Multi-user quantum private comparison with scattered preparation and one-way convergent transmission of quantum states

Tian-Yu Ye*, Zhao-Xu Ji

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, P.R.China
*E-mail: happyyiv@alisyun.com

Abstract: Quantum private comparison (QPC) aims to accomplish the equality comparison of the secrets from different users without disclosing their genuine contents by using the principles of quantum mechanics. In this paper, we summarize eight modes of quantum state preparation and transmission existing in current QPC protocols first. Then, by using the mode of scattered preparation and one-way convergent transmission, we construct a new multi-user quantum private comparison (MQPC) protocol with two-particle maximally entangled states, which can accomplish arbitrary pair’s comparison of equality among $\kappa$ users within one execution. Analysis turns out that its output correctness and its security against both the outside attack and the participant attack are guaranteed. The proposed MQPC protocol can be implemented with current technologies. It can be concluded that the mode of scattered preparation and one-way convergent transmission of quantum states is beneficial to designing the MQPC protocol which can accomplish arbitrary pair’s comparison of equality among $\kappa$ users within one execution.

Keywords: Multi-user quantum private comparison (MQPC); scattered preparation; one-way convergent transmission

1 Introduction

With the rapid development of quantum information processing in recent years, quantum cryptography, which was first invented by Bennett and Brassard [1] in 1984 with the concept of quantum key distribution (QKD), has attracted more and more attention. Up to date, quantum cryptography can be classified into several famous branches, such as QKD [1-8], quantum secret sharing (QSS) [9-13], quantum secure direct communication (QSDC) [14-28], quantum private query (QPQ) [29-33], etc.

Secure multi-user computation (SMC) is an interesting topic in classical cryptography. It is well known that the security of classical SMC relies on the computation complexity, which is susceptible to the powerful ability of quantum computation. In order to overcome its shortcomings on security, classical SMC has been generalized into its counterpart in the realm of quantum mechanics. Accordingly, quantum secure multi-user computation (QSMC) was derived.

As an important branch of QSMC, quantum private comparison (QPC), which was first proposed by Yang and Wen [34] in 2009 with Einstein-Podolsky-Rosen (EPR) pairs, aims to accomplish the equality comparison of the secrets from different users without disclosing their genuine contents based on the principles of quantum mechanics. However, since it is impossible to design a secure equality function in a two-party scenario [35], some additional assumptions, for example, a third party (TP), are always required in QPC. Up to now, numerous QPC protocols employing a TP [34,36-64] have been constructed with different quantum states and quantum technologies.

As far as the role of TP in QPC is concerned, there are three different models, which have been explained in detail by Zhang and Zhang [47]. (1) TP is honest. TP helps complete the protocol successfully and does not try to steal users’ secrets. In this situation, the users only need to send their private secrets to TP through one-time-pad encryption, then TP compares the decrypted secrets and announces the comparison result. However, this situation is too perfect to be practical in reality. (2) TP is dishonest. He may refuse to participate, forge intermediate computations, stop the protocol before it is normally finished, or try to obtain the users’ secrets. In this situation, the users cannot trust TP at all. This situation equals to the two-party scenario, whose insecurity has been validated by Lo in Ref.[35]. (3) TP is semi-honest, which implies two different definitions. The first one, introduced by Chen et al. [36] for the first time, is that TP executes the protocol loyally and keeps a record of all its intermediate computations and might try to steal the users’ private secrets from the record, but he cannot be corrupted by the adversary including the dishonest user. However, Yang et al. [46] first pointed out definitely that this definition is unreasonable, and the reasonable one is that TP is allowed to try to steal the users’ private secrets with any possible means but cannot be corrupted by the adversary including the dishonest user. Up to now, the second definition of a semi-honest TP has been widely accepted as the best assumption for TP in the realm of QPC.

Suppose that there are $\kappa$ users, who want to know whether their individual secret is equal to either of the other $\kappa-1$ secrets or not. If the two-user QPC protocol is used to solve this multi-user problem of equality comparison, it has to be executed with $(\kappa-1) \sim K(\kappa-1)/2$ times, which results in the reduction of
efficiency. Under this circumstance, the first multi-user quantum private comparison (MQPC) protocol was suggested by Chang et al. [51] in 2013 with \( n \)-particle GHZ class states, which can accomplish arbitrary pair’s comparison of equality among \( K \) users within one execution. Subsequently, the MQPC protocols based on multi-level quantum system [62,63] and based on the entanglement swapping of two-level Bell entangled states [64] were designed, respectively. However, up to date, the number of MQPC protocols is still few. The research on MQPC should be accelerated.

In this paper, we first investigate the modes of quantum state preparation and transmission in current MQPC protocols carefully, then utilize the mode of scattered preparation and one-way convergent transmission to design a special kind of MQPC protocol. It turns out that this mode is beneficial to designing the MQPC protocol which can accomplish arbitrary pair’s comparison of equality among \( K \) users within one execution.

The rest of this paper is structured as follows: the modes of quantum state preparation and transmission in current MQPC protocols are summarized in Sec.2; a new MQPC protocol with two-particle maximally entangled states based on the mode of scattered preparation and one-way convergent transmission and its analysis are described in Sec.3; finally, discussion and conclusion are given in Sec.4.

2 Modes of quantum state preparation and transmission in current QPC protocols

After looking into the current QPC protocols [34,36-64] in depth, without considering the eavesdropping check processes, we summarize eight modes of quantum state preparation and transmission existing in these protocols as follows, which are also depicted in Fig.1.

1. **Centralized preparation and circed transmission** (shown in Fig.1(a)). TP prepares quantum state \( |\Phi\rangle \) as the quantum carrier first. Then, he transmits partial particles of his prepared quantum state, \( |\Pi\rangle \), to the user \( P_i \). After certain quantum operation, \( P_i \) transmits \( |\Pi\rangle \) to another user \( P_j \). Finally, after certain quantum operation, \( P_j \) transmits \( |\Pi\rangle \) back to TP. In this mode, TP is the only person who prepares quantum state as the quantum carrier. Moreover, a part of particles from the prepared quantum state, \( |\Pi\rangle \), is transmitted among TP, \( P_i \) and \( P_j \) in a circed way. The protocols in Refs.[38,42,49,63] adopt this kind of quantum state preparation and transmission mode.

2. **Centralized preparation and one-way divergent transmission** (shown in Fig.1(b)). TP prepares quantum state \( |\Phi\rangle \) as the quantum carrier first. Then, he transmits two parts of particles from his prepared quantum state, \( |\Pi_i\rangle \) and \( |\Pi_j\rangle \), to the users \( P_i \) and \( P_j \), respectively. In this mode, TP is the only person who prepares quantum state as the quantum carrier. Moreover, two parts of particles, \( |\Pi_i\rangle \) and \( |\Pi_j\rangle \), are transmitted from TP to \( P_i \) and \( P_j \) in a one-way divergent way. The protocols in Refs.[36,37,40,43-47,51,54-56,58-61,63] adopt this kind of quantum state preparation and transmission mode.

3. **Centralized preparation and bidirectional divergent transmission** (shown in Fig.1(c)). TP prepares quantum state \( |\Phi\rangle \) as the quantum carrier first. Then, he transmits two parts of particles from his prepared quantum state, \( |\Pi_i\rangle \) and \( |\Pi_j\rangle \), to the users \( P_i \) and \( P_j \), respectively. Finally, after certain quantum operation, \( P_i \) and \( P_j \) transmit \( |\Pi_i\rangle \) and \( |\Pi_j\rangle \) back to TP, respectively. In this mode, TP is the only person who prepares quantum state as the quantum carrier. Moreover, \( |\Pi_i\rangle \) (\( |\Pi_j\rangle \)) is transmitted between TP and \( P_i \) (\( P_j \)) forth and back. The protocols in Refs.[34,48,62] adopt this kind of quantum state preparation and transmission mode.

4. **Scattered preparation and bidirectional transmission** (shown in Fig.1(d1&d2)). There are two cases for this mode. In the first case (shown in Fig.1(d1)), TP, \( P_i \) and \( P_j \) prepare quantum states \( |\Phi_i\rangle,|\Phi_j\rangle \) and \( |\Phi_k\rangle \) as the quantum carriers, respectively. Then, \( P_i \) (\( P_j \)) transmits partial particles of her prepared quantum state, \( |\Pi_i\rangle \) (\( |\Pi_j\rangle \)), to TP. Moreover, TP transmits two parts of particles from his prepared quantum state, \( |\Pi_j\rangle \) and \( |\Pi_k\rangle \), to \( P_i \) and \( P_j \), respectively. In this case, all of TP, \( P_i \) and \( P_j \) are the persons who prepare quantum state as the quantum carrier. Moreover, TP and \( P_i \) (\( P_j \)) send particles to each other. The protocol in Ref.[39,64] adopts this kind of quantum state preparation and transmission mode. In the second case (shown in Fig.1(d2)), \( P_i \) and \( P_j \) prepare quantum states \( |\Phi_i\rangle \) and \( |\Phi_k\rangle \) as the quantum carriers, respectively. Then, \( P_i \) (\( P_j \)) transmits partial particles of her prepared quantum state, \( |\Pi_i\rangle \) (\( |\Pi_j\rangle \)), to \( P_i \) (\( P_j \)) . In this case, both \( P_i \) and \( P_j \) are the persons who prepare quantum state as the quantum carrier. Moreover, \( P_i \) and \( P_j \) send particles to each other. The protocol in Ref.[53] adopts this kind of quantum state preparation and transmission mode.

5. **Scattered preparation and one-way convergent transmission** (shown in Fig.1(e)). \( P_i \) and \( P_j \) prepare quantum states \( |\Phi_i\rangle \) and \( |\Phi_j\rangle \) as the quantum carriers, respectively. Then, \( P_i \) (\( P_j \)) transmits partial
particles of her prepared quantum state, $|\Pi_{ij}\rangle$ ($|\Pi_{ij}\rangle$), to TP. In this mode, both $P_i$ and $P_j$ are the persons who prepare quantum state as the quantum carrier. Moreover, TP is the convergent destination of the particle transmissions from $P_i$ and $P_j$. The protocol in Ref.[41] adopts this kind of quantum state preparation and transmission mode.

(6) Scattered preparation and hybrid transmission (shown in Fig.1(f)). $P_i$ and $P_j$ prepare quantum states $|\Phi_i\rangle$ and $|\Phi_j\rangle$ as the quantum carriers, respectively. Then, $P_i$ ($P_j$) transmits partial particles of her prepared quantum state, $|\Pi_{ij}\rangle$ ($|\Pi_{ij}\rangle$), to TP. Moreover, $P_i$ ($P_j$) transmits partial particles of her prepared quantum state, $|\Pi_{ij}\rangle$ ($|\Pi_{ij}\rangle$), to $P_i$ ($P_j$). In this mode, both $P_i$ and $P_j$ are the persons who prepare quantum state as the quantum carrier. Moreover, there are both single-directional and bidirectional particle transmissions. The protocol in Ref.[50] adopts this kind of quantum state preparation and transmission mode.

(7) Scattered preparation and one-way transmission (shown in Fig.1(g)). $P_i$ and $P_j$ prepare quantum states $|\Phi_i\rangle$ and $|\Phi_j\rangle$ as the quantum carriers, respectively. Then, $P_i$ ($P_j$) transmits partial particles of her prepared quantum state, $|\Pi_{ij}\rangle$ ($|\Pi_{ij}\rangle$), to TP. Moreover, $P_i$ transmits partial particles of her prepared quantum state, $|\Pi_{ij}\rangle$ to $P_j$. In this mode, both $P_i$ and $P_j$ are the persons who prepare quantum state as the quantum carrier. Moreover, all of the particle transmissions are single-directional. The protocol in Ref.[52] adopts this kind of quantum state preparation and transmission mode.

(8) Centralized preparation and one-way transmission (shown in Fig.1(h)). $P_i$ prepares quantum state $|\Phi\rangle$ as the quantum carrier first. Then, she transmits partial particles of her prepared quantum state, $|\Pi_{ij}\rangle$, to $P_j$. In this mode, $P_i$ is the only person who prepares quantum state as the quantum carrier. Moreover, $|\Pi_{ij}\rangle$ is transmitted from $P_i$ to $P_j$ in a single-directional way. The protocols in Ref.[57] adopt this kind of quantum state preparation and transmission mode.

In the following, we will use the mode of scattered preparation and one-way convergent transmission to design a special kind of MQPC protocol. It can be found out that this mode is beneficial to designing the MQPC protocol which can accomplish arbitrary pair’s comparison of equality among $K$ users within one execution.

3 The proposed MQPC protocol
3.1 Protocol description

Assume that there are $K$ users, $P_1, P_2, \ldots, P_K$, where $P_i$ has a secret named $X^i$, $i=1,2,\ldots,K$. The binary representation of $X^i$ in $F_2$ is \(x^i_1, x^i_2, \ldots, x^i_m\), where $x^i_d \in \{0,1\}$ and $d=0,1,\ldots,m-1$. They want to know whether every two different $X$'s are equal or not under the help of a semi-honest TP. Note that throughout this paper, we adopt Yang et al.[46]'s definition of the semi-honest TP, which is regarded to be the most reasonable. Here, in order to accomplish this goal, we construct a new MQPC protocol with two-particle maximally entangled states by using the mode of scattered preparation and one-way convergent transmission.

The Bell states defined in Eq.(1) are two-particle maximally entangled states, and form a complete orthogonal basis of four-dimensional Hilbert space. Without loss of generality, we use $|\phi^+\rangle$ as the quantum carrier here. Throughout this paper, the $\sigma_z$ basis means \(|\{0\}, |\{1\}\}\).

\[
|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle).
\]  

(1)

The proposed MQPC protocol is described as follows.

**Preliminary:** $P_i$ ($i=1,2,\ldots,K$) divides her binary representation of $X^i$ into L groups, $G_{1i}, G_{2i}, \ldots, G_{Li}$, where each group contains one binary bit of $X^i$. $P_i$ and $P_j$ ($i,j=1,2,\ldots,K$ and $i \neq j$) share a common key sequence, $K_{ij}^k = \{K_{1i}^k, K_{2i}^k,\ldots,K_{Li}^k\}$, with a QKD protocol [1-8] in advance, where $K_{ij}^k \in \{0,1\}$ and $k=1,2,\ldots,L$. Note that $K_{ij}^k$ is the same to $K_{ji}^k$.

**Step 1:** $P_i$ ($i=1,2,\ldots,K$) prepares a quantum state sequence composed of $L$ $|\phi^+\rangle$, i.e.,

\[S_k = \{Q_{1i}^0, Q_{2i}^0, Q_{3i}^0, \ldots, Q_{Li}^0\}.\]

Here, the subscripts $P_{1i}, P_{Ti}$ represent two particles of each $|\phi^+\rangle$, while the superscripts $1,2,\ldots,L$ indicate the orders of $|\phi^+\rangle$ in $S_k$. Then, $P_i$ divides $S_k$ into two sequences. Concretely speaking, she picks particle $P_{Ti}$ out from each $|\phi^+\rangle$ in $S_k$ to form an ordered sequence.
$S_{\tau r}=[Q^i_{\tau r}, Q^j_{\tau r}, \ldots, Q^k_{\tau r}]'$; the remaining particles in $S_{\tau r}$ automatically compose another ordered sequence $S_{\tau r}'=[Q^i_{\tau r}, Q^j_{\tau r}, \ldots, Q^k_{\tau r}]$.

**Step 2:** $P_i (i=1,2,\ldots,K)$ prepares one set of decoy photons, $D_i$, which is randomly chosen from the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Then, $P_i$ randomly inserts $D_i$ into $S_{\tau r}$ to form a new sequence $S_{\tau r}'$. Afterward, $P_i$ sends $S_{\tau r}'$ to TP in the way of block transmission [14].

After confirming TP’s receipt of $S_{\tau r}'$, $P_i$ tells TP the positions and the preparation basis of decoy photons $D_i$. In the meanwhile, as for TP, he only needs to measure decoy photons $D_i$ in $S_{\tau r}'$ to TP in the way of $\sigma$ basis. The measurement result of $D_i$ tells TP the positions and the preparation basis of $D_i$.

**Step 3:** $P_i (i=1,2,\ldots,K)$ measures $Q_{\tau r}$ in $S_{\tau r}$ with $\sigma$ basis. The measurement result of $Q_{\tau r}$ is denoted as $M^k_{\tau r}$. If $M^k_{\tau r}$ is $|0\rangle$, then $C^1_{\tau r}$ is 0; and if $M^k_{\tau r}$ is $|1\rangle$, then $C^1_{\tau r}$ is 1. Here, $C^i_{\tau r}$ is the classical one-bit code of $M^i_{\tau r}$, and $k=1,2,\ldots,L$. Then, $P_i$ computes $R^i_{\tau r} = G^i_{\tau r} \odot C^i_{\tau r} \oplus K^i_{\tau r}$, where $j=1,2,\ldots,K$ and $i \neq j$. Finally, $P_i$ publishes $R^i_{\tau r}$ to TP, where $R^i_{\tau r} = [R^i_{\tau r1}, R^i_{\tau r2}, \ldots, R^i_{\tau rL}]$. After receiving $R^i_{\tau r}$, TP keeps a record of $R^i_{\tau r}$ on his site.

**Step 4:** TP drops out the decoy photons in $S_{\tau r}' (i=1,2,\ldots,K)$ to restore $S_{\tau r}$. Then, TP measures another ordered state of decoy photons $Q_{\tau r}'$ in $S_{\tau r}$ with $\sigma$ basis, where $k=1,2,\ldots,L$. The measurement result of $Q_{\tau r}'$ is denoted as $M^k_{\tau r}'$. TP keeps a record of $M^k_{\tau r}'$ on his site, where $M_{\tau r}' = [M^1_{\tau r}', M^2_{\tau r}', \ldots, M^L_{\tau r}']$.

**Step 5:** For $k=1,2,\ldots,L$: According to the state of $M^k_{\tau r}M^k_{\tau r}' (i,j=1,2,\ldots,K$ and $i \neq j$), TP establishes a classical one-bit code $C^k_{\tau r}$. Concretely speaking, if $M^k_{\tau r}M^k_{\tau r}' \in \{|0\rangle|0\rangle, |1\rangle|1\rangle\}$, TP sets $C^k_{\tau r} = 0$; and if $M^k_{\tau r}M^k_{\tau r}' \in \{|0\rangle|1\rangle, |1\rangle|0\rangle\}$, TP sets $C^k_{\tau r} = 1$. Then, TP computes $R^k_{\tau r} = R^k_{\tau r1} \odot R^k_{\tau r2} \oplus C^k_{\tau r}$. If $R^k_{\tau r} \neq 0$, TP concludes that $X' \neq X$ and finishes the protocol immediately; otherwise, he sets $k=k+1$ and repeats from the beginning of this Step. If he finds out that $R^k_{\tau r} = 0$ for all $k$ in the end, he will conclude that $X' = X$.

Finally, TP tells $P_i$ and $P_j$, the comparison result of $X'$ and $X$.

For clarity, the flow chart of this protocol is depicted in Fig.2, taking the comparison between $P_i$ and $P_j$ ($i,j=1,2,\ldots,K$ and $i \neq j$) for example. Apparently, each user individually prepares initial quantum states as quantum carriers and consistently transmits traveling particles to TP. It is equivalent to say that this protocol employs the mode of scattered preparation and one-way convergent transmission.

It is easy to know that within one execution, the proposed protocol can finish comparing the equality of $X'$ and $X$, where $i,j=1,2,\ldots,K$ and $i \neq j$. In other words, the proposed protocol can accomplish arbitrary pair’s comparison of equality among $K$ users within one execution. It is worthy emphasizing that in the proposed protocol, as for $P_i$, in order to judge whether her secret (i.e., $X'$) is equal to any of the other $K-1$ secrets (i.e., $X$, $j=1,2,\ldots,K$ and $j \neq i$), she only needs to prepare $S_{\tau r}$, send $S_{\tau r}$ to TP and measure $Q^i_{\tau r}$ in $S_{\tau r}$ each for one time. In the meanwhile, as for TP, he only needs to measure $Q^i_{\tau r}$ in $S_{\tau r}$ for one time. It can be concluded that the mode of scattered preparation and one-way convergent transmission is beneficial to designing the MQPC protocol which can accomplish arbitrary pair’s comparison of equality among $K$ users within one execution.

### 3.2 Analysis
We analyze the proposed protocol from the aspects concerning the output correctness and the security in this Section. The output correctness is analyzed in Subsec.3.2.1, while the security is analyzed in Subsec.3.2.2.

#### 3.2.1 Output correctness
Here, we take the comparison between $P_i$ and $P_j$ ($i,j=1,2,\ldots,K$ and $i \neq j$) for example to demonstrate the output correctness of the proposed protocol. In this situation, the relations among essential parameters $M^i_{\tau r}, C^i_{\tau r}, M^j_{\tau r}, C^j_{\tau r}, M^k_{\tau r}, C^k_{\tau r}, M^k_{\tau r}'$, $C^k_{\tau r}'$ can be summarized in Table 1. According to Table 1, we have $C^i_{\tau r} \odot C^j_{\tau r} \oplus C^k_{\tau r} = 0$. Accordingly, it follows
\[ R_i^v = R_i^v \oplus R_i^v \oplus C_i^v \]
\[ = (G_i^v \oplus C_i^v \oplus K_i^v) \oplus (G_i^v \oplus C_i^v \oplus K_i^v) \oplus C_i^v \]
\[ = (G_i^v \oplus G_i^v) \oplus (C_i^v \oplus C_i^v \oplus C_i^v) \]
\[ = G_i^v \oplus G_i^v. \]  

(2)

According to formula (2), \( R_i^v \) is the XOR value of \( G_i^v \) and \( G_i^v \). If \( R_i^v = 0 \), it follows \( G_i^v = G_i^v \); otherwise, \( G_i^v \neq G_i^v \). It can be concluded that the output of the proposed protocol is correct.

### 3.2.2 Security

Two cases of security need to be considered in this Subsection. One is the attack from an outside eavesdropper, while the other is the attack from a dishonest participant.

**i) Outside attack**

The outside attack is discussed according to each step of the proposed protocol.

In the proposed protocol, there is no any quantum transmission or classical transmission in Steps 1 and 4. As a result, an outside eavesdropper has no opportunity to launch an attack in these two steps.

In Step 2, \( P_i \) sends \( S_{ij} \) to TP. It is apparent that the decoy photon technology [65,66] is used to detect the attacks from an outside eavesdropper in this Step, such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack, etc. Actually, this kind of eavesdropping detection technology can be regarded as a variant of that in the BB84 protocol [1], whose unconditional security has been confirmed in Ref.[67]. The effectiveness of decoy photon technology has also been explicitly demonstrated in Refs.[27,28]. In addition, the proposed protocol is automatically immune to the Trojan horse attacks from an outside eavesdropper, such as the invisible photon eavesdropping attack [68] and the delay-photon Trojan horse attack [69], as its quantum transmission is in a single-directional way.

In Step 3, \( P_i \) publishes \( R_i \) to TP. An outside eavesdropper may hear \( R_i \). However, she still cannot obtain \( G_i^v \) in this Step, since \( G_i^v \) is encrypted with \( K_i^v \) and \( C_i^v \) which she has no access to.

In Step 5, TP tells \( P_i \) and \( P_j \) the comparison result of \( X^i \) and \( X^j \). An outside eavesdropper still cannot get \( X^i \) and \( X^j \) even though she receives the comparison result. It can be concluded now that the proposed protocol is immune to the outside attack.

**ii) Participant attack**

In 2007, Gao et al. [70] first pointed out that the attack from a dishonest participant, i.e., the participant attack, is generally more powerful and should be paid more attention to. Three cases of participant attack need to be considered, including the attack from one dishonest user, the collusion attack from two or more dishonest users and the attack from the semi-honest TP.

**Case 1: The attack from one dishonest user**

A dishonest user may try her best to get the other users’ secrets. During the comparison between \( X^i \) and \( X^j \) \((i, j = 1, 2, ..., K, \ i \neq j\) ), there are two situations of participant attack from one dishonest user. One is the participant attack from \( P_i \) or \( P_j \), while the other is the participant attack from \( P_t \), where \( t = 1, 2, ..., K \) and \( t \neq i, j \).

(a) **The participant attack from \( P_i \) or \( P_j \)**

During the comparison between \( X^i \) and \( X^j \) \((i, j = 1, 2, ..., K, \ i \neq j\) ), the role of \( P_i \) is similar to that of \( P_j \). Without loss of generality, suppose that \( P_i \) is the dishonest user.

Firstly, \( P_j \) may try to intercept \( S_{ij} \). \( P_i \) sends it to TP in Step 2. However, she will be caught as an outside eavesdropper since she will inevitably leave her trace, due to having no knowledge about the positions and the preparation basis of decoy photons in \( S_{ij} \). Secondly, \( P_j \) may hear \( R_i \) when \( P_j \) publishes it to TP in Step 3. However, as for \( P_i \), \( M_i \) is randomly in one of the two states \([|0\rangle, |1\rangle] \). It is equivalent to say that \( C_i^v \) is completely random to \( P_i \). Consequently, since \( R_i^v = G_i^v \oplus C_i^v \oplus K_i^v \), \( P_i \) cannot know \( G_i^v \) at all.

Thirdly, in Step 5, TP tells \( P_i \) and \( P_j \) the comparison result of \( X^i \) and \( X^j \). \( P_i \) cannot know \( G_i^v \) either.

(b) **The participant attack from \( P_t \) (\( t = 1, 2, ..., K \) and \( t \neq i, j \))**

In the proposed protocol, \( K \) users are independent from each other in the sense that they individually prepare quantum sequences and send particles to TP. During the comparison between \( X^i \) and \( X^j \) \((i, j = 1, 2, ..., K, \ i \neq j\) ), if a dishonest user \( P_t \) \((t = 1, 2, ..., K \) and \( t \neq i, j \)) launches an attack, as for \( P_i \) and \( P_j \), she will essentially act as an outside eavesdropper. According to the analysis on the outside attack in
Subsec.3.2.2, the proposed protocol can be immune to the participant attack from \( P_t \left( t = 1,2, \ldots, K \text{ and } t \neq i, j \right) \) during the comparison between \( X^i \) and \( X^j \left( i, j = 1,2, \ldots, K \text{ and } i \neq j \right) \).

**Case 2: The collusion attack from two or more dishonest users**

Two or more dishonest users may collaborate to perform the collusion attack to get the other users’ secrets. During the comparison between \( X^i \) and \( X^j \left( i, j = 1,2, \ldots, K \text{ and } i \neq j \right) \), there are two situations of this collusion attack. One is that the colluding dishonest users include \( P_i \) or \( P_j \), while the other is that the colluding dishonest users do not include \( P_i \) and \( P_j \).

(a) **The colluding dishonest users include \( P_i \) or \( P_j \)**

During the comparison between \( X^i \) and \( X^j \left( i, j = 1,2, \ldots, K \text{ and } i \neq j \right) \), the role of \( P_i \) is similar to that of \( P_j \). Without loss of generality, suppose that in this situation of collusion attack, \( P_i \) is a honest user and \( P_j \) is one of the dishonest users. Since \( K \) users are independent from each other in quantum state preparation and transmission, during the comparison between \( X^i \) and \( X^j \left( i, j = 1,2, \ldots, K \text{ and } i \neq j \right) \), each of the dishonest users excluding \( P_i \) will essentially act as an outside eavesdropper. Even though they collude together, they merely get the same amount of information to that a genuine outside eavesdropper obtains. As a result, if \( P_i \) colludes with them, the valuable information available for all colluding dishonest users is equivalent to that under the situation where only \( P_i \) is the dishonest user. According to the analysis on Case 1 of participant attack in Subsec.3.2.2, this situation of collusion attack is ineffective.

(b) **The colluding dishonest users do not include \( P_i \) and \( P_j \)**

Since \( K \) users are independent from each other in quantum state preparation and transmission, during the comparison between \( X^i \) and \( X^j \left( i, j = 1,2, \ldots, K \text{ and } i \neq j \right) \), as for \( P_i \) and \( P_j \), each of dishonest users excluding \( P_i \) and \( P_j \) will essentially act as an outside eavesdropper. Even though they collude together, they merely get the same amount of information to that a genuine outside eavesdropper obtains. According to the analysis on the outside attack in Subsec.3.2.2, they cannot obtain anything useful about \( X^i \) or \( X^j \).

**Case 3: The attack from the semi-honest TP**

The semi-honest TP may try his best to obtain users’ secrets without conspiring with either of them. In Step 3, TP gets \( R_i \) from \( P_i \). Even though TP can know \( C_{ij}^i \) from his measurement result of \( Q_{EG}^i \), he still cannot deduce \( G_{ij}^i \) from \( R_i \), since \( G_{ij}^i \) is encrypted with \( K_{ij}^i \) which he has no knowledge about.

It should be emphasized that TP knows the comparison result of \( X^i \) and \( X^j \).

4 **Discussion and conclusion**

We further compare the proposed protocol with some current representative two-party QPC protocols, such as the protocols in Refs.[34,36,38-40,44], without considering the eavesdropping check processes, as the eavesdropping check process can be regarded as a standard procedure independent from the working principle of one protocol. The comparison results are summarized in Table 2. It is apparent from Table 2 that each of these protocols relatively has advantages and disadvantages more or less. Undoubtedly, when accomplishing the equality comparison among \( K \) users, the proposed protocol exceeds the protocols of Refs.[34,36,38-40,44] in number of times of protocol execution, because arbitrary pair’s comparison of equality among \( K \) users can be achieved within one execution in the proposed protocol.

Moreover, we compare the proposed protocol with current MQPC protocols in Refs.[51,62-64] also omitting the eavesdropping check processes. The comparison results are summarized in Table 3. Here, the qubit efficiency \([12,13,21]\) is defined as \( \eta = \frac{c}{t} \), where \( c \) and \( t \) are the numbers of compared classical bits and consumed particles, respectively. Note that there are two MQPC protocols proposed in Ref.[63]: accordingly, we represent them with Ref.[63]-A and Ref.[63]-B, respectively. It is apparent from Table 3 that each of the involved protocols relatively has advantages and disadvantages more or less. For example, as the protocol of Ref.[63]-B is based on the \( d \)-level quantum system, its realization of quantum state preparation and quantum state measurement may be difficult in actual situation. Moreover, it needs unitary operation for users. Fortunately, the proposed protocol does not have these troubles, although its qubit efficiency is not the highest.

On the implementation of the proposed protocol, the technologies for preparing two-photon maximally entangled states as well as storing and measuring single photons are needed. Multi-photon entangled states have been realized in experiment, such as the two-photon entanglement [71], the four-photon entanglement [72], the six-photon entanglement [73], etc. The storage of single photons can be realized by optical delays in a fiber [16]. The measurement of single-photon can be accomplished via single-photon detector [74]. Thus, the proposed protocol can be implemented with current technologies.

In summary, in this paper, we summarize eight modes of quantum state preparation and transmission existing in current QPC protocols first. Then, by using the mode of scattered preparation and one-way convergent transmission, we construct a new MQPC protocol with two-particle maximally entangled states,
which can accomplish arbitrary pair’s comparison of equality among K users within one execution, and analyze its output correctness and its security against both the outside attack and the participant attack in detail. The proposed protocol can be implemented with current technologies. It can be concluded that the mode of scattered preparation and one-way convergent transmission of quantum states is beneficial to designing the MQPC protocol which can accomplish arbitrary pair’s comparison of equality among K users within one execution.

Acknowledgements
The authors would like to thank the anonymous reviewers for their valuable comments that help enhancing the quality of this paper. Funding by the National Natural Science Foundation of China (Grant Nos.61402407 and 11375152) is gratefully acknowledged.

Reference
[1] Bennett, C.H., Brassard, G.: Quantum cryptography: Public-key distribution and coin tossing. Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, 1984, 175-179
[2] Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys Rev Lett, 1991, 67(6):661-663
[3] Bennett, C.H., Brassard, G., Mermin, N.D.: Quantum cryptography without Bell theorem. Phys Rev Lett, 1992, 68:557-559
[4] Cabello, A.: Quantum key distribution in the Holevo limit. Phys Rev Lett, 2000, 85:5635
[5] Deng, F.G., Long, G.L.: Controlled order rearrangement encryption for quantum key distribution. Phys Rev A, 2003, 68:042315
[6] Deng, F.G., Long, G.L.: Bidirectional quantum key distribution protocol with practical faint laser pulses. Phys Rev A, 2004, 70:012311
[7] Su, X.L.: Applying Gaussian quantum discord to quantum key distribution. Chin Sci Bull, 2014, 59(11):1083-1090
[8] Zhang, C.M., Song, X.T, Treeviriyanupap, P., et al.: Delayed error verification in quantum key distribution. Chin Sci Bull, 2014, 59(23): 2825-2828
[9] Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys Rev A, 1999, 59:1829-1834
[10] Karlsson, A., Koashi, M., Imoto, N.: Quantum entanglement for secret sharing and secret splitting. Phys Rev A, 1999, 59:162-168
[11] Xiao, L., Long, G.L., Deng, F.G., Pan, J.W.: Efficient multiparty quantum-secret-sharing schemes. Phys Rev A, 2004, 69:052307
[12] Lin, J., Hwang, T.: An enhancement on Shi et al.’s multiparty quantum secret sharing protocol. Opt Commun, 2011, 284(5):1468-1471
[13] Chen, J.H., Lee, K.C., Hwang, T.: The enhancement of Zhou et al.’s quantum secret sharing protocol. Int J Mod Phy C, 2009, 20(10):1531-1535
[14] Long, G.L., Liu, X.S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002,65: 032302
[15] Bostrom, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89:187902
[16] Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68:042317
[17] Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
[18] Wang, C., Deng, F.G., Li, Y.S., Liu, X.S., Long, G.L.: Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71:044305
[19] Wang,C., Deng, F.G., Long, G.L.: Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253(1-3): 15-20
[20] Chen, X.B., Wen, Q.Y., Guo, F.Z., Sun, Y., Xu, G., Zhu, F.C.: Controlled quantum secure direct communication with W state. Int J Quant Inform, 2008, 6(4):899-906.
[21] Chong, S.K., Hwang, T.: The enhancement of three-party simultaneous quantum secure direct communication scheme with EPR pairs. Opt Commun, 2011, 284(1):515-518
[22] Liu, D., Chen, J.L., Jiang, W.: High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. Int J Theor Phys, 2012, 51:2923-2929
[23] Sun, Z.W, Du, R.G, Long, D.Y.: Quantum secure direct communication with two-photon four-qubit cluster states. Int J Theor Phys, 2012, 51:1846-1952
[24] Ren, B.C., Wei, H.R., Hua, M., Li, T., Deng, F.G.: Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems. Eur Phys J D, 2013, 67:30-37
[25] Zou, X.F., Qiu, D.W.: Three-step semi-quantum secure direct communication protocol. Sci China-Phys Mech Astron, 2014, 57(9):1696-1702
[26] Chang, Y., Xu, C.X., Zhang, S.B., et al.: Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. Chin Sci Bull, 2014, 59(21):2541-2546
[27] Chen, Y., Man, Z.X., Xia, Y.J.: Quantum bidirectional secure direct communication via entanglement swapping. Chin Phys Lett, 2007, 24(1):19
[28] Ye, T.Y., Jiang, L.Z.: Improvement of controlled bidirectional quantum direct communication using a GHZ state. Chin Phys Lett, 2013, 30(4):040305
[29] Jakobi, M., Simon, C., Gisin, N., Bancal, J.D., Branciard, C., Walenta, N., Zbinden, H.: Practical private database queries based on a quantum-key-distribution protocol. Phys Rev A, 2011, 83:022301
[30] Gao, F., Liu, B., Wen, Q.Y, et al.: Flexible quantum private queries based on quantum key distribution. Opt Express, 2012, 20:17411-17420
[31] Gao, F., Liu, B., Huang, W., Wen, Q.Y : Postprocessing of the oblivious key in quantum private query. IEEE J Sel Top Quant Electron, 2015, 21(3):6600111
[32] Liu, B., Gao, F., Huang, W., Wen, Q.Y: QKD-based quantum private query without a failure probability. Sci China-Phys Mech Astron, 2015, 58(10):100301
[33] Wei, C.Y, Wang, T.Y, Gao, F.: Practical quantum private query with better performance in resisting joint-measurement
[72] Weinfurter, H., Zukowski, M.: Four-photon entanglement from down-conversion. Phys Rev A, 2001, 64:010102
[73] Lu, C.Y., Zhou, X.Q., Gühne, O., et al.: Experimental entanglement of six photons in graph states. Nat Phys, 2007, 3:91-95
[74] You, L.X., Shen, X.F., Yang, X.Y.: Single photon response of superconducting nanowire single photon detector. Chin Sci Bull, 2010, 55:441-445
Fig. 1  The flow charts of eight modes of quantum state preparation and transmission in current QPC protocols
(a) The mode of centralized preparation and circled transmission. Here, the rectangle with solid lines denotes the quantum state preparation operation, and the solid line with an arrow denotes the quantum state transmission operation; (b) The mode of centralized preparation and one-way divergent transmission; (c) The mode of centralized preparation and bidirectional divergent transmission; (d) The mode of scattered preparation and bidirectional transmission, where d1 is the first case and d2 is the second case; (e) The mode of scattered preparation and one-way convergent transmission; (f) The mode of scattered preparation and hybrid transmission; (g) The mode of scattered preparation and one-way transmission; (h) The mode of centralized preparation and one-way transmission.

Table 1  The relations among essential parameters $M^i_k$, $C^i_k$, $M^j_k$, $C^j_k$, $M^m_k$, $C^m_k$, $C^l_k$, $C^l_k$ and $C^l_k$, and $C^l_k \oplus C^l_k \oplus C^l_k$
(taking the comparison between $P_i$ and $P_j$ ($i, j = 1, 2, \ldots, K$ and $i \neq j$) for example)

| $M^i_k$ | $C^i_k$ | $M^j_k$ | $C^j_k$ | $M^m_k$ | $C^m_k$ | $C^l_k \oplus C^l_k \oplus C^l_k$ |
|---------|---------|---------|---------|---------|---------|-------------------------------|
| $|0\rangle$ | $0$ | $0$ | $0$ | $0$ | $0$ | $0$ |
| $|0\rangle$ | $0$ | $0$ | $1$ | $1$ | $1$ | $0$ |
\[
\begin{array}{cccccccc}
| i \rangle & | 1 \rangle & | j \rangle & | 0 \rangle & | 1 \rangle & | 0 \rangle \\
| i \rangle & | 1 \rangle & | j \rangle & | 1 \rangle & | 0 \rangle & | 0 \rangle \\
\end{array}
\]

![Diagram](image)

**Fig. 2** The flow chart of the proposed MQPC protocol
(taking the comparison between \( \psi_i \) and \( \psi_j \) for example)

(a) \( \psi_i \) prepares quantum state \( Q_{0i} \) \( (Q_{0j}) \) as the quantum carrier. Here, the rectangle with solid lines denotes the quantum state preparation operation; (b) \( \psi_i \) \( (\psi_j) \) transmits particle \( Q_{0i} \) \( (Q_{0j}) \) to TP, and keeps particle \( Q_{1i} \) \( (Q_{1j}) \) intact. Here, the solid line with an arrow denotes the quantum state transmission operation; (c) \( \psi_i \) \( (\psi_j) \) measures particle \( Q_{0i} \) \( (Q_{0j}) \), computes \( R_{0i} \) \( (R_{0j}) \) and sends \( R_{0i} \) \( (R_{0j}) \) to TP. Here, the dotted rectangle, the dotted circle and the dotted line with an arrow denote the quantum state transmission operation; (d) TP measures particles \( Q_{1i} \) and \( Q_{1j} \); (e) TP computes \( R_{0i} \) and sends OR to \( P_i \) and \( P_j \). Here, OR denotes the comparison result.

| The protocol of Ref. [34] | The protocol of Ref. [36] | The protocol of Ref. [38] | The protocol of Ref. [39] | The protocol of Ref. [40] | The protocol of Ref. [44] | The proposed protocol |
|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|--------------------------|------------------------|
| Quantum state            | Bell state               | Triple GHZ state         | Single-photon state      | Single-photon state      | Bell state               | Bell state             |
| Quantum measurement for TP | Bell basis measurement  | Single-photon measurement | Bell basis measurement  | Single-photon product state | No                      | Bell state               |
| Quantum measurement for users | No                        | No                        | No                        | No                        | No                      | No                      |
| Unitary operation for TP | No                        | Yes                       | No                        | No                        | No                      | No                      |
| Unitary operation for users | Yes                       | No                        | Yes                       | No                        | No                      | No                      |
| Quantum memory for users | No                        | Yes                       | No                        | Yes                       | No                      | No                      |
| Number of times of protocol execution | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) | (\{K=1\}, \{K=2\}) |

\( K \) denotes the comparison result.
### Table 3. Comparisons of the proposed MQPC protocols and current MQPC protocols

| Quantum state | The protocol of Ref.[51] | The protocol of Ref.[62] | The protocol of Ref.[63]-A | The protocol of Ref.[63]-B | The proposed protocol |
|---------------|--------------------------|--------------------------|--------------------------|--------------------------|----------------------|
| Quantum state | n-particle GHZ class state | d-level n-particle entangled state | d-level two-particle entangled state | d-level two-particle entangled state | Bell state |
| Quantum measurement for TP | No | d-level single-photon measurement | d-level single-photon measurement | d-level two-photon collective measurement | Single-photon measurement |
| Quantum measurement for users | Single-photon measurement | No | No | No | No |
| Unitary operation for TP | No | Yes | No | No | No |
| Unitary operation for users | No | No | Yes | Yes | Yes |
| Quantum memory | No | Yes | Yes | Yes | Yes |
| Number of times of protocol execution | 1 (whether the k-th group bits from any two parties are equal or not equal) | 1 (whether the k-th group bits from K parties are all equal or not all equal) | 1 (whether the k-th group bits from K parties are all equal or not all equal) | 1 (whether the k-th group bits from any two parties are equal or not equal) | 1 (whether the k-th group bits from any two parties are equal or not equal) |
| The mode of quantum state preparation and transmission | Centralized preparation and bidirectional divergent transmission | Centralized preparation and one-way divergent transmission | Centralized preparation and one-way divergent transmission | Scattered preparation and one-way convergent transmission | Centralized preparation and one-way convergent transmission |
| Quantum technology used | The entanglement correlation among different particles from one quantum entangled state | Quantum fourier transform | Quantum phase shifting operation | The entanglement swapping of Bell states | The entanglement correlation among different particles from one quantum entangled state |
| Qubit efficiency | \( \frac{L}{L} \) | \( \frac{L}{L} \) | \( \frac{L}{L} \) | \( \frac{L}{L} \) | \( \frac{L}{L} \) |

(without considering the quantum resource used by a QKD protocol)