**Efficient semi-quantum private comparison protocol of size relation based on high dimensional Bell states**

Mao-Long Li 1, 2, Yan-Yan Liu 2, Li-Guo Qin 3, Li-Hua Gong 1, Jie-Hui Huang 3,[[1]](#footnote-1)

**Abstract:** An efficient semi-quantum private comparison protocol is proposed with Bell states to assist two classical parties in comparing the size relation of their secret information. Compared with the existing semi-quantum private comparison protocols, the devised protocol eliminates the wastage of quantum resources. After completing the comparison process, all  Bell states could be reused in other quantum task since they still retain the corresponding entanglement property, which greatly facilitates the recycle of quantum resources. The presented protocol has a higher qubit efficiency than other similar counterparts, since the legal participants can compare a two-bit privacy each time with one qubit. Moreover, the devised scheme has a greater advantage in comparing relatively larger private numbers. Besides, correctness analyses indicate that the output results of the suggested scheme are accurate. Meanwhile, security analyses demonstrate that the designed scheme is immune to both external attack and internal attack. Furthermore, the proposed semi-quantum private comparison protocol can be converted into an efficient semi-quantum key distribution protocol.

**Keywords:** Semi-quantum private comparison; Size relation;  Bell state; Recycle of quantum resource; Quantum computation

# 1. Introduction

Since Bennett and Brassard invented the first quantum cryptographic protocol, i.e., BB84 protocol [1], numerous quantum cryptographic protocols have been proposed to provide various levels of security, such as quantum key distribution (QKD) [2, 3], quantum secret sharing (QSS) [4, 5], quantum secret direct communication (QSDC) [6, 7], and quantum private comparison (QPC) [8-10]. As a crucial component of quantum secure multiparty computing (QSMC), QPC focuses on comparing participants’ privacies without divulging any relevant information. In 1982, Yao put forward the well-known millionaire problem, whose purpose is to ascertain who is richer without exposing the actual wealth of two millionaires [11]. In 2009, Yang et al. initially put forward the QPC protocol based on Bell states to settle the puzzle raised by Yao [12]. From then on, QPC has garnered significant interest and a variety of QPC protocols have been presented for various purposes. To save time and quantum resources, an efficient QPC scheme was designed based on the triplet GHZ state and single-particle measurement [13], which is weak to withstand the intercept-measure attack [14]. Lately, Chang et al. presented a QPC scheme with multi-particle GHZ states to implement the comparison of private information among multiple clients [15]. However, these protocols are restricted to determining the equality of the participants’ confidential information. Thus, to compare the size relation of participants’ privacies, Jia et al. invented a two-party QPC protocol using  entangled states [16]. Lin et al. presented a new QPC of size relationship with  Bell states to assist participants [17]. Afterwards, various QPC protocols have been put forward to judge the size relationship of participants’ privacies under ideal condition.

In the above-mentioned QPC schemes, each user is obligated to possess full quantum abilities. Nevertheless, it is extremely challenging for us to equip expensive quantum devices under current technology conditions. To alleviate the costs and lower the difficulty in implementing quantum protocols, Boyer et al. initially introduced the idea of “semi-quantum” and designed the earliest semi-quantum key distribution protocol in 2007 [18]. The semi-quantum scheme involves two types of users: quantum users and classical ones. Specifically, quantum users should possess full quantum ability, whereas classical ones only possess restricted partial quantum abilities. Since then, an increasing number of semi-quantum schemes have been presented by introducing the semi-quantum concept into other quantum cryptography applications, such as semi-quantum key distribution (SQKD) [19, 20], semi-quantum secret sharing (SQSS) [21, 22], semi-quantum secret direct communication (SQSDC) [23, 24], semi-quantum private comparison (SQPC) [25-27], etc. In 2016, the first semi-quantum private comparison (SQPC) protocol was proposed by Chou et al. based on entanglement swapping of Bell states [28]. Ye et al. successfully devised a measure-resend SQPC protocol to improve the performance of previous protocols. [29]. Absorbing the idea of semi-quantum into Sun et al.’s QPC schemes, Lang converted them into the corresponding SQPC ones [30]. However, Lin et al. indicated that [29, 30] may be vulnerable, subsequently they dwelt on a secure and efficient SQPC protocol [31]. To counteract collective noises, Gong er al. designed two QPC protocols with decoherence-free states [32]. The majority of previous SQPC protocols are limited to comparing the equality of privacies between two classical users. Thus, to compare the size relation of privacies, Zhou et al. came up with an SQPC protocol based on the  Bell states [33]. Subsequently, to enhance the qubit efficiency, Gong et al. put forward an SQPC protocol to judge the size of secrets with  GHZ states [34]. Recently, two SQPC protocols of size relationship were raised by utilizing  single particles as quantum resource [35]. When multiple users need to compare the size relation of privacies, Lian et al. came up with a pioneering multi-party QPC (MQPC) protocol with  Bell states [36].

However, in the previously mentioned SQPC protocols, quantum resources involved are disposable and cannot be recycled, leading to a significant increase in depletion of quantum resources. Inspired by this, an efficient SQPC protocol is designed based on  Bell states. With the aid of a semi-honest TP, the proposed protocol could determine the size relationship of classical participants’ privacies. Further, after completing the comparison task, these  Bell states still can be reused as initial quantum states in other SQPC protocols.

The remainder of this paper is structured as follows. Sec. 2 gives crucial preliminaries and Sec. 3 describes the whole procedure of the presented SQPC scheme. In Sec. 4, an efficient SQKD protocol is designed by extending the presented SQPC protocol. In Sec. 5, the correctness of output result is verified, and several examples are offered. The security of the devised scheme against both outside and inside attacks is analyzed in Sec. 6. The comparisons between the designed protocol and other similar counterparts are given in Sec. 7. Finally, a brief conclusion is provided in Sec. 8.

# 2. Preliminary Theory

The quantum resource utilized in the proposed SQPC is  Bell states. In a  Hilbert space, they can be denoted as [37]

 (1)

where , and  denotes the addition modulo . In addition, in a quantum system,  and  can be defined, respectively, as

 (2)

 (3)

where ;  represents quantum Fourier transform. Besides, in the presented scheme, classical participants are restricted to executing the following two operations on the received particles:

1. CTRL operation: letting the particle go back without any disturbance;
2.  operation: randomly performing a unitary operation on the received qubit.

The unitary operation executed by classical participants could be expressed as

 (4)

If Alice (Bob) executes unitary operation  on one particle of the  Bell state, the Bell state will be transformed into

 (5)

Besides, when both classical users select to perform unitary operations on the received particles, the  Bell state will be evolved into

 (6)

where  is a complete phase of  without any physical effects. Therefore, one could conclude

 (7)

# 3. Proposed semi-quantum private comparison scheme

Suppose that two classical users Alice and Bob intend to compare the size relationship of their privacies under the aid of a semi-honest user TP. The “semi-honest” means although TP can comply with the process of the protocol honestly, he can also perform any possible attack to obtain the secrets of other participants except colluding with any participant. Suppose that the confidential privacies of Alice and Bob are and , respectively, where , , , . Meanwhile, to prevent information leakage, classical participants need to pre-share a key sequence  with a secure SQKD protocol, where . As given in Fig. 1, the detailed steps of the designed SQPC scheme are outlined as follows.

图示

描述已自动生成

**Fig. 1** Framework of the proposed SQPC scheme

**Step 1:** TP prepares   Bell states in . Subsequently, the first particles of these Bell states are selected by TP to form sequence , whereas the second particles are utilized to construct sequence . Subsequently, TP sends sequence  () to Alice (Bob).

**Step 2:** When receiving the particles in  () from TP, Alice (Bob) will choose either CTRL operation or  () operation at random. Note that once Alice (Bob) selects to execute  ()on the received particles, she (he)needs to record the value of  () based on the label (), where . The specific assignment rule is  . After performing the above-mentioned operations on all particles in  (), Alice (Bob) obtains a fresh sequence  () and returns it to TP.

**Step 3:** When TP confirms that each qubit in  () has been received, he will request classical users to publish their selections in Step 2. According to the announced information, TP will carry out various functions as indicated in Table 1.

**Case 1:** If both Alice and Bob select to perform CTRL operation on the received particles at the same positions, TP will measure  and  with Bell basis to detect eavesdropping, since the presence of an eavesdropper can be determined by TP according to the measurement outcomes and the original Bell states. Once the error rate surpasses the predetermined threshold, the protocol should be terminated.

**Case 2:** If Alice (Bob) selects to execute CTRL operation and Bob (Alice) chooses to perform  () operation on particles at the same position, TP will measure  and  with Bell basis and require Bob (Alice) to promulgate  () for eavesdroppers. In this scenario, the Bell measurement results and the corresponding  () operation executed by Alice (Bob) should conform to Eq. (5). Otherwise, it means the transferred particles may be disturbed by an eavesdropper. For instance, suppose that the generated  Bell state is in  and the unitary operation implemented by Bob (Alice) is , the corresponding Bell measurement result should be  according to Eq. (5). Once the error rate is higher than the predetermined threshold, the protocol should be suspended.

**Case 3:** If Alice and Bob select to operate  and  on the received qubits at the same positions, respectively, TP will measure  and  with  Bell basis and send a “comparison” message containing these particles’ current positions to them. Meanwhile, TP establishes a new variable , whose value is obtained without any difficulty through comparing the initial Bell state  and the obtained measurement outcome .

**Step 4:** Upon receiving the “comparison” message from TP, Alice (Bob) extracts the corresponding values from   based on the positions of particles. Then Alice (Bob) will rerecord these extracted values as  and compute  . Subsequently, Alice (Bob) delivers   to TP via the established authenticated classical channel.

**Table 1** Three cases based on participants’ operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Case | Alice’s operation | Bob’s operation | TP’s operation | Function |
| Case 1 | CTRL | CTRL | Performing Bell measurement | Detecting eavesdropper |
| Case 2 | (CTRL) | CTRL() | Detecting eavesdropper |
| Case 3 |  |  | Comparison |

**Step 5:** After obtaining and , TP calculates  and then establishes another variable , where  and  represents the subtraction modulo . The relationship between  and  could be denoted as

 (8)

TP will publish  to Alice (Bob), and the size relation  of their privacies could be deduced by Alice (Bob) with .

 (9)

# 4. Semi-quantum key distribution protocol

Semi-quantum key distribution (SQKD) provides a secure way to transmit key between two classical participants with limited quantum abilities. The constructed SQPC protocol can be converted into an efficient SQKD protocol by modifying certain participants’ operations. The detailed steps are as follows.

**Step 1\* and Step 2\*:** The two steps are same as those of the above SQPC scheme, respectively.

**Step 3\*:** After receiving the particles sent by Alice and Bob, TP will perform  Bell measurement on particles and , then publish the corresponding measurement results. According to these announced results, Alice and Bob could detect eavesdroppers or obtain a raw key.

**Case 1\*:** If both Alice and Bob choose CTRL, the Bell measurement results should be identical to the initial Bell states. Once the number of errors exceeds the threshold they preset, both Alice and Bob will abort this protocol.

**Case 2\*:** Ifeither of the two users performs CTRL operation and the rest performs unitary operation, the Bell measurement result and the corresponding operation  () executed by Alice (Bob) should conform to Eq. (5). If the error rate exceeds the predefined threshold, both Alice and Bob will terminate the protocol.

**Case 3\*:** If both Alice and Bob apply unitary operations, Alice (Bob) could deduce Bob’s (Alice’s) operation by comparing the initial Bell states and the measurement results. In other words, Alice (Bob) can obtain the value of  () easily. Eventually, Alice and Bob will obtain a raw key according to the encoding rules illustrated in Table 2.

**Step 4\*:** Alice and Bob implement privacy amplification on the raw key bits to derive the final secret key.

**Table 2** Encoding rule

|  |  |  |
| --- | --- | --- |
| Comparison of  and | Comparison of  and | Code |
|  |  | 00 |
|  |  | 01 |
|  |  | 10 |
|  |  | 11 |

# 5. Performance analyses

## 5.1 Correctness

From Eq. (7),  could be easily obtained by TP. Consequently, if TP has received  and  from the participants,  can be calculated as

 (10)

As demonstrated by Eqs. (8) and (9), the output result of the proposed protocol is accurate. If  or  when , TP will derive  and . Otherwise, .

## 5.2 Examples

Several examples will be provided to further verify its correctness illustrated in Sec. 5.1. Assume that the initial  Bell state generated by TP is  and . The secret integers of Alice and Bob are 30 and 20, respectively, i.e., and . Additionally, Alice and Bob have prearranged a confidential key 12, i.e., . After Alice and Bob perform operations  and , respectively,  and  will be obtained. Meanwhile, according to the original Bell states and the corresponding measurement outcomes,  could be easily determined. In Step 4, Alice (Bob) can calculate   and deliver   to TP. Finally, based on Eqs. (8) and (9), , , and  can be drawn. To further elaborate the comparison process, Table 2 displays the values of essential parameters.

**Table 3** Relationship of parameters for several examples

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Initial state |  |  |  |  |  |  |  | Measurement result |  |  |  |  |
|  | 13 | 25 | 23 | 45 | 56 | 95 | 56 |  | 91 | 02 | 1 |  |
| 13 | 25 | 25 | 44 | 55 | 94 | 56 |  | 91 | 00 | 0 |  |
| 13 | 25 | 29 | 66 | 86 | 76 | 86 |  | 10 | 09 | −1 |  |
|  | 13 | 35 | 32 | 73 | 76 | 63 | 76 |  | 13 | 03 | 1 |  |
| 13 | 35 | 35 | 77 | 77 | 67 | 77 |  | 10 | 00 | 0 |  |
| 13 | 35 | 39 | 76 | 29 | 66 | 29 |  | 93 | 09 | −1 |  |
|  | 15 | 35 | 32 | 73 | 86 | 83 | 86 |  | 03 | 03 | 1 |  |
| 15 | 35 | 35 | 88 | 89 | 78 | 89 |  | 11 | 00 | −1 |  |
| 15 | 35 | 92 | 76 | 19 | 86 | 19 |  | 83 | 93 | 0 |  |

# 5.3 Simulation on IBM Quantum Cloud Platform

The IBM Quantum Cloud Platform is an online platform that allows users to access IBM’s prototype quantum processors over the network. Next, some operations involved in the presented scheme will be verified by simulating on the IBM Quantum Cloud Platform. Suppose that the initial quantum state prepared by TP is a  Bell state, i.e., , it can be expressed as

 (11)

As demonstrated by Eq. (11), there are 16 possible Bell states in a  Hilbert space. For the convenience of simulation, the  quantum states need to be transformed into  quantum states with the following corresponding conversion.

 (12)

Therefore, one can obtain

 (13)

Assume that the generated  Bell state is  in Step 1, the corresponding quantum circuit can be designed as shown in Fig. 2.

卡通人物

中度可信度描述已自动生成

**Fig. 2** Quantum circuit of quantum state for 

Similarly, the  Bell measurement can be represented as well and the specific process is

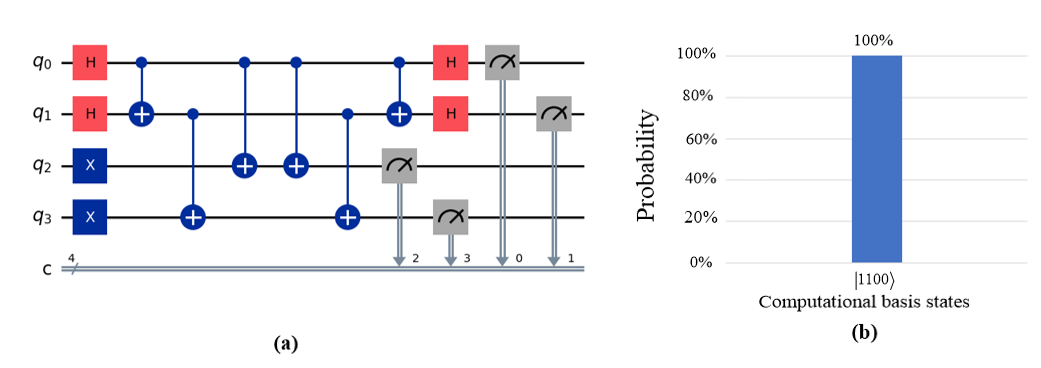
 (14)

Provided that the original Bell state generated by TP is , three different cases are simulated. In Case 1, if both Alice and Bob select CTRL operation on the received particles, the quantum circuit and the homologous measurement outcome are displayed inFig. 3. If there is no eavesdropping, the measurement result is , indicating that the outcome of Bell measurement is , as Eq. (14) shown. If either of the two users performs CTRL operation and the rest performs  operation in Case 2, the corresponding quantum circuit and the measurement outcome are depicted in Fig. 4. The final measurement result obtained by TP is  (namely ) satisfying Eq. (5). In case the two unitary operations implemented by the participants are  and , respectively, the quantum circuit is designed in Fig. 5(a) and the corresponding measurement outcome is  (namely ) as Fig. 5(b) depicted. Based on the measurement outcome and Eq. (7), Alice (Bob) can obtain   while TP can acquire , which enables TP to achieve the comparison of their privacies.

图示

描述已自动生成

**Fig. 3** Quantum circuit and measurement outcome **(a)** Quantum circuit for both CTRL operations, **(b)** measurement outcome



**Fig. 4** Quantum circuit and measurement outcome (a) Quantum circuit executing CTRL and  by Alice and Bob, respectively, (b) measurement outcome

图示, 示意图

描述已自动生成

**Fig. 5** Quantum circuit and measurement outcome (a) Quantum circuit performing  and  by Alcie and Bob, respectively, (b) measurement outcome

# 6. Security analyses

## 6.1 External attack

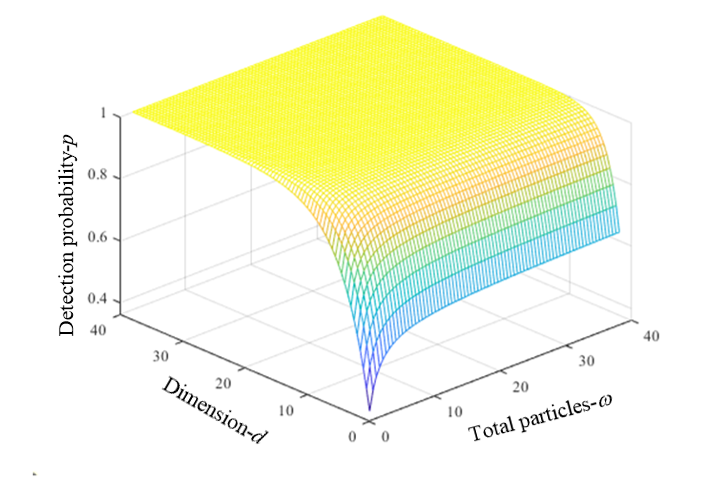
Suppose that Eve is an external eavesdropper who is eager for the private information of Alice and Bob without being noticed. To achieve her goal successfully, Eve may launch three possible attacks on the conveying qubits: the intercept-measure-resend attack, the entangle-measure attack and the modification attack.

### 6.1.1 Intercept-measure-resend attack

In the intercept-measure-resend attack, Eve could intercept and measure each particle transmitted from TP in Step 1. Subsequently, she generates fresh particles that possess identical states to the corresponding measurement results and transmits them to Alice (Bob). When Alice (Bob) returns the particles to TP in Step 2, Eve endeavors to intercept and measure them once again to obtain valuable information. However, the state of the particles will change due to Eve’s measurement operation. Hence, Eve’s illegal behavior could be perceived by TP in Step 3. Compared to the previous protocols, the detection rate of our scheme will be higher. When Alice and Bob select to perform CTRL and  ( and CTRL) operations, respectively, TP could discover Eve with a probability of . When both classical users select CTRL operation directly, the probability of discovering Eve is . Therefore, it can be inferred that the probability of evading participants’ detection is

 (15)

In other words, when one qubit is attacked, the probability of introducing error by Eve is  substantially. Thus, the total rate that Eve would be detected is , if  particles are attacked. As illustrated in Fig. 6, the probability  of detecting Eve increases as both the total number  of particles and the dimension  of Bell states increase. Besides, Fig. 6 also reveals that the probability of detecting Eve approaches 1 when both  and  increase to 4 .Therefore, it can be concluded that the suggested protocol could resist the intercept-measure-resend attack.



**Fig. 6** Eavesdropping detection probability

### 6.1.2 Entangle-measure attack

When the particles are sent from TP, Eve could attach an auxiliary particle  to the particles sent by TP and then execute unitary operation  on each particle. Then Eve will strive to acquire available information by measuring the auxiliary particle. When Eve performs unitary operation , she can derive

 (16)

 (17)

where  for ,  and  is the pure auxiliary state. Whether Alice (Bob) executes CTRL or , she (he) does not need to measure the particle sent by TP, which means that the entanglement of the entangled particle pairs in Eqs. (16) and (17) is not destroyed. Thus, to prevent these states from causing error rates, Eve is compelled to set , where . In other words, Eqs. (16) and (17) can be reexpressed as

 (18)

 (19)

Similarly, Eve must set  to avoid her actions being detected, that is to say,

 (20)

Meanwhile, when Eve executes unitary operation  on the first particle of a  Bell state, the whole quantum system will evolve into

 (21)

Recalling Eqs. (18)-(21), one can obtain

 (22)

In accordance with Eq. (22), Eve cannot distinguish the auxiliary states . That is to say, Eve is unable to access any useful information from the ancillary states. In a nutshell, one can assert that the presented protocol is able to withstand this entangle-measure attack.

### 6.1.3 Modification attack

In the modification attack, Eve may attempt to modify the contents of traveling particles to manipulate participants into obtaining incorrect comparison results without being detected. By performing unitary operation  on the transmitting particles, Eve can attain her goal of tampering with secret information. However, once Eve executes  on one particle in  Bell state, the Bell state will be transformed into

 (23)

Obviously, in Cases 1 and 2, TP will discover that the measurement outcomes deviate from the expected outcomes. For instance, suppose that both Alice and Bob select to perform CTRL operation on the received particles, and Eve launches the modification attack on the particles, TP’s measurement result will be  instead of  as expected. Therefore, the existence of Eve can be easily detected by participants. In other words, the devised protocol can thwart this modification attack.

## 6.2 Internal attack

In general, the internal attack is more menacing than the external attack [38]. In the inside attack, two types of participant attacks are considered, one is from dishonest Alice or Bob, the other is from dishonest TP.

### 6.2.1 Attack from Alice (Bob)

Without loss of generality, assume that Bob is a dishonest participant who strives to acquire the personal message of Alice. To achieve the purpose, Bob could just need to know  to figure out Alice’s privacy from . Hence, Bob could launch any possible attack strategy to derive . Nevertheless, once Bob attempts to obtain  by performing outside attack in Step 1, he will be treated as an outside attacker and his illegal behavior will result in an error rate approaching 100% in Section 6.1. In conclusion, no matter what kind of attacks Bob launched, he is unable to access Alice’s privacy without being detected. In a similar vein, it can be concluded that Alice could not dope out Bob’s privacy information either.

### 6.2.2 Attack from TP

Compared with other attacks, semi-honest TP has a higher probability of obtaining confidential information due to his dual role as both the sender and the receiver of particles. Assume that the semi-honest TP is dishonest and tries to disclose the privacies of Alice and Bob. Except for colluding with other participants, TP could employ any possible attack. In the devised protocol, the values of  and  are delivered to TP, besides he also could obtain the information from  () and  (). However, TP is still unable to extract the private information of Alice and Bob from  and  since the pre-share key  is out of his reach. Thus, TP can only conclude the size relation of  and  but can’t derive their precise values.

# 7. Comparison

The detailed comparisons among the presented protocol and those similar works in [31, 33-35] are listed in Table 4. The designed scheme, similar to the protocols in [33-35], also could judge size relation of two classical users’ privacies. On the contrary, the SQPC protocol in [31] is only capable of determining the equality of privacies. Besides, it is well known that the qubit efficiency of SQPC protocols is denoted as , where  represents the number of compared secrets, while  denotes the overall number of particles prepared by participants. In the presented scheme, to compare  privacies, TP should prepare eight  Bell states, i.e., sixteen particles, while classical users are not required to generate any qubit. Therefore, the qubit efficiency of the suggested protocol is , which could be up to  when . By contrast, in [33-35], the comparison process requires each participant to produce qubits, leading to a significant decrease in qubit efficiency.

图表, 折线图

描述已自动生成

**Fig. 7** Relationship between dimension and compared secret information

The proposed SQPC protocol exhibits a higher qubit efficiency than [31, 33-35], as shown in Table 4. Furthermore, the proposed protocol and [33-35] employ high dimensional quantum states to compare the size relation of privacies. However, when considering the same dimension, the number of compared bits varies for each particle. The proposed scheme could compare  secrets with one qubit, whereas [33-35] only could compare  privacies with one qubit. As the dimension increases, the number of compared bits in the protocol increases faster than those in other schemes, as illustrated in Fig. 7. Similarly, as dimension increases, the maximal private number that our protocol can compare is much greater than that of [33-35] as Fig. 8 shown. Consequently, if the participants intend to compare relatively larger private numbers, the proposed protocol has more significant advantages. Moreover, in [31, 33, 34], classical users need to possess the ability of measuring and preparing quantum states. In [35], although the classical users do not need to measure the qubits, they still should generate qubits. By contrast, in the proposed protocol, it is not necessary for the classical users to any particle and to measure any particle, which greatly degrades the difficult of protocol implementation.

**图表, 折线图

描述已自动生成**

**Fig. 8** Relationship between dimension and the maximal number of secret information

**Table 4** Comparison among the designed protocol and the other typical SQPC protocols

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Protocols | [31] | [33] | [34] | Protocol 1 [35] | Protocol 2 [35] | Proposed protocol |
| QR | Single photon | Bell state | GHZ state | single photon | single photon | Bell state |
| CSQPC | Equality | Size | Size | Size | Size | Size |
| NMQCU | Yes | Yes | Yes | No | No | No |
| NPQCU | Yes | Yes | Yes | Yes | Yes | No |
| RQR | No | No | No | No | No | Yes |
| QE |  |  |  |  |  |  |
| Secure | Yes | Yes | Yes | Yes | Yes | Yes |

QR (quantum resource), CSQPC (category of SQPC), NMQCU (need of measuring qubits for classical users), NPQCU (need of preparing qubits for classical users), RQR (recycle quantum resources), QE (qubit efficiency).

Furthermore, different from other typical protocols, the quantum resources can be recycled. That is to say, after fulfilling the comparison task, these  Bell states can still be utilized as initial quantum states in other quantum protocols, which greatly minimizes the consumption of quantum resources. To guarantee protocol security, all the protocols mentioned in Table 4 need pre-share secret keys between the classical participants. In the presented protocol, each participant refrains from disclosing any information about particles, including the positions and the values. This approach effectively minimizes the risk of potential information leakage.

# 8. Conclusion

An efficient semi-quantum private comparison protocol is devised with  Bell states, which could compare the size relation of two classical participants’ privacies under the control of a semi-honest TP. Different from other existing SQPC protocols, the proposed protocol ensures that the entanglement characteristic of  Bell states is not destroyed, therefore it is possible to recycle  Bell states. Meanwhile, it is not necessary for the classical parties to invoke measuring and preparing quantum states, which effectively minimizes the quantum resource wastage and substantially alleviates the demand on quantum devices. Besides, compared with existing protocols, the designed protocol has a distinct advantage in terms of qubit efficiency. By extending the devised SQPC scheme, an efficient semi-quantum key distribution scheme is designed. Furthermore, security analysis indicates that our protocol can thwart various kinds of attacks, including outside attack from attacker Eve and inside attack launched by the participants.

**Acknowledgments:** This work is supported by the National Natural Science Foundation of China (Grant No. 62161025), the Top Double 1000 Talent Programmer of Jiangxi Province (Grant No. JXSQ2019201055).

**Date availability statement:** The date that supports the fundings of this study are available within the article.

**Author Declarations:** The authors have no conflicts of interest to disclose.

**References**

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560, 7-11 (2014)
2. Zheng, X., Zhao, Z.: Quantum key distribution with two-way authentication. Opt. Quant. Electron. 53, 304 (2021)
3. Chen, G., Wang, Y., Jian, L., Zhou, Y., Liu, S.: Ternary quantum key distribution protocol based on Hadamard Gate. Int. J. Theor. Phys. 61, 26 (2022)
4. Tsai, C., Wang, C.: Efficient mediated quantum secret sharing protocol in a restricted quantum environment. Ann. Phys. 535, 2300116 (2023)
5. Khorrampanah, M., Houshmand, M.: Effectively combined multi-party quantum secret sharing and secure direct communication. Opt. Quant. Electron. 54, 213 (2022)
6. Zhang, Q., Du, M., Zhong, W., Sheng, Y., Zhou, L., Guo, G.C.: Single-photon based three-party quantum secure direct communication with identity authentication. Ann. Phys. 536, 2300407 (2024)
7. Qin, H., Sun, W., Tang, W.K.S.: Quantum secure direct communication based on single particles. Opt. Quant. Electron. 54, 508 (2022)
8. Liu, C., Zhou, S., Gong, L.H., Chen, H.Y.: Quantum private comparison protocol based on 4D GHZ-like states. Quantum Inf. Process.22, 255 (2023)
9. Lian, J.Y., Li, X., Ye, T.Y.: Multi-party quantum private comparison of size relationship with two third parties based on d-dimensional Bell states. Phys. Scr. 98, 035011 (2023)
10. Liu, C., Zhou, S., Gong, L.H., Chen, H.Y.: Quantum private comparison protocol via 4D layered states and DQC model. Quantum Inf. Process. 23, 156 (2024)
11. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), pp. 160-164 (1982)
12. Yang, Y.G., Wen, Q.Y.: An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J. Phys. A: Math. Theor. 42, 055305 (2009)
13. Chen, X.B., Xu, G., Niu, X.X., Wen, Q.Y., Yang, Y.X.: An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement. Opt. Commun. 283, 1561-1565 (2010)
14. Lin, J., Tseng, H.Y., Hwang, T.: Intercept-resend attacks on Chen et al.’s quantum private comparison protocol and the improvements. Opt. Commun. 284, 2412-2414 (2010)
15. Chang, Y.J., Tsai, C.W., Hwang, T.: Multi-user private comparison protocol using GHZ class states. Quantum Inf. Process.12, 1077-1088 (2013)
16. Jia, H.Y., Wen, Q.Y., Song, T.T., Gao, F.: Quantum protocol for millionaire problem. Opt. Commun. 284, 545-549 (2011)
17. Lin, S., Sun, Y., Liu, X.F., Yao, Z.Q.: Quantum private comparison protocol with *d*-dimensional Bell states. Quantum Inf. Process. 12, 559–568 (2013)
18. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. 99, 140501 (2007)
19. Ye, T.Y., Geng, M.J., Xu, T.J., Chen, Y.: Efficient semiquantum key distribution based on single photons in both polarization and spatial-mode degrees of freedom. Quantum Inf. Process. 21, 123 (2022)
20. Zhou, S., Xie, Q.M., Zhou, N.R.: Measurement-free mediated semi-quantum key distribution protocol based on single-particle states. Laser Phys. Lett. 21, 065207 (2024)
21. Hu, W., Zhou, R.G., Luo, J.: Semi-quantum secret sharing in high-dimensional quantum system using product states. Chinese J. Phys. 77, 1701-1712 (2022)
22. Tsai, C.W., Yang, C.W., Lee, N.Y.: Semi-quantum secret sharing protocol using W-state. Mod. Phys. Lett. A 34, 1950213 (2019)
23. Rong, Z., Qiu, D., Mateus, P., Zou, X.: Mediated semi-quantum secure direct communication. Quantum Inf. Process. 20, 58 (2021)
24. Yan, L., Sun, Y., Chang, Y., Zhang, S., Wan, G., Sheng, Z.: Semi-quantum protocol for deterministic secure quantum communication using Bell states. Quantum Inf. Process. 17, 315 (2018)
25. Gong, L.H., Li M.L., Cao, H., Wang, B.: Novel semi-quantum private comparison protocol with Bell states. Laser Phys. Lett. 21, 055209 (2024)
26. Ye, T.Y., Lian, J.Y.: A novel multi-party semiquantum private comparison protocol of size relationship with *d*-dimensional single-particle states. Physica A611, 128424 (2023)
27. Gong, L.H., Ye, Z.J., Liu, C., Zhou, S.: One-way semi-quantum private comparison protocol without pre-shared keys based on unitary operations. Laser Phys. Lett. 21, 035207 (2024)
28. Chou, W.H., Hwang, T., Gu, J.: Semi-quantum private comparison protocol under an almost-dishonest third party. arXiv preprint arXiv:1607.07961 (2016)
29. Ye, T.Y., Ye, C.Q.: Measure-resend semi-quantum private comparison without entanglement. Int. J. Theor. Phys. 57, 3819-3834 (2018)
30. Lang, Y.F.: Semi-quantum private comparison using single photons. Int. J. Theor. Phys. 57, 3048-3055 (2018)
31. Lin, P.H., Hwang, T., Tsai, C.W.: Efficient semi-quantum private comparison using photons. Quantum Inf. Process.18, 207 (2019)
32. Gong, L.H., Chen, Z.Y., Qin, L.G., Huang, J.H.: Robust multi-party semi-quantum private comparison protocols with decoherence-free states against collective noises. Adv. Quantum Tech.2300097 (2023)
33. Zhou, N.R., Xu, Q.D., Du, N.S., Gong, L.H.: Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. Quantum Inf. Process. 20,124 (2021)
34. Wang, B., Liu, S.Q. Gong, L.H.: Semi-quantum private comparison protocol of size relation with d-dimensional GHZ states. Chinese Phys. B 31, 010302 (2022)
35. Li, Y.C., Chen, Z.Y., Xu, Q.D., Gong, L.H.: Two semi-quantum private comparison protocols of size relation based on single particles. Int. J. Theor. Phys. 61, 157 (2022)
36. Lian, J.Y., Li, X., Ye, T.Y.: Multi-party semiquantum private comparison of size relationship with *d*-dimensional Bell states. EPJ Quantum Technol. 10, 10 (2023)
37. Liu, Z.H., Chen, H.W., Xu, J., Liu, W.J., Li, Z.Q.: High-dimensional deterministic multiparty quantum secret sharing without unitary operations. Quantum Inf. Process. 11, 1785-1795 (2013)
38. Gao, F., Qin, S.J., Wen, Q.Y., Zhu, F.C.: A simple participant attack on the Bradler-Dusek protocol. Quantum Inf. Comput. 7, 329-334 (2007)

1. 🖂 Jiehui Huang

   E-mail: [hkbuer@126.com](mailto:wangbing@ncu.edu.cn)

   1 School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China

   2 Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

   3 School of Mathematics, Physics and Statistics, Shanghai University of Engineering Science, Shanghai 201620, China [↑](#footnote-ref-1)