

Unidirectional quantum private comparison based on quantum private query

Hexiang Sun(孙鹤翔), Ding Xing(邢丁), Zhao Dou(窦钊), Jian Li(李剑), Xiubo Chen(陈秀波), and Lixiang Li(李丽香)

Citation: Chin. Phys. B, 2025, 34 (**5**): 050308. DOI: 10.1088/1674-1056/adc662
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Multi-party semi-quantum private comparison protocol of size relation based on two-dimensional Bell states

Bing Wang(王冰), Li-Hua Gong(龚黎华), and San-Qiu Liu(刘三秋)
Chin. Phys. B, 2024, 33 (**11**): 110303. DOI: 10.1088/1674-1056/ad73ae

Approximate error correction scheme for three-dimensional surface codes based reinforcement learning

Ying-Jie Qu(曲英杰), Zhao Chen(陈钊), Wei-Jie Wang(王伟杰), and Hong-Yang Ma(马鸿洋)
Chin. Phys. B, 2023, 32 (**10**): 100307. DOI: 10.1088/1674-1056/acd8a9

Efficient quantum private comparison protocol utilizing single photons and rotational encryption

Tian-Yi Kou(寇天翊), Bi-Chen Che(车碧琛), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**6**): 060307. DOI: 10.1088/1674-1056/ac65f0

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

Jv-Jie Wang(王莒杰), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**5**): 050308. DOI: 10.1088/1674-1056/ac5a3f

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

SPECIAL TOPIC — Quantum communication and quantum network

Unidirectional quantum private comparison based on quantum private query

Hexiang Sun(孙鹤翔)[1], Ding Xing(邢丁)[1], Zhao Dou(窦钊)[1,†], Jian Li(李剑)[2], Xiubo Chen(陈秀波)[1], and Lixiang Li(李丽香)[1]

[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 13 February 2025; revised manuscript received 7 March 2025; accepted manuscript online 28 March 2025)

Previous bidirectional quantum private comparison (BQPC) protocols cannot meet the requirements in some special application scenarios, where only one party needs to obtain the comparison results without a third party (TP), such as scenarios for authority surveys or healthcare data sharing. In addition to this, the BQPC protocol has the potential of information leakage in multiple comparisons. Therefore, we design a new unidirectional quantum private comparison (UQPC) protocol based on quantum private query (QPQ) protocols with ideal database security and zero failure probability (IDS-ZF), for the reason that they have excellent unidirectionality and security. Concretely, we design a UQPC protocol based on Wei *et al.*'s work [*IEEE Transactions on Computers* **67** 2 (2017)] and it includes an authentication process to increase the resistance to outside attacks. Moreover, we generalize the protocol and propose a general model that can transform a QPQ protocol with or without the IDS-ZF property into a secure UQPC protocol. Finally, our study shows that protocols using our model are secure, practical, and have the IDS-ZF property.

Keywords: quantum private comparison, unidirectionality, identification, general model

PACS: 03.67.Hk

DOI: 10.1088/1674-1056/adc662 **CSTR:** 32038.14.CPB.adc662

1. Introduction

In a general scenario of private comparison, two participants, Alice and Bob, possess two secret input numbers, a and b, respectively. They aim to compare these numbers without knowing each other's input. Originating from Yao's work[1] in 1982, this problem is also known as Yao's millionaires' problem and is the foundation for secure multi-party computation (SMC). However, the classical private comparison is not unconditionally secure, and to achieve unconditional security, we need to introduce quantum mechanical properties.

In 1984, Bennett and Brassard proposed the first quantum key distribution protocol (BB84),[2] ensuring the secure sharing of a common random key between two remote users. Subsequently, researchers attempted to use principles of quantum mechanics to address security tasks that are problematic or impossible in classical cryptography.[3] The quantum counterpart of private comparison is a hot research topic in the field of quantum information known as quantum private comparison (QPC). Unfortunately, achieving two-party quantum secure computation is impossible, as Lo demonstrated in Ref. [4]. However, this goal may be realized with additional assumptions, such as the inclusion of a third party (TP). The first QPC protocol was proposed by Yang *et al.*,[5] using Einstein–Podolsky–Rosen (EPR) pairs. In their protocol, a TP is required to prepare photons and announce the comparison results. Afterward, numerous entangled-state-based QPC protocols[6–11] have been proposed. Recently, Gong *et al.*[12] proposed two semi-quantum privacy comparison protocols based on decoherence-free states to resist collective noise. One protocol can effectively resist collective dephasing noise, and the other can resist collective rotation noise. In addition, there has been abundant research on semi-quantum QPC[13–16] in recent years, which reduces the requirement of quantum capability of users, extends the application environment and promotes multiple-party comparison. To reduce the difficulty of quantum state preparation and measurement, Liu *et al.*[17] proposed a privacy comparison protocol based on GHZ-like states of three four-dimensional particles. This protocol reduces the difficulty of quantum state preparation and measurement and does not involve unitary operations; only single-particle measurements are required.

In addition to the QPC protocol, there is another hot research topic in the field of quantum information, i.e., quantum private query (QPQ). In this scenario, Bob has a secret database comprising N entries, each containing valuable and sensitive information that he intends to sell. Alice, as a potential buyer, aims to purchase a specific entry from Bob, knowing its address in the database. She expects her interest to

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

© 2025 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

remain confidential. To ensure privacy for both parties:

• Bob should not know which entry Alice is purchasing.

• Alice should not access any entries other than the one she is interested in.

However, because Lo demonstrated in Ref. [4], its security requirements of QPQ are generally relaxed: (i) Alice is sensitive to Bob's illegal behavior (i.e., Alice has a nonzero probability of detecting Bob's illegal behavior after the protocol). (ii) Alice may obtain more than the ideal requirement (exactly one entry), but the total number of entries she can obtain is strictly limited.

In 2008, Giovannetti *et al.*[18] proposed the first QPQ protocol, encoding the entire database as a unified operation, referred to as an oracle. Later, Olejnik,[19] Yu and Qiu[20] made improvements to the proposed solution. Subsequently, Jakobi *et al.*[21] proposed a new QPQ protocol based on quantum oblivious key transfer (QOKT), which is based on the SARG04 QKD protocol.[22] Despite the numerous excellent QPQ protocols[23–25] having been proposed, it is noteworthy that Wei *et al.*[26] presented a QPQ protocol with ideal database security and zero failure probability (IDS-ZF), providing a general QOKT-PQ model. The IDS property means that Alice can only access the entry she purchased, without gaining additional information. The ZF property ensures that the protocol does not fail under normal conditions, in contrast to many QPQ protocols that still have a failure probability even when executed smoothly without outside interference. The IDS property enhances the security of the protocol by preventing the random leakage of other data, while the ZF property improves the protocol's efficiency by avoiding failures, thus preventing losses caused by protocol failure. QPQ protocols with this IDS-ZF feature have excellent unidirectionality, i.e., only one party can obtain information from the other party. Recently, due to the limitations of devices, Sun *et al.*[27] proposed a semi-device-independent multi-user QPQ scheme, which allows each user to retrieve different items simultaneously while protecting their privacy; Qin *et al.*[28] proposed a bidirectional communication decoy-state quantum private query protocol, which can effectively resist multi-photon pulse attacks; Jiao *et al.*[29] proposed user privacy analysis and protection in non-ideal light source quantum private query. This scheme enables users to detect and effectively resist multi-photon attacks launched by the database by calculating the proportion of multi-photon pulses, moving keys, and selecting appropriate light sources.

Even though many QPC protocols have been designed, they still cannot satisfy all application scenarios. The previous QPC protocols are all bidirectional with a TP, which means both parties can know the result of the protocol. However, in some application scenarios, the private information of the parties will be leaked in a large number of comparisons. Here are two examples: authority surveys and healthcare data sharing. In the authority surveys scenario, a state department or authoritative organization Alice needs to conduct a statistical survey of all citizens, and multiple comparisons will cause Alice's information to be leaked to a certain extent. Because every comparison result will reveal the scope of Alice's private data. In the healthcare data sharing scenario, suppose that Alice is a hospital and Bob is a pharmaceutical company, and both parties want to compare data to determine the efficacy of certain drugs for patients, but do not want to expose sensitive patient information. The BQPC protocol allows Bob to access the comparison results, which means that Bob knows whether a certain drug is effective for certain patients, and this disclosure may violate the principle of minimal data disclosure because Bob has access to sensitive information that may reveal the health status of patients. If a new QPC protocol can be designed, in which only Alice, one of the two parties in the agreement, can obtain the comparison results and no TP is involved, this will solve the information leakage problem caused by the above scenarios.

Under such a requirement, we design a unidirectional QPC (UQPC) protocol based on the QPQ protocol. For this reason, the QPQ protocol has excellent unidirectionality as well as security. Its security has already been mentioned before, and unidirectionality is reflected in the fact that Alice can privately query data from Bob while Bob knows nothing about Alice's query. Since the application scenarios of the UQPC protocol and the BQPC protocol are different, the required security is also different. Therefore, we give the new security requirements for the UQPC protocol:

• Alice and Bob's private information will not be leaked to anyone.

• The comparison result of the protocol is only known to Alice.

It is due to the limitations of the previous QPC protocols that we design a new UQPC protocol to meet the application requirements of special scenarios. Our protocol is designed based on Wei *et al.*'s protocol[26] because it has the IDS-ZF feature, which ensures the security between two parties in our protocol. It also has an authentication process, which enhances the resilience against outside attacks. Furthermore, we generalize the protocol and propose a general model. Applying our model, QPQ protocols[28–31] with or without the IDS-ZF feature can securely perform the unidirectional comparison task. We take the Jacobi *et al.* protocol (J-protocol)[21] as an example to use our model. Finally, the analysis shows that protocols using our model are secure, practical, and have IDS-ZF. In the UQPC protocol, we extend the concept of the IDS-ZF property. The IDS property implies that Alice knows only one of the bits of the final key, which ensures that Alice only has exactly one result when using the final key to obtain the com-

parison result. The concept of ZF property is the same as that of ZF property in QPQ, which is used to ensure that the UQPC protocol obtained by the transformation of QPQ does not have a probability of failure and avoids the waste of resources. In summary, we designed a secure unidirectional QPC protocol with an authentication process that does not require a TP and extended it to a general model.

The rest of the paper is organized as follows. In Section 2, we give a brief review of the protocol of Wei *et al.*[26] and J-protocol.[21] In Section 3, we describe the detailed steps of our protocol. In Section 4, we provide a general model and use the J-protocol as an example. In Section 5, we analyze the protocol in more detail, including correctness, parameters, security, IDS-ZF features, practicality, and comparison of UQPC and BQPC. Finally, we give a brief conclusion in Section 6.

2. Review of protocols

In this section, we first briefly review the protocol of Wei *et al.*[26] and then give a brief review of J-protocol.

2.1. Review of Wei *et al.*'s protocol[26]

1. Bob prepares multiple pulse trains, each consisting of $l+1$ single photons with randomly modulated phases (0 or π), and constructs the quantum state:

$$|\Psi_S\rangle = \frac{1}{\sqrt{l+1}}\sum_{i=0}^{l}(-1)^{s_i}|i\rangle, \tag{1}$$

where $s_i \in \{0,1\}$ represents the i-th bit of the randomly chosen bit string $S = s_0 s_1 \cdots s_l$. Bob sends these pulse trains to Alice.

2. Alice splits the pulse trains into two paths using a beam splitter and randomly selects a shift value $r \in \{1,2,\ldots,l\}$. She shifts the pulses accordingly. After shifting, Alice measures the pulses and obtains one-bit value $s_n \oplus s_{n'}$, where $n' = (n+r) \bmod (l+1)$. Alice records the bit value and publishes the measurement position n.

3. If Alice detects no photon, both parties discard the corresponding pulse train. Otherwise, the result is retained for generating the shared key. Repeating this process for multiple pulse trains allows Alice and Bob to accumulate enough valid bits to construct a raw key.

4. Alice and Bob divide the raw key into k substrings, each of N bits, corresponding to different segments of the database. Alice selects and claims a shift $f_i \in \{-(l-1), -(l-2), \ldots, l-1\}$ for each substring to Bob and accesses the desired index in the database. The shifted substrings are processed bitwise to compute the final key.

5. Bob encrypts the database with the final shared key and sends the encrypted database to Alice. Alice decrypts the encrypted database using the shared key to recover the desired data item.

2.2. Review of J-protocol[21]

1. Bob generates a long random sequence of qubits, where each qubit is prepared in one of the states $|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$. The states $|0\rangle$ and $|1\rangle$ encode the bit value 0, while $|+\rangle$ and $|-\rangle$ encode the bit value 1. Bob sends these qubits to Alice.

2. Alice measures each received qubit in a randomly chosen basis, either $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. Due to the possible mismatch between Bob's prepared state and Alice's measurement basis, Alice cannot directly infer the sent bit value at this stage.

3. Alice announces which qubits she successfully detected, while the lost or undetected qubits are discarded.

4. For each qubit Alice successfully measured, Bob announces a pair of states, namely, the photon's original state and one state randomly chosen from another basis. For example, Bob will announce $\{|0\rangle, |+\rangle\}$ or $\{|0\rangle, |-\rangle\}$ at random if the photon's state is $|0\rangle$. Alice uses this information and her measurement results to eliminate some possibilities and infer the sent bit value.

5. Using Bob's announced basis information and her measurement results, Alice decodes the bit values for the successfully measured qubits. Only deterministically decoded results are kept. This process generates a shared key of length $k \times N$, which can be divided into N-bit substrings for subsequent private query operations.

6. Alice uses part of the shared key $\mathrm{Key_A}$ to perform a private query. Suppose Alice knows the j-th bit of $\mathrm{Key_A}$, and wants to query the i-th database item. She announces the shift $s = j - i$. Bob uses this shift to encode the database by applying a bitwise XOR operation and sends to Alice. Using her known bit, Alice decodes the target data.

3. The proposed protocol

Based on the work of Wei *et al.*,[26] we provide a new UQPC protocol without TP, in which only one of the two parties has access to the comparison result. Let us assume that Alice and Bob hold two secret inputs a and b and Alice wants to know the relationship between the sizes of a and b. They can execute the following steps to complete the private comparison task.

1. Bob randomly generates multiple $(l+1)$-bit binary string $S = \{s_i\}_{i=0}^{l}$, $s_i \in \{0,1\}$. Using the generated string, Bob prepares the corresponding single-photon continuous coherent $(l+1)$-pulse train $|\Psi_S\rangle$. Here,

$$|\Psi_S\rangle = \frac{1}{\sqrt{l+1}}\sum_{i=0}^{l}(-1)^{s_i}|i\rangle, \tag{2}$$

where the photon is in the state $|i\rangle$ within the i-th pulse. Subsequently, Bob sends $|\Psi_S\rangle$ to Alice.

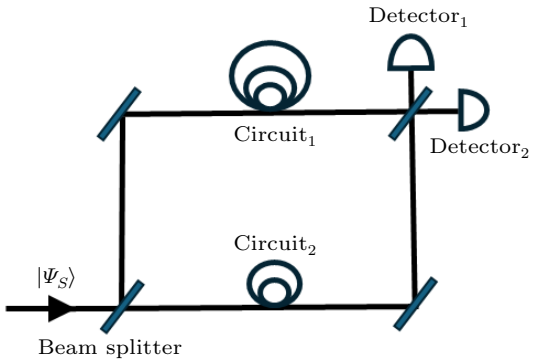


Fig. 1. Alice passes the received pulses through the first beam splitter and divides it into two light paths. In one light path, the length of Circuit$_1$ is $(l+1)$ and is only applicable to the first r pulses, while the remaining pulses can take a shortcut without passing through Circuit$_1$. The length of Circuit$_2$ in the other light path is r and is applicable to all pulses. Therefore, at the last beam splitter, Alice can obtain the interference results of the pulse sequences in the two light paths.

2. Alice first passes each received pulse train through a half-beam splitter and changes the order of the pulses in one of the light paths by r, where r is randomly chosen from $\{1,2,\ldots,l\}$. While the order of the pulses in the other light path remains unchanged. Then she superposes the pulses in the light paths in order. The interference process in this step can be found in Fig. 1. After measuring, Alice announces n to Bob if she gets the value $s_n \oplus s_{n'}$, $n' = (n+r) \bmod (l+1)$, from S', where n represents the $(n+1)$-th value of S'.

$$S' = \{s_i \oplus s_{i'}\}_{i=0}^{l}, \quad i' = (i+r) \bmod (l+1), \tag{3}$$

where $\oplus$ denotes modulo-2 summation. As a result, Bob has the full l-bit key $\mathrm{Key_B}$, while Alice knows only one bit $\mathrm{Key_A}$.

$$\mathrm{Key_B} = \{s_n \oplus s_0, \ldots, s_n \oplus s_{n-1}, s_n \oplus s_{n+1}, \ldots, s_n \oplus s_l\}, \tag{4}$$

$$\mathrm{Key_A} = \{s_n \oplus s_{n'}\}. \tag{5}$$

If Alice declares that she has failed to detect any photon, they discard the pulse train and repeat the above steps.

3. Bob sends enough single-photon pulses to Alice to make sure they share a $(N+l)$-bit string. N is the value larger than a and b, and l is much smaller than N and divides N. For example, if $b = 114, a = 150$, then $N = 200$ and $l = 4$; if $b = 5142, a = 4000$, then $N = 7000$ and $l = 8$. For the first l bits $\mathrm{Key_B}$ of the $(N+l)$-bit string, Bob announces their values, positions, and measurement bases to Alice to do a key authentication process. Alice compares key_a and key_b ($\mathrm{key}_a = s_n \oplus s_{n'} \in \mathrm{Key_A}$, key_b is the n'-th bit of $\mathrm{Key_B}$) and the measurement bases. If $\mathrm{key}_a \neq \mathrm{key}_b$ or measurement bases are different, the protocol is canceled. Otherwise, the protocol continues and they discard these l bits.

4. Alice and Bob repeat the above steps until they share a k N-bit raw key, where k is a security parameter dependent on N. It will be discussed in more detail in the protocol analysis section. If Alice and Bob go through the key authentication process k times and the values are all equal, Bob passes the identification authentication process.

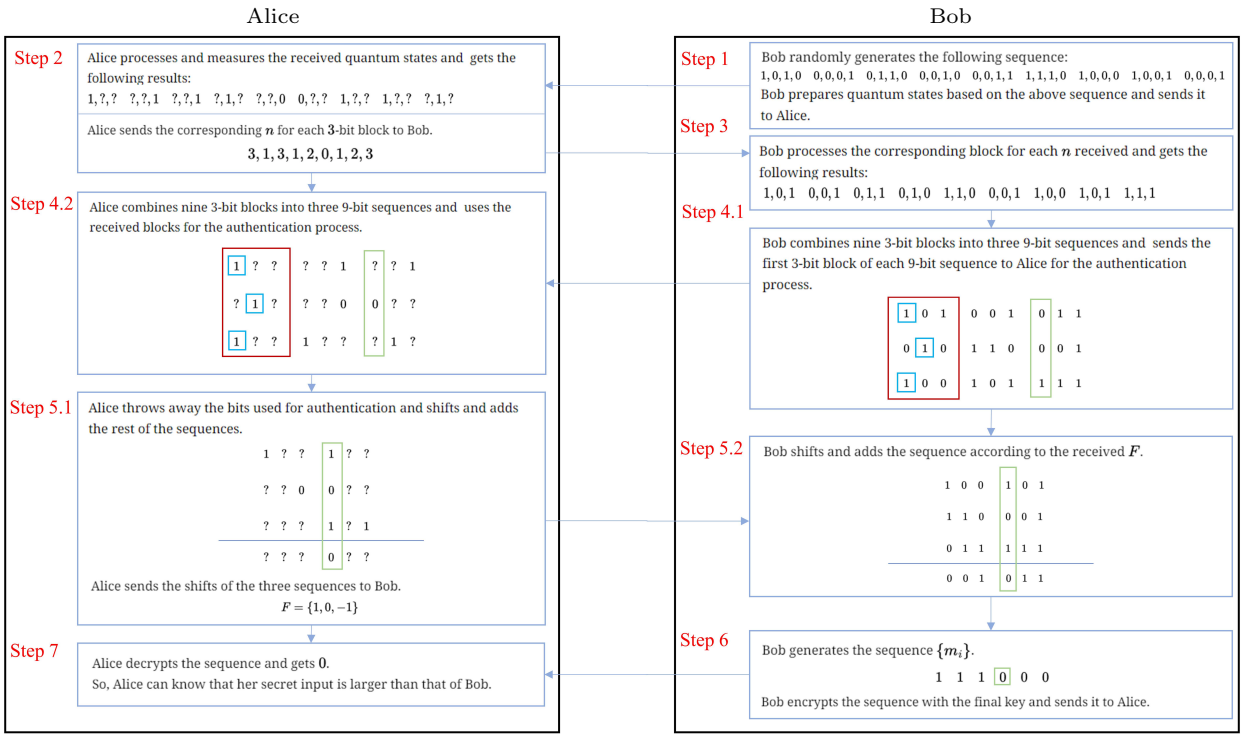


Fig. 2. Suppose Alice and Bob hold secret inputs 4 and 3. For convenience, let $N = 6$, $l = 3$ and $k = 3$. Here, Bob sends 9 pulse trains to Alice. Then, Alice passes them through the interference circuit and randomly gets one value in the sequence. After that, Alice announces n to Bob. They share a key now. The red box represents the bits Bob sends to Alice for authentication, the blue box represents the bits Alice uses to verify Bob's identity, and the green box represents the location of the value of Alice's privacy input. Alice verifies Bob's identity and they finalize the sequence. Finally, Bob constructs the special sequence and encrypts it to send to Alice, who decrypts it to get the result.

5. Alice and Bob share k N-bit keys, aligning the k keys by bits. Since Alice holds the secret input a, she chooses a shifting $f_i \in \{-(l-1),-(l-2),\ldots,l-1\}$ for the i-th ($i = 1,2,\ldots,k$) N-bit key such that Alice knows the bit at position a. Then Alice performs a modulo-2 summation on the key after shifting bitwise and announces $F = \{f_i\}_{i=1}^{k}$ to Bob.

6. Bob shifts the k N-bit key according to F. After shifting, he performs a bitwise modulo-2 summation to get the final key. Then Bob prepares N-bit strings $\{m_i\}_{i=1}^{N}$ with

$$m_i = \begin{cases} 1, & i \le b, \\ 0, & \text{otherwise}. \end{cases} \tag{6}$$

Finally, Bob encrypts $\{m_i\}$ with the final key to get $\{M_i\}$ and sends $\{M_i\}$ to Alice.

7. Alice receives $\{M_i\}$ and decrypts it with her key to get the value of the a-th bit. If the value is 1, then $a \le b$. Otherwise, $a > b$. A sketch of this protocol is shown in Fig. 2. It can be seen from this protocol process that Alice has not revealed information about her private input a to Bob and has not announced the result of the protocol to Bob at the end. So our protocol is unidirectional, only Alice knows the result of the comparison, and neither Alice nor Bob is aware of the other's private input.

4. General model

We generalize the protocol and propose a general model for transforming QPQ protocols into secure UQPC protocols. And we will also illustrate the model using J-protocol[21] as an example.

4.1. Model details

Assume Alice and Bob have secret inputs a and b. N is larger than a and b, and l is much smaller than N but divides N.

1. Bob generates a random string $\{s_i\}_{i=0}^{T-1}, s_i \in \{0,1\}$ with

$$T = \left\lceil \frac{k(N+l)}{1-(1-p)^l} \right\rceil, \tag{7}$$

where T is the total number of bits Bob sends to Alice, and k is the safety factor. Quantum states are prepared and transmitted to Alice using the preparation method in the original QPQ protocol. Value p is the probability that Alice knows each bit.

2. Alice detects the quantum state from Bob and has the string $\{s_i'\}$ ($s_i' = s_i$ or '?', '?' means that Alice does not know the value of this bit). Then Alice splits the string $\{s_i'\}$ into many short l-bit blocks. If Alice knows at least one bit of that l-bit block, the block is kept, otherwise, it is discarded. Clearly, Alice and Bob share $k[(N/l)+1]$ l-bit blocks:

$$\text{Key}_{\text{ModelA}} = \{T_j'\}_{j=0}^{k[(N/l)+1]-1}, \quad T_j' = \{s_i'\}_{i=p_j l+1}^{(p_j+1)l}, \tag{8}$$

$$\text{Key}_{\text{ModelB}} = \{T_j\}_{j=0}^{k[(N/l)+1]-1}, \quad T_j = \{s_i\}_{i=p_j l+1}^{(p_j+1)l}, \tag{9}$$

where p_j is the ordinal number of the l-bit block in the original string. For example, T_2' is the fourth l-bit block in the original string and since two previous l-bit blocks were discarded, the p_2 of T_2' is equal to 4.

3. Alice and Bob split $\text{Key}_{\text{ModelA}}$ and $\text{Key}_{\text{ModelB}}$ into k $(N+l)$-bit strings,

$$\text{key}_{\text{ModelA}}^{i} = \{T_j'\}_{j=i[(N/l)+1]}^{(i+1)[(N/l)+1]-1}, \quad i = 0,1,\ldots,k-1, \tag{10}$$

$$\text{key}_{\text{ModelB}}^{i} = \{T_j\}_{j=i[(N/l)+1]}^{(i+1)[(N/l)+1]-1}, \quad i = 0,1,\ldots,k-1, \tag{11}$$

and use each first l-bit block of $\text{key}_{\text{A}}^{i}$ to authenticate Bob's identity. These l-bit blocks are discarded if the authentication is passed, otherwise the protocol is canceled.

4. Now Alice and Bob share k N-bit keys. Alice knows at least one bit every l-bit block, while Bob knows every bit. Then Alice chooses a shifting $f_i \in \{-(l-1),-(l-2),\ldots,l-1\}$ for the i-th ($i = 1,2,\ldots,k$) N-bit key based on a and performs modulo-2 summation bitwise on the k shifted keys. After that, Alice sends $F = \{f_i\}_{i=1}^{k}$ to Bob.

5. Bob shifts the k N-bit key according to F and performs a bitwise modulo-2 summation to get the final key. Then, Bob generates an N-bit string $\{m_i\}_{i=1}^{N}$ with

$$m_i = \begin{cases} 1, & i \le b, \\ 0, & \text{otherwise}. \end{cases} \tag{12}$$

Finally, Bob encrypts $\{m_i\}$ with the final key to get $\{M_i\}$ and sends $\{M_i\}$ to Alice.

6. Alice receives $\{M_i\}$ and decrypts it with her key to get the value of the a-th bit. If the value is 1, $a \le b$. Otherwise, $a > b$.

4.2. An example: performing J-protocol with model

To illustrate the model in more detail, we use the J-protocol as an example to apply this model.

1. Bob sends a random string of $\lceil \frac{k(N+l)}{1-(3/4)^l} \rceil$ qubits in states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$. States $|0\rangle$ and $|1\rangle$ code for bit value 0, $|+\rangle$ and $|-\rangle$ correspond to bit value 1.

2. Alice measures each state in the $\{|0\rangle,|1\rangle\}$ or $\{|+\rangle,|-\rangle\}$ basis at random and announces to Bob which particles she has successfully received. For each qubit that Alice has successfully received, Bob announces a pair of two states: the one that has been sent and one from the other basis, so $\{|0\rangle,|+\rangle\}$, $\{|0\rangle,|-\rangle\}$, $\{|1\rangle,|+\rangle\}$ or $\{|1\rangle,|-\rangle\}$. Therefore, there is a $1/4$ probability that Alice can inform Bob the value. Alice splits the string into many short l-bit blocks. If Alice knows at least one bit of the l-bit block, the l-bit block is kept, otherwise it is discarded. So the length of the key they left behind should be $k(N+l)$.

3. Alice and Bob need to combine their l-bit blocks into k $(N+l)$-bit strings separately. After that, Alice uses the first l-bit block of every $(N+l)$-bit string to authenticate Bob's

identity and cancels the protocol if the authentication is not passed.

4. After discarding the l-bit blocks for the authentication, Alice and Bob share a kN-bit key and Alice has knowledge of at least one bit in every l-bit block, whereas Bob possesses knowledge of every bit in each l-bit block. Then Alice chooses a shifting f_i for the i-th N-bit key and performs modulo-2 summation on the k strings after shifting. Afterwards, Alice sends $F = \{f_i\}_{i=1}^{k}$ to Bob.

5. Bob shifts the k N-bit keys with F and performs modulo-2 summation on them to get the final key. Then he generates $\{m_i\}_{i=1}^{N}$, encrypts it with the final key to get $\{M_i\}$ and sends $\{M_i\}$ to Alice.

6. Alice receives $\{M_i\}$ and decrypts it to get the value of the a-th bit. If the value is 1, $a \leq b$. Otherwise, $a\ b$.

5. Analysis

We begin with a detailed description of the correctness of the protocol. After that, we discuss the parameters, security, practicality, IDS-ZF of the model, and comparison of UQPC and BQPC. For convenience, we use our protocol as an example to show the properties of the model, which can be shared by other protocols that utilize our model.

5.1. Correctness

In this subsection, we focus on the correctness of the proposed protocol. The initial input quantum state is

$$|\psi_s\rangle = \frac{1}{\sqrt{l+1}} \sum_{i=0}^{l} (-1)^{s_i} |i\rangle. \tag{13}$$

After the first beam splitter the quantum state is

$$|\psi_2\rangle = \frac{1}{\sqrt{2(l+1)}} \left[\sum_{i=0}^{l} (-1)^{s_i} |i\rangle|0\rangle + \mathrm{i} \sum_{i=0}^{l} (-1)^{s_i} |i\rangle|1\rangle \right]. \tag{14}$$

It is worth noting that state $|0\rangle$ represents that the photon is in the transmission path and $|1\rangle$ represents the photon is in the reflection path. In addition, i denotes an imaginary number, and i denotes the quantum state $|i\rangle$. The quantum state after Circuit$_1$ and Circuit$_2$ is

$$\begin{aligned} |\psi_3\rangle &= \frac{1}{\sqrt{2(l+1)}} \left[\mathrm{i} \sum_{i=0}^{l} (-1)^{s_i} |i\rangle|0\rangle + (\mathrm{i})^2 \sum_{i=0}^{l} (-1)^{s_{i'}} |i\rangle|1\rangle \right] \\ &= \frac{\mathrm{i}}{\sqrt{2(l+1)}} \left[\sum_{i=0}^{l} (-1)^{s_i} |i\rangle|0\rangle + \mathrm{i} \sum_{i=0}^{l} (-1)^{s_{i'}} |i\rangle|1\rangle \right], \\ & i' := (i+r) \bmod (l+1). \end{aligned} \tag{15}$$

The quantum state after passing through the last beam splitter is

$$\begin{aligned} |\psi_4\rangle &= \frac{\mathrm{i}}{\sqrt{2(l+1)}} \left[\mathrm{i} \sum_{i=0}^{l} (-1)^{s_i} |i\rangle|0'\rangle + \sum_{i=0}^{l} (-1)^{s_i} |i\rangle|1'\rangle \right. \\ &\quad \left. + \mathrm{i} \sum_{i=0}^{l} (-1)^{s_{i'}} |i\rangle|0'\rangle + (\mathrm{i})^2 \sum_{i=0}^{l} (-1)^{s_{i'}} |i\rangle|1'\rangle \right] \\ &= \frac{\mathrm{i}}{\sqrt{2(l+1)}} \left\{ \sum_{i=0}^{l} [(-1)^{s_i} - (-1)^{s_{i'}}] |i\rangle|1'\rangle \right. \\ &\quad \left. + \mathrm{i} \sum_{i=0}^{l} [(-1)^{s_i} + (-1)^{s_{i'}}] |i\rangle|0'\rangle \right\}. \end{aligned} \tag{16}$$

The state $|0'\rangle$ means that the photon is in the light path leading to the Detector$_1$ while $|1'\rangle$ means that the photon is in the light path leading to the detector Detector$_2$.

From the results we can see that if $s_i = s_{i'}$, then Alice may find a photon in Detector$_1$ but not in Detector$_2$. Conversely, if $s_i \neq s_{i'}$, then Alice may find a photon in Detector$_2$ but not in Detector$_1$. Therefore, as long as Alice detects the presence of photons in the $(n+1)$-th pulse, she will know that the value is $s_n \oplus s_{n'}, n' = (n+r) \bmod (l+1)$.

5.2. Parameters

In the first step of the model, Bob prepares a random sequence of T bits,

$$T = \left\lceil \frac{k(N+l)}{1-(1-p)^l} \right\rceil, \tag{17}$$

where p is Alice's success probability in knowing each bit, and k and l will be described later. Thus, the probability that Alice knows nothing about a l-bit block is $(1-p)^l$, while the probability that Alice knows at least one bit is $1-(1-p)^l$. So, it can be calculated that the number of blocks left after Alice throws away the unusable blocks is $k[(N/l)+1]$. After identification, Alice leaves $k(N/l)$ blocks. We make the expected number of bits that Alice's key holds after k dilutions n_k, where diluting once means that the key held by Alice is then summed bitwise with an N-bit string. We can get

$$n_{k+1} = p(n_k - 1) + 1, \tag{18}$$

and we can go further and make simple estimates

$$n_k = (N-1)p^k + 1. \tag{19}$$

The above equation is the expected case. Using our protocol as an example, we can make $p = 1/l$ and get

$$n_k = \frac{N-1}{l^k} + 1. \tag{20}$$

The $(N-1)/l^k$ will rapidly converge to 0 as k increases. Moreover, we can calculate the probability that the number of Alice's bits does not change after one dilution according to Ref. [26]:

$$P(n_{k+1} = n_k) \leq (2l-1)p^{n_k}. \tag{21}$$

Therefore, we can get

$$P(n_{k+1} < n_k) = 1 - P(n_{k+1} = n_k). \tag{22}$$

Take our protocol as an example,

$$P(n_{k+1} < n_k) = 1 - P(n_{k+1} = n_k) \geq \left(\frac{l-1}{l}\right)^2, \quad n_k \geq 2. \quad (23)$$

It can be seen that as k increases, the probability that the number of bits in Alice's possession decreases is greater than $[(l-1)/l]^2$ when $n_k \geq 2$. So, we can quickly reduce the number of bits in Alice's hands to 1 by choosing the right k.

According to the analysis in Ref. [26], there are maximum, minimum, and mean recommended values of k for different N, l, and u (the average number of photons in the weakly coherent source system). In the case of $l = 8$, $u = 0.1$, and $N = 10000$, the maximum value of k is only 8 and the minimum value is 5. In the application scenario where the security requirements are not so high, k is sufficient at the minimum value.

For the choice of other parameters, it needs to be adjusted according to the private inputs of both parties in the protocol. Theoretically, N can be simply as long as it is greater than a and b or negotiated by both parties. As for the choice of l, it can be found in Ref. [26].

5.3. Security

Our protocol is based on the QPQ protocol and thus inherits its security. For the two parties comparison, we do not decrease the security of the original protocol, but add the authentication process on top of it, which enhances the resistance of the protocol to outside attacks. According to the security requirements of UQPC presented in the Introduction section, the following discussion will be conducted from three aspects: inside attack, outside attack, and comparison result.

5.3.1. Inside attack

For Alice's attack, Bob's security can be guaranteed. Alice could have measured multiple photons in a pulse before declaring the measuring successfully, but such behavior would have resulted in an extremely high photon loss rate, and Bob would have easily detected this attack. Meanwhile, the quantum memory attack is not possible because Bob does not leak information about the photons or private input b. In the face of dishonest Alice, the upper bound on the dishonest Alice's information about Bob's database via the Holevo bound[32] can be calculated:

$$H(A: \text{Database}) \leq \log(N+1), \quad (24)$$

where $H(A: \text{Database})$ denotes the amount of information that Alice can gain about Bob's database.

For Bob's attack, Alice's security can also be guaranteed. In a mutually untrusted two-party computation, the party responsible for generating the quantum signal has a greater deception advantage than the other party,[33] including QPQ. In our protocol, Bob has this advantage, however, our protocol has deception sensitivity and authentication to protect Alice's privacy. Deception sensitivity means Alice can detect Bob's illegal behaviors. And similar to the analysis in the original round-robin differential-phase-shift (RRDPS) QKD protocol,[30] our protocol has deception sensitivity. Not only that, our protocol has an authentication process in which Alice can verify Bob's honesty by verifying some of the measurement bases and results. Finally, a brief proof of the deception sensitivity of the protocol is given below.

Suppose that Bob prepares the following entangled state to send to Alice:

$$\sum_{i=1}^{2^l} \lambda_i |\Lambda_i\rangle_{\mathrm{B}} |\Psi_{S_i}\rangle_{\mathrm{A}}, \quad (25)$$

where $\sum_i |\lambda_i|^2 = 1$ and $|\Lambda_i\rangle$ is the orthogonal measurement basis selected by Bob satisfying $\langle\Lambda_i|\Lambda_j\rangle = \sigma_{ij}$. The state $|\Psi_{S_i}\rangle$ is further defined as

$$|\Psi_{S_i}\rangle = \frac{1}{\sqrt{l+1}} \left(|0\rangle + \sum_{k=1}^{l} (-1)^{S_{i,k}} |k\rangle\right),$$
$$\langle\Psi_{S_i}|\Psi_{S_j}\rangle \neq 1, \text{ for } i \neq j. \quad (26)$$

Ignoring the overall phase, it is easy to find that $|\Psi_{S_i}\rangle$ is the same as

$$|\Psi'_{S_i}\rangle = \frac{1}{\sqrt{l+1}} \left(-|0\rangle + \sum_{k=1}^{l} (-1)^{S_{i,k}\oplus 1} |k\rangle\right). \quad (27)$$

Bob sends system A to Alice and keeps system B. After Alice measures system A, Bob can measure system B from measurement basis $|\Lambda_i\rangle$ to get the value of S_i and give the correct result of the comparison, but he will not know which bit Alice has. However, Bob can also use other measurements to get the location information of the bit Alice has, but he will not be able to obtain complete information about S_i and he cannot be sure to give Alice the correct result. Thus, our protocol is deception-sensitive.

5.3.2. Outside attack

The security of protocols against outside attacks will be analyzed from three perspectives: information theory, imperfect device for Alice, imperfect device for Bob, and the role of authentication in outside attack. In the context of information theory, during the key distribution phase, Bob's private information b has nothing to do with the published information S and M_i, so the mutual information

$$I(b; S, M_i) = 0. \quad (28)$$

Due to the dilution effect of bitwise addition following the shifts of Alice's k N-bit sequences, the intermediate information stolen by an outside attacker E_2 during the protocol process contributes nearly nothing to Alice's final key K. In other

words, the mutual information

$$I(K;E_2) = 0, \tag{29}$$

thereby significantly limiting the attacker's ability to infer Alice's final key.

In the face of imperfect device for Alice, Alice passes the received photon beam through the splitter and performs a series of operations to obtain $\mathrm{Key_A} = \{s_n \oplus s_{n'}\}$ in the second step of the protocol. Alice publishes n, but does not publish the randomly selected parameter r. Even if an outside attacker exploits the vulnerability of the imperfect device to get extra photons, he does not know r after using the splitter, and therefore cannot perform the same operation as Alice in the second step of the protocol. So he cannot get Alice's $\mathrm{Key_A}$, much less Alice's final key. Therefore, Alice will not leak the private information a in the face of attacks brought about by imperfect devices.

In addition, in the face of imperfect devices of Bob, if the outside attacker wants to use the vulnerabilities from imperfect devices to obtain Bob's private information b, he needs to intercept all single-photon pulse sequences and only allow multiple-photon pulse sequences to pass. Because he needs to separate the photons from the multi-photon pulse sequences to get the information. However, as long as he engages in this kind of behavior, it will inevitably lead to an extremely high photon loss rate, which will be discovered by Bob. So, despite the presence of the imperfect devices, the outside attacker cannot know Alice or Bob's private inputs and keys.

From the perspective of the role of authentication in outside attack, Alice may get the wrong comparison result under the interference of outside attacks. If there is no means to defend against outside attacks, this error will not be distinguishable from Bob's illegal behavior.[24] Our protocol has an authentication process, which can confirm Bob's identity as well as detect eavesdropping.[33] If Bob fails the authentication process, the protocol is canceled. However, as long as the authentication process and eavesdropping detection are passed, where Alice successfully compares the keys and measurement bases, there is no outside attack. After the authentication process, if Alice gets the wrong comparison result, Alice can determine that it is caused by Bob's illegal behavior.

5.3.3. Security of comparison result

The protocol ensures the security of Alice's final key and comparison results by limiting the information shared with Bob in two ways.

The first aspect is that since Bob does not know the location of the bits and exact bit values obtained by Alice in step 2, Bob cannot access the $\mathrm{Key_A}$ that Alice has. Also, the use of the offset F and the sum-by-bit in step 5 prevents Bob from reconstructing the key, which enhances the security. Thus, the protocol prevents Bob from learning Alice's private keys.

The second aspect is that after Bob sends the final encryption sequence M_i, only Alice can use her final key to decrypt the sequence. Since the protocol guarantees the security of Alice's final key, it also ensures that only Alice has access to the final comparison result. In practice, this control by Alice ensures that the final comparison result is protected.

5.4. IDS-ZF property

The protocols using our model have the IDS-ZF and we will illustrate this property from IDS and ZF perspectives. From the previous parameters analysis, it is clear that after dilution, the number of bits in Alice's possession can be quickly reduced to 1. Therefore, our model has IDS, which means the result is only one bit. In addition, our model has ZF. In our model, Alice always knows at least one bit for each l-bit block, because she discards those blocks she knows nothing. So, for the final key after the k N-bit keys dilutions, Alice always knows at least one bit of the final key. In summary, whether or not the original protocol has the IDS-ZF, it will have the property after using our model.

From another perspective, suppose that the protocol does not have IDS-ZF, it will cause some problems. If it does not have IDS, then Alice has more than one bit of the final key and these bits are $\{s_{a_1}, s_{a_2}, \ldots, s_{a_n}\}$ (a_i is the position of the value in the final key). If Alice uses s_{a_i} and $s_{a_{i+1}}$ to decode M_{a_i} and $M_{a_{i+1}}$ and gets results 1 and 0, respectively, then Alice can learn that $a_i \leq b < a_{i+1}$. This will leak information about Bob's private input to some extent. Besides, many QPQ protocols have a certain probability of failure without ZF, which generally leads to the probability of failure of the corresponding unidirectional QPC protocols, and it will lead to a decrease in communication efficiency and a waste of resources. However, these are not problems with our model.

5.5. Practicality

Our protocol is practical because it has many excellent properties such as loss tolerance, practicability for large numbers, no TP, and physically ease to implement. Our protocol is fully loss-tolerant for channels because Bob can recreate the l-bit random sequence and recreate the quantum state to send to Alice without any security impact. Therefore, our protocol can be used in imperfect devices and is also easy to incorporate error correction mechanisms. In addition, it can be used for large numbers. Because even if the values of a and b are large and the value of N is large, the l we use to prepare the quantum state is still a small value, which means the state is easy to prepare. Moreover, as a QPC protocol, both parties of our protocol can directly perform the task of unidirectional comparison without a TP. Besides, the transmitters and receivers we use are physically implementable, and for channels with high error rates, our protocol becomes better than the decoy-state

BB84 protocol[2] even in the asymptotic limit.[30] The physical processes involved in Fig. 1, such as the beam splitter, Circuit$_1$, and Circuit$_2$, are all easy to implement. Therefore, our protocol is physically easy to realize. In conclusion, our protocol is practical.

5.6. Comparison of UQPC and BQPC

We compare the UQPC and BQPC protocols in two subsections, in the first one we compare the frameworks of UQPC and BQPC to illustrate the security advantages of the UQPC protocol in multiple comparison scenarios, and in the second one we compare UQPC with existing BQPC protocols in terms of quantum state, efficiency, communication cost, necessity of TP, authentication, and comparison scenario. Among the existing BQPC protocols, we choose the protocols of Hou *et al.*[34], Li *et al.*[35] and Gianni *et al.*[36] as examples.

5.6.1. Comparison of UQPC and BQPC frameworks

In this subsection, we compare the frameworks of UQPC and BQPC to illustrate the security advantages of the UQPC protocol in multiple comparison scenarios.

In scenarios where a single user performs multiple comparisons with other users, the BQPC protocol poses a potential risk to the single user's privacy. For example, if Alice compares her private information with multiple users, each of whom has private values (e.g., b_1, b_2 up to b_n), the result of the protocol could reveal that Alice's value lies within a specific range (e.g., between b_1 and b_2). As the number of users increases, this range becomes narrower, potentially exposing Alice's private information completely. To avoid this privacy leakage, the protocol requires that only Alice receives the comparison results, or that the users and TP do not collude. However, such conditions increase the complexity and security demands of the BQPC protocol, making it less secure in scenarios where privacy is crucial.

In the same scenario, the UQPC protocol offers significant advantages in terms of privacy protection. With UQPC, only a single user, Alice, can access the results of the comparisons, regardless of how many users are involved. Since the comparison results are known solely to Alice, her private information a remains confidential, even as the number of users increases. The UQPC protocol does not rely on a TP for comparison results and it is more suitable for protecting private information in cases where only the single user needs to know the outcome of the comparisons. For more specific examples of UQPC and BQPC protocols, refer to Fig. 3.

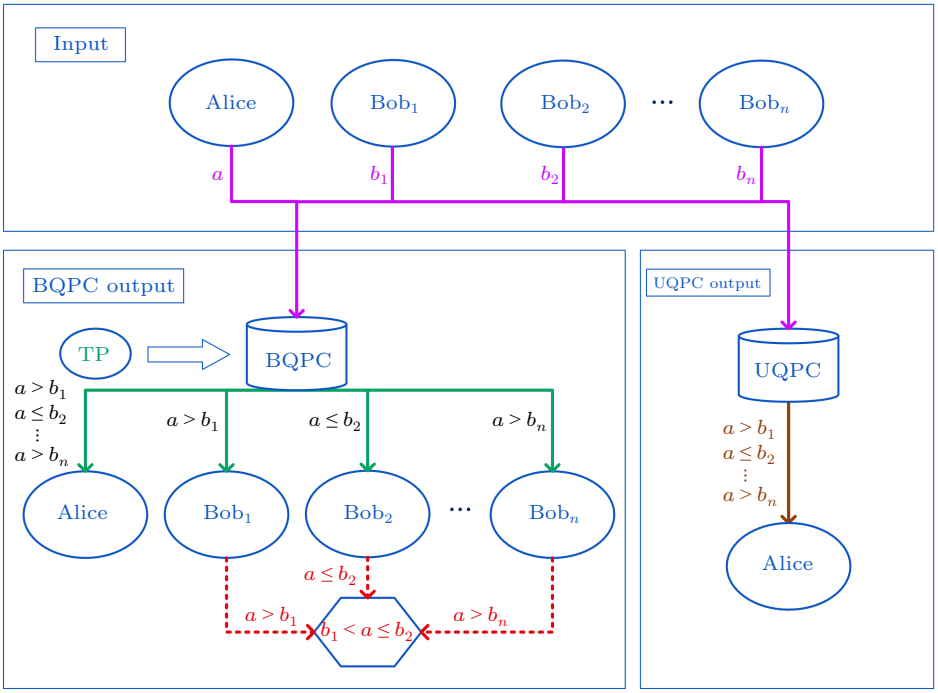


Fig. 3. In this scenario where Alice is comparing private information with Bob$_1$, Bob$_2$ to Bob$_n$, Alice's private information is a, Bob$_1$'s is b_1, Bob$_2$'s is b_2 and so on. The data inputs of the two protocols are the same, namely, a, b_1, b_2 and so on, but BQPC requires TP participation. The output of the BQPC protocol is that Alice obtains all the comparison results, while Bobs obtain their own comparison results. Unfortunately, Bobs can collude to obtain $b_1 < a \le b_2$. On the other hand, in the output of the UQPC protocol, only Alice obtains comparison results. Regardless whether Bobs collude or not, Alice's private information will not be leaked.

5.6.2. Comparison of proposed protocol and existing BQPC protocols

We compare the proposed protocol with Hou *et al.*'s,[34] Li *et al.*'s[35] and Gianni *et al.*'s[36] protocols in six aspects: quantum state, efficiency, communication cost, necessity of TP, authentication, and application scenario.

The quantum state of the proposed protocol is $\frac{1}{\sqrt{l+1}}\sum_{i=0}^{l}(-1)^{s_i}|i\rangle$, while the quantum states of Hou *et*

al.'s,[34] Li *et al.*'s,[35] and Gianni *et al.*'s[36] protocols are Bell state, GHZ-like state, and GHZ state, respectively.

The quantum efficiency is defined as $\zeta = q_s/q_t$, where q_s represents the classical bits that can be compared, and q_t denotes the total photons for one comparison.[34] The q_s of the proposed protocol is $\lceil \log_2 \max\{a,b\} \rceil$, while the q_t is $k(N+l/l) = k[(N/l)+1]$. It is worth mentioning that the symbol $\lceil \cdot \rceil$ means rounding up. Therefore, we can get $\zeta = \frac{\lceil \log_2 \max\{a,b\} \rceil}{k[(N/l)+1]}$. The efficiencies of the protocols proposed by Hou *et al.*,[34] Li *et al.*,[35] and Gianni *et al.*[36] are 50%, 66%, and 66%, respectively.

Regarding communication cost, we have $\mathcal{C} = N_q/N_c$, where N_q represents the total qubits transmitted during the communication process and N_c denotes the classical bits that can be compared. The communication cost of the proposed protocol is $\frac{k(N+l)}{l\lceil \log_2 \max\{a,b\} \rceil}$ qubits while those of the protocols of Hou *et al.*[34], Li *et al.*,[35] and Gianni *et al.*[36] are 4 qubits, 4 qubits, and 2 qubits, respectively.

In terms of necessity of TP, authentication process, and application scenarios, the TP of the proposed protocol is unnecessary, while it is necessary for the other three protocols. The proposed protocol includes an authentication process and is applied to a unidirectional comparison scenario, while the other three protocols do not include an authentication process and are applied to bidirectional comparison scenarios.

A summary is present in Table 1.

Table 1. A comparison between the proposed protocol and existing BQPC protocols.

	Proposed protocol	Ref. [34]	Ref. [35]	Ref. [36]
Quantum state	$\frac{1}{\sqrt{l+1}}\sum_{i=0}^{l}(-1)^{s_i}\|i\rangle$	Bell state	GHZ-like state	GHZ state
Efficiency	$\frac{\lceil \log_2 \max\{a,b\} \rceil}{k(\frac{N}{l}+1)}$	50%	66%	66%
Communication cost	$\frac{k(N+l)}{l\lceil \log_2 \max\{a,b\} \rceil}$ qubits	4 qubits	2 qubits	2 qubits
TP	unnecessary	necessary	necessary	necessary
Authentication	√	×	×	×
Application scenario	unidirectional comparison	bidirectional comparison	bidirectional comparison	bidirectional comparison

6. Conclusion

Because the BQPC protocols could not satisfy the special scenarios of unidirectional comparison without TP, such as authority surveys or healthcare data-sharing scenarios, we provided a new UQPC protocol with an authentication process based on the QPQ protocol.[26] Moreover, we extended the protocol and presented a general model that can transform a QPQ protocol into a secure UQPC protocol. Particularly, we took the J-protocol[21] as an example and used the general model to transform it into a UQPC protocol. Subsequently, we analyzed and concluded that the proposed protocol is correct, secure, practical, possesses the IDS-ZF property, and has advantages over the BQPC protocol in some scenarios. In summary, we proposed a UQPC protocol with an authentication process and extended it to a general model, which offers advantages over the previous BQPC protocols in some scenarios.

In further research, we will continue to improve the UQPC protocol. For example, the efficiency of the UQPC protocol can be further improved. We can refer to the idea of the block QPQ protocol[25,37–39] and convert the single-bit comparison in the final sequence into multi-bit comparison, which greatly reduces the number of bits required and makes it more efficient.

Acknowledgments

Project supported by the National Key Research and Development Program of China (Grant Nos. 2024YFB2906504 and 2024YFB2906500), the National Natural Science Foundation of China (Grant Nos. 62401067 and 62272051), and the 111 Project (Grant No. B21049).

References

[1] Yao A C 1982 23*rd annual symposium on foundations of computer science (sfcs* 1982*)* pp. 160–164
[2] Bennett C H and Brassard G 2014 *Theoretical Computer Science* **560** 7
[3] Luo M X 2024 *Quantum Networks* (Springer)
[4] Lo H K 1997 *Phys. Rev. A* **56** 1154
[5] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[6] Chen X B, Su Y, Niu X X and Yang Y X 2014 *Quantum Inf. Process.* **13** 101
[7] Lin S, Sun Y, Liu X F and Yao Z Q 2013 *Quantum Inf. Process.* **12** 559
[8] Liu W, Wang Y B and Jiang Z T 2011 *Opt. Commun.* **284** 3160
[9] Liu W, Wang Y B, Jiang Z T and Cao Y Z 2012 *International Journal of Theoretical Physics* **51** 69
[10] Tseng H Y, Lin J and Hwang T 2012 *Quantum Inf. Process.* **11** 373
[11] Fan P, Rahman A U, Ji Z, Ji X, Hao Z and Zhang H 2022 *Mod. Phys. Lett. A* **37** 2250026
[12] Gong L H, Chen Z Y, Qin L G and Huang J H 2023 *Advanced Quantum Technologies* **6** 2300097
[13] Li H H, Gong L H and Zhou N R 2020 *Chin. Phys. B* **29** 110304
[14] Gong L H, Li M L, Cao H and Wang B 2024 *Laser Physics Letters* **21** 055209

[15] Wang B, Gong L H and Liu S Q 2024 *Chin. Phys. B* **33** 110303
[16] Gong L H, Ye Z J, Liu C and Zhou S 2024 *Laser Physics Letters* **21** 035207
[17] Liu C, Zhou S, Gong L H and Chen H Y 2023 *Quantum Inf. Process.* **22** 255
[18] Giovannetti V, Lloyd S and Maccone L 2008 *Phys. Rev. Lett.* **100** 230502
[19] Olejnik L 2011 *Phys. Rev. A* **84** 022313
[20] Yu F and Qiu D 2014 *Quantum Information and Computation* **14** 91
[21] Jakobi M, Simon C, Gisin N, Bancal J D, Branciard C, Walenta N and Zbinden H 2011 *Phys. Rev. A* **83** 022301
[22] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[23] Giovannetti V, Lloyd S and Maccone L 2010 *IEEE Transactions on Information Theory* **56** 3465
[24] Gao F, Qin S, Huang W and Wen Q 2019 *Science China Physics, Mechanics & Astronomy* **62** 70301
[25] Wei C Y, Gao F, Wen Q Y and Wang T Y 2014 *Scientific Reports* **4** 7537
[26] Wei C Y, Cai X Q, Liu B, Wang T Y and Gao F 2017 *IEEE Transactions on Computers* **67** 2
[27] Sun J, Qian J, Shi C, Zhu D, Zhu Y and Jiang Y 2024 *Optical and Quantum Electronics* **56** 761
[28] Qin L, Liu B, Gao F, Huang W, Xu B and Li Y 2024 *Physica A* **633** 129427
[29] Jiao Y F, Huang W, Liu B, Shao W Z, Shen Z D and Xu B J 2024 *Quantum Inf. Process.* **23** 133
[30] Sasaki T, Yamamoto Y and Koashi M 2014 *Nature* **509** 475
[31] Liu B, Xia S, Xiao D, Huang W, Xu B and Li Y 2022 *Science China Physics, Mechanics & Astronomy* **65** 240312
[32] Liu B, Gao F, Huang W and Wen Q 2015 *Science China Physics, Mechanics & Astronomy* **58** 100301
[33] Yang Y G, Sun S J, Tian J and Xu P 2014 *Optik* **125** 5538
[34] Hou M and Wu Y 2024 *Entropy* **26** 682
[35] Li J, Che F, Wang Z and Fu A 2023 *Entropy* **25** 1552
[36] Gianni J and Qu Z 2021 *Journal of Quantum Computing* **3** 45
[37] Basak J 2023 *Quantum Inf. Process.* **22** 276
[38] Hu S, Song X and Xu A 2021 *Proceedings of the 6th International Conference on Big Data and Computing* pp. 104–108
[39] Yang Y G, Yang P Z, Xu G B, Jiang D H, Zhou Y H, Shi W M and Li D 2024 *International Journal of Theoretical Physics* **63** 180