particles' states are $U_{\mathrm{o}}^{m_1-m_2}|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}$. Because $0\leq m_1,\ m_2\leq d-1$, so that $-(d-1)\leq m_1-m_2\leq d-1$. When $m_1=m_2$ the $U_{\mathrm{o}}^{m_1-m_2}$ equals to $I_{\mathrm{c}}\otimes I_{\mathrm{p}}$. According to Lemma 1 and Lemma 2, the following result can be proved:

if $m_1>m_2$, the measurement results may appear $|0\rangle_{\mathrm{p}}$, but not all of them are;

if $m_1=m_2$, the measurement result can only be $|0\rangle_{\mathrm{p}}$;

if $m_1<m_2$, the measurement results won't appear $|0\rangle_{\mathrm{p}}$.

Therefore, the proposition holds.

4.2. Outside attack

During the execution of our protocol, there might exist an outside attacker Eve. We assume that she tries a variety of approaches to obtain the secret messages such as intercept-resend attack, entangle-measure attack.

4.2.1. Intercept-resend attack

The intercept-resend attack means the eavesdropper will measure the particles and send fake quantum particles to the receiver according to the measurement results.[27] Our protocol performs well in detecting this kind of attack.

We utilize the decoy particle in our proposed protocol, which has been widely used in other protocols,[26,29–31] to detect the intercept-resend attack. It is familiar with the method adopted in the BB84 protocol,[9] and the security of BB84 has been proven already.

In our proposed protocol, we insert 2λ decoy particles, which belong to the set $\{|0\rangle,|1\rangle,\ldots,|d-1\rangle,F|0\rangle,F|1\rangle,\ldots,F|d-1\rangle\}$, into the QWs particles. Under the circumstance of the decoy particles' randomizing, Eve would not know the measurement basis and the position of the decoy particles. As a result, each particle has a probability of $\frac{d-1}{2d}$ in introducing mistakes. If λ is large enough, the probability of detecting the existence of the eavesdropper will close to 1.

Furthermore, even if the attack is undetected, the eavesdropper cannot obtain any useful message because we encrypt the QWs particles using $P_{k1}/P_{k2}/P_{k3}$ before each transmission.

4.2.2. Entangle-measure attack

The entangle-measure attack means the attacker Eve intercepts the particles from the quantum channel. Then she applies a unitary operator on the particles to entangle them with his auxiliary quantum state. So that she may achieve the secret messages with the help of the auxiliary quantum state. We will demonstrate that our proposed protocol can withstand such an attack.

We adopt the d-dimensional quantum state as the decoy particle. Eve's unitary transformation can be expressed as

$$
E(|j\rangle|e\rangle)=\sum_{k=0}^{d-1}\lambda_{jk}\left|m_{jk}\right\rangle\left|e_{jk}\right\rangle, \qquad (21)
$$

where $\sum_{k=0}^{d-1}\left|\lambda_{jk}\right|^2=1$, and $\left|m_{jk}\right\rangle$, $\left|e_{jk}\right\rangle$ are two sets of the orthogonal basis of the systems to which $|j\rangle$ and $|e\rangle$ belong. The particle $|e\rangle$ is the auxiliary particle that belongs to Eve.

Eve tries not to introduce error during the attack and aims to get useful messages from the intercepted particles. The equations can be expressed as

$$
\begin{cases}
E|j\rangle|e\rangle=|j\rangle\left|e_j\right\rangle,\\
E\cdot(F|j\rangle|e\rangle)=F|j\rangle\left|e_{Fj}\right\rangle.
\end{cases} \qquad (22)
$$

The auxiliary particles should satisfy the following rules $\langle e_j|e_k\rangle = 0$, $(j \neq k)$. Now we rewrite the left part of the second equation in Eq. (22) as

$$\begin{aligned}|\varphi\rangle &= E\cdot(F|j\rangle|e\rangle) = E\left(\frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\mathrm{e}^{\frac{2\pi \mathrm{i}jk}{d}}|k\rangle|e\rangle\right)\\ &= \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\sum_{y=0}^{d-1}\lambda_{ky}\mathrm{e}^{\frac{2\pi \mathrm{i}jk}{d}}|m_{ky}\rangle|e_{ky}\rangle. \end{aligned} \tag{23}$$

We can compute the density matrixes of the whole system as

$$\begin{aligned}|\varphi\rangle\langle\varphi| &= \frac{1}{d}\left(\sum_{k=0}^{d-1}\sum_{y=0}^{d-1}\lambda_{ky}\mathrm{e}^{\frac{2\pi \mathrm{i}jk}{d}}|m_{ky}\rangle|e_{ky}\rangle\right)\\ &\times\left(\sum_{k=0}^{d-1}\sum_{y=0}^{d-1}\lambda_{ky}\mathrm{e}^{\frac{-2\pi \mathrm{i}jk}{d}}\langle m_{ky}|\langle e_{ky}|\right). \end{aligned} \tag{24}$$

Therefore, the reduced density matrixes of the participants' system are

$$\frac{1}{d}\sum_{k=0}^{d-1}\sum_{y=0}^{d-1}(\lambda_{ky})^2|m_{ky}\rangle\langle m_{ky}|. \tag{25}$$

The reduced density matrices clearly have little to do with the variable j Therefore, after the eavesdropper entangles the auxiliary particles with the participants' particles, all the subsystems of decoy particles are the same to the eavesdropper That means Eve cannot obtain any useful messages.

Above all, our protocol can detect the usual outside attack.

4.3. Internal attack

In this subsection we will discuss the probability of the attack from Alice, Bob and TP. In our proposed protocol, if Alice (Bob) wants to obtain the secret messages by intercepting the particles sent through the quantum channel, they are the same as the outside attackers. Thus, the proof in Subsection 4.2 can ensure the detection of their attacks.

The brute-force attack[54] means the attacker measures the particles to obtain the secret messages, even though he is at the risk of being detected. In our proposed protocol, there is no chance for the participants to launch attacks. (1) In Step 4, Alice may try to send fake particles $|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}$ to TP and adopts the brute-force attack in Step 6 to obtain Bob's secret messages. However, TP makes another encryption P_{k2} in Step 5, which makes Alice would not obtain any useful messages through this kind of method. (2) Bob may launch a brute-force attack in Step 4. Since Bob does not know the original encryption P_{k1} of TP, he will not be aware of Alice's secret messages even if he adopts the brute-force attack.[54] (3) TP may launch an attack at Step 4 and Step 6. However, Alice makes an encryption P_{k3} to prevent TP from obtaining the secrets in Step 4. The QWs state in Step 6 is $U^{m_1-m_2}|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}$, therefore, TP would not obtain the secret messages of each participant in Step 6.

In conclusion, the participants have little probability of gaining the secret messages.

5. Comparison

We analyze the advantages of our protocol from three perspectives: efficiency, security and implementation. Because the QPC protocol based on quantum walks is novel, we mainly focus on the comparison of our protocol with Chen *et al.*'s protocol.[48]

5.1. Qubit efficiency

Qubit efficiency is a widely used method to measure the efficiency of protocol execution. It is defined as $\eta = c/q$, where c represents the maximum compared bits of the secret messages, and q denotes the consumed qubit during the protocol execution. Because the qubits in our protocol are in d dimensions, we redefine the qubit efficiency as $\eta' = c/q'$, where $q' = q\times\log_2 d$.

In our proposed protocol, there are k pair of walker states and coin states. The walker states are in d dimensions, and the coin states are the two-dimensional qubits. The secret messages of the participants are in range $[0, d-1]\cap\mathrm{Z}$, which means the maximum compared bits of the secret messages are $\log_2 d$. Therefore, the qubit efficiency of our protocol is $\eta = \frac{\log_2 d}{k\cdot(\log_2 d+1)}$. In Chen *et al.*'s protocol[48] however, the secret messages of the participants belong to the range $\left[0, \left\lfloor\frac{d-1}{2}\right\rfloor\right]\cap\mathrm{Z}$, which means the qubit efficiency of Chen *et al.*'s protocol[48] is $\eta = \frac{\log_2 d-1}{k\cdot(\log_2 d+1)}$.

Although our definition of qubit efficiency differs from the standard one, it can still accurately describe the protocol's efficiency. The comparison result above suggests that the maximum compared classical bits in our protocol have one more than the bits in Chen *et al.*'s protocol.[48] As a result, Alice and Bob's maximum secret messages in our protocol are double those in Chen *et al.*'s protocol.[48]

5.2. Security

The QWs particle has its uniqueness in security. Compared with the protocols that adopt the entanglement state,[27–31] there is no pre-distribution with the QWs particle. Thus, plenty of attacks on the entangled states can be avoided.

Furthermore, there is no security check in Chen *et al.*'s protocol[48] to ensure that the transmitted particles are the original particles prepared by TP. Therefore, Alice has a variety of attack options such as the brute-force attack. We fix this slight defect by changing the structure of the protocols, ensuring all the participants are unable to launch attacks.

5.3. Implementation

The initial QWs state is $|0\rangle_{\mathrm{c}}|0\rangle_{\mathrm{p}}$, which is a product state. Compared with the entangled state, it has some clear advantages. The measurement and the preparation of the QWs state

are much easier than that of the entangled state.[44] Furthermore, we only use the evolution operator U_o during the execution of our protocol, which makes our proposed protocol can be easily realized by the quantum gate and circuits. This reduced the costs and equipment requirements Above all, our protocol is easy to be implemented.

6. Conclusion

In summary, the previous QWs-based QPC protocol is not efficient enough. We proposed a protocol based on ODQWC with a semi-honest third party. The QWs particles do not exist entanglement in the initial state, and it moves by applying the evolution operator. This makes our protocol has the advantages of the single-particle protocol, which is easy to be implemented. In terms of efficiency, we enlarged twice the range of the participants' messages than the previous protocols by setting a flag to judge the comparison results. The correctness of our protocol has been proven. Moreover, we analyzed the security of our protocol from the participants' attacks and the outside attacks. Our protocol can protect against well-known attacks and brute-force attacks from the participants.

Although our proposed protocol has several advantages, however, it still needs more discussions and investigations. Such as the extension of QWs-based QPC protocols to multi-party comparison. Besides, the number of QWs particles consumed in our proposed protocol still needs diminution.

Acknowledgements

Project supported by the National Key R&D Program of China (Grant No. 2020YFB1805405), the 111 Project (Grant No. B21049), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2019BDKFJJ014), and the Fundamental Research Funds for the Central Universities, China (Grant No. 2020RC38).

References

[1] Yao A C 1982 *23rd annual symposium on foundations of computer science (sfcs 1982)*, November 3–5, 1982 Chicago, IL, p. 160
[2] Benaloh J C and Yung M 1986 *Proceedings of the fifth annual ACM symposium on Principles of distributed computing*, August 11–13, 1986, Calgary Alberta, Canada, p. 52
[3] Li T, Yang H, Wang Y and Xu Q 2015 *IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, March 24–27, 2015, Gwangiu, South Korea, p. 293
[4] Pu H, Cui Z, Liu T, Wu Z and Du H 2021 *Int. J. Netw. Secur.* **23** 97
[5] Karnin E, Greene J and Hellman M 1983 *IEEE Trans. Inf. Theory* **29** 35
[6] Beimel A 2011 *International conference on coding and cryptology*, May, 2011, Berlin, Heidelberg, p. 11
[7] Fălămaş D E, Marton K and Suciu A 2021 *Symmetry* **13** 894
[8] Rieffel E and Polak W 2000 *ACM Comput Surv* **32** 300
[9] Bennet C 1984 *Systems and Signal Processing, Systems and Signal Processing*, December 10–12, 1984, Bangalore, India, p. 175
[10] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[11] Wang L, Zhao S M, Gong L Y and Cheng W W 2015 *Chin. Phys. B* **24** 120307
[12] Lucamarini M, Yuan Z L, Dynes J F and Shields A J 2018 *Nature* **557** 400
[13] Sekga C and Mafu M 2021 *Chin. Phys. B* **30** 120301
[14] Hillery M, Buzek V and Berthiaume A 1999 *Phys. Rev. A* **59** 1829
[15] Zhang Z, Yang J, Man Z and Li Y 2005 *Eur. Phys. J. D* **33** 133
[16] Hwang T, Hwang C C and Li C M 2011 *Phys. Scr.* **83** 045004
[17] Zhou Y, Yu J, Yan Z, Jia X, Zhang J, Xie C and Peng K 2018 *Phys. rev. lett.* **121** 150502
[18] Wu X, Wang Y and Huang D 2020 *Phys. Rev. A* **101** 022301
[19] Long G L, Deng F G, Wang C, Li X H, Wen K and Wang W Y 2007 *Front. Phys. China* **2** 251
[20] Long G L, Wang C, Deng F G and Zheng C 2013 *Conference on Coherence and Quantum Optics*, June 17–20, 2013, Rochester, New York, United States, p. M6. 42
[21] Zhang W, Ding D S, Sheng Y B, Zhou L, Shi B S and Guo G C 2017 *Phys. rev. lett.* **118** 220501
[22] Zhu F, Zhang W, Sheng Y and Huang Y 2017 *Sci. Bull.* **62** 1519
[23] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[24] Liu W, Wang Y B and Cui W 2012 *Commun. Theor. Phys.* **57** 583
[25] Zhang W W, Li D, Zhang K J and Zuo H J 2013 *Quantum inf. process* **12** 2241
[26] Lin S, Sun Y, Liu X F and Yao Z Q 2013 *Quantum inf. process* **12** 559
[27] Jiang L Z 2020 *Quantum inf. process* **19** 1
[28] Lang Y F 2021 *Int. J. Theor. Phys.* **60** 4030
[29] Zhou N R, Xu Q D, Du N S and Gong L H 2021 *Quantum inf. Process* **20** 1
[30] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[31] Liu W and Wang Y B 2012 *Int. J. Theor. Phys.* **51** 3596
[32] Xu Q D, Chen H Y, Gong L H and Zhou N R 2020 *Int. J. Theor. Phys.* **59** 1798
[33] Huang X, Zhang S B and Cheng W 2021 *IEEE AFRICON 2021* September 13–15, 2021, Arusha, Tanzania, p. 1
[34] Liu W and Yin H W 2021 *Mod. Phys. Lett.* **36** 2150083
[35] Guo F Z, Gao F, Qin S J, Zhang J and Wen Q Y 2013 *Quantum inf. process* **12** 2793
[36] Ji Z X and Ye T Y 2017 *Quantum Inf. Process* **16** 1
[37] Huang X, Zhang S B, Chang Y, Hou M and Cheng W 2021 *Int. J. Theor. Phys.* **60** 3783
[38] Ji Z, Fan P and Zhang H 2022 *Physica. A* **585** 126400
[39] Jia H Y, Wen Q Y, Li Y B and Gao F 2012 *Int. J. Theor. Phys.* **51** 1187
[40] Chang Y J, Tsai C W and Hwang T 2013 *Quantum inf. process* **12** 1077
[41] Yang Y G, Xia J, Jia X, Shi L and Zhang H 2012 *Int. J. Quantum Inf.* **10** 1250065
[42] Liu B, Gao F, Jia H y, Huang W, Zhang W W and Wen Q Y 2013 *Quantum inf. process* **12** 887
[43] Liu B, Xiao D, Huang W, Jia H Y and Song T T 2017 *Quantum Inf. Processing* **16** 180
[44] Pan H M 2018 *Int. J. Theor. Phys.* **57** 3389
[45] Yan-Feng L 2018 *Int. J. Theor. Phys.* **57** 3048
[46] Lin P H, Hwang T and Tsai C W 2019 *Quantum Inf. Processing* **18** 1
[47] Gao F, Wen Q Y and Zhu F C 2007 *Phys. Lett. A* **360** 748
[48] Chen F L, Zhang H, Chen S G and Cheng W T 2021 *Quantum Inf. Processing* **20** 178
[49] Xue P, Qin H, Tang B, Zhan X, Bian Z H and Li J 2014 *Chin. Phys. B* **23** 110307
[50] Li D, Michael M G, Zhang W W and Zhang K J 2015 *Chin. Phys. B* **24** 050305
[51] Li T Y, Zhang Y S and Yi W 2021 *Chin. Phys. Lett* **38** 030301
[52] Farhi E and Gutmann S 1998 *Phys. Rev. A* **58** 915
[53] Mohseni M, Rebentrost P, Lloyd S and Aspuru-Guzik A 2008 *J. Chem. Phys.* **129** 174106
[54] Wen Q, Qin S and Gao F 2014 *Journal of Cryptologic Research* **1** 200
[55] Hao Q and Xue P 2015 *Chin. Phys. B* **25** 010501