

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

Jie-Hui Huang(黄接辉), Mao-Long Li(李茂龙), Yan-Yan Liu(刘妍妍), Li-Guo Qin(秦立国), and Li-Hua Gong(龚黎华)

Citation: Chin. Phys. B, 2026, 35 (**8**): 080304. DOI: 10.1088/1674-1056/ae2abd
http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Three-party quantum key agreement with seven-particle entangled states against collective noise: IBM Qiskit implementation

She-Xiang Jiang(蒋社想) and Jin-Huan Li(李金欢)
Chin. Phys. B, 2026, 35 (**7**): 070307. DOI: 10.1088/1674-1056/ae53b6

Verifiable quantum secret sharing scheme based on orthogonal product states

Chen-Ming Bai(白晨明), Lu Liu(刘璐), and Sujuan Zhang(张素娟)
Chin. Phys. B, 2024, 33 (**7**): 070302. DOI: 10.1088/1674-1056/ad342a

Efficient semi-quantum secret sharing protocol using single particles

Ding Xing(邢丁), Yifei Wang(王艺霏), Zhao Dou(窦钊), Jian Li(李剑),Xiubo Chen(陈秀波), and Lixiang Li(李丽香)
Chin. Phys. B, 2023, 32 (**7**): 070308. DOI: 10.1088/1674-1056/ace159

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦), Yan Chang(昌燕), Wen Cheng(程稳), Min Hou(侯敏), and Shi-Bin Zhang(张仕斌)
Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103

New semi-quantum key agreement protocol based on high-dimensional single-particle states

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), and Nan-Run Zhou(周南润)
Chin. Phys. B, 2020, 29 (**11**): 110304. DOI: 10.1088/1674-1056/abaedd

---

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

Jie-Hui Huang(黄接辉)[1], Mao-Long Li(李茂龙)[2,3], Yan-Yan Liu(刘妍妍)[3], Li-Guo Qin(秦立国)[1], and Li-Hua Gong(龚黎华)[2,†]

[1] *School of Mathematics, Physics and Statistics, Shanghai University of Engineering Science, Shanghai* 201620, *China*
[2] *School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai* 201620, *China*
[3] *Department of Electronic Information Engineering, Nanchang University, Nanchang* 330031, *China*

(Received 20 September 2025; revised manuscript received 8 December 2025; accepted manuscript online 10 December 2025)

An efficient semi-quantum private comparison protocol is proposed with d-dimensional Bell states to assist two classical parties in comparing the size relation of their secret information. With the assistance of a third party (TP), Alice and Bob do not need to measure qubits or prepare new qubits, reducing the consumption of quantum resources. The presented protocol has a higher qubit efficiency than other similar protocols, since the legal participants can compare two bits of privacy (i.e., secret information unknown to others) each time with one qubit. Moreover, the proposed scheme offers a greater advantage when comparing larger private numbers, with the correctness of its outputs verified through analytical methods. Simulation experiments further verified the correctness of the proposed protocol, and security analyses demonstrated its robustness against external and internal attacks. Furthermore, the proposed semi-quantum private comparison protocol can be converted into an efficient semi-quantum key distribution protocol.

Keywords: quantum cryptography, semi-quantum private comparison, size relation, recycle of quantum resource

PACS: 03.67.Dd, 03.67.Ac, 03.67.Hk, 03.67.–a

DOI: 10.1088/1674-1056/ae2abd **CSTR:** 32038.14.CPB.ae2abd

1. Introduction

Since Bennett and Brassard invented the first quantum cryptographic protocol, i.e., the 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] and quantum private comparison (QPC).[6–8] As a crucial component of quantum secure multiparty computing (QSMC), QPC focuses on comparing participants' privacies without divulging any relevant information. In 1982, Yao introduced the well-known millionaire problem, whose purpose is to ascertain who is richer without exposing the actual wealth of two millionaires.[9] For example, quantum protocols can be employed in banking and finance to protect customer transaction records and account information from disclosure. To address this challenge, Yang *et al.* initially put forward the QPC protocol based on Bell states to settle the puzzle raised by Yao.[10] 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.[11] To withstand the intercept-measure attack in Ref. [12], Liu *et al.*[13] and Tseng *et al.*[14] presented two QPC protocols employing single photons and EPR pairs, respectively. Wang *et al.* implemented a QPC protocol based on one-direction quantum walks by introducing a semi-honest third-party marker to determine the comparison result with improved qubit efficiency.[15] Kou *et al.* designed a QPC protocol that achieves 100% qubit efficiency, employing homomorphic rotation encryption and circular transmission mode.[16]

Based on the unique characteristics of Bell states, Hou *et al.* presented a novel and secure QPC protocol.[17] Afterwards, various QPC protocols have been put forward to judge the size relationship of participants' privacies under ideal conditions.

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 the current technological 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 environment comprises two user types: the quantum users and the classical ones. Specifically, the quantum users possess full quantum ability, whereas the classical ones only possess restricted quantum abilities. Since then, an increasing number of semi-quantum schemes have been introduced by applying the semi-quantum concept to other quantum cryptography applications, such as semi-quantum key distribution

[†]Corresponding author. E-mail: lhgong@sues.edu.cn

© 2026 Chinese Physical Society and IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved.

(SQKD),[19,20] semi-quantum secret sharing (SQSS),[21–23] semi-quantum secret direct communication (SQSDC),[24,25] semi-quantum private comparison (SQPC),[26–28] etc. In 2016, the first semi-quantum private comparison (SQPC) protocol was proposed by Chou *et al.* based on entanglement swapping of Bell states.[29] Ye *et al.* successfully devised a measure-resend SQPC protocol to improve the performance of previous protocols.[30] Absorbing the conception of semi-quantum, Lang converted Sun *et al.*'s QPC schemes into the corresponding SQPC ones.[31] However, Lin *et al.* indicated that the protocols in Ref. [30,31] may be vulnerable, subsequently they dwelt on a secure and efficient SQPC protocol.[32] To counteract the collective noises, Gong *et al.* designed two SQPC protocols with the decoherence-free states.[33] Utilizing a method of combining two classes of W states and identifying the provenance of quantum states, Li *et al.* pioneered an efficient SQPC protocol.[34] Besides, Tian *et al.* put forward a more efficient and secure SQPC protocol based on W state.[35] Most prior SQPC protocols only support equality comparison between two classical users. Thus, to determine the size relation of the participants' privacies, Zhou *et al.* came up with an SQPC protocol based on the d-level Bell states.[36] Subsequently, to enhance the qubit efficiency, Gong *et al.* put forward an SQPC protocol to judge the size of secrets with d-level GHZ states.[37] Recently, two SQPC protocols of size relationship were raised by considering d-dimensional single particles as quantum resource.[38] Wang *et al.* introduced a new SQPC protocol to compare the participants' privacies by leveraging two-dimensional Bell states.[39] Hu *et al.* introduced three efficient multi-party SQPC schemes that address collective dephasing, rotation and amplitude damping noise, respectively.[40] Kong *et al.* innovatively presented a multi-party SQPC protocol, which can be further enhanced by integrating machine learning for noise recognition to strengthen security verification.[41]

However, the quantum resources in the aforementioned SQPC protocols are single-use, leading to significant resource depletion. Inspired by this, an efficient SQPC protocol is designed based on the d-dimensional 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 d-dimensional Bell states still can be reused as initial quantum states in other SQPC protocols.

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

2. Preliminary theory

The quantum resource utilized in the proposed SQPC is the d-dimensional Bell states. In a d-dimensional Hilbert space, they can be denoted as[38]

$$|\phi_{u,v}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} ju}{d}} |j\rangle_{\mathrm{A}} |j \oplus v\rangle_{\mathrm{B}}, \tag{1}$$

where $u, v \in \{0, 1, \ldots, d-1\}$, and $\oplus$ denotes the addition modulo d. In addition, in a d-dimensional quantum system, Z-basis and X-basis can be defined, respectively, as

$$\overline{Z} = \{ |k\rangle | k = 0, 1, \ldots, d-1 \}, \tag{2}$$

$$\overline{X} = \{ F|k\rangle | k = 0, 1, \ldots, d-1 \}, \tag{3}$$

where $F|k\rangle = |F_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} jk}{d}} |j\rangle$, $j = 0, 1, \ldots, d-1$; F represents quantum Fourier transform. Using the semi-quantum environment shown in Ref. [42], classical participants are restricted to executing the following two operations on the received particles in the presented scheme:

(a) CTRL operation: letting the particle go back without any disturbance;

(b) U_{nm} operation: randomly performing a unitary operation on the received qubit.

The unitary operation executed by classical participants could be expressed as

$$U_{nm} = \sum_{j=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} jn}{d}} |j\rangle \langle (j+m) \bmod d|, \quad n = 0, 1, \ldots, d-1. \tag{4}$$

If Alice (Bob) executes unitary operation U_{nm} on one particle of the d-dimensional Bell state $|\phi_{u,v}\rangle$, the Bell state will be transformed into

$$\begin{aligned} U_{nm} |\phi_{u,v}\rangle &= \sum_{r=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} rn}{d}} |r\rangle \langle (r+m) \bmod d| \\ &\quad \otimes \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} ju}{d}} |j\rangle_{\mathrm{A\,B}} \langle (j+v) \bmod d| \\ &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} j(u+n)}{d}} |j\rangle_{\mathrm{A\,B}} \langle (j+v-m) \bmod d| \\ &= |\phi_{u+n,v+m}\rangle . \end{aligned} \tag{5}$$

Besides, when both classical users select to perform unitary operations on the received particles, the d-dimensional Bell state $|\phi_{u,v}\rangle$ will be evolved into

$$\begin{aligned} &\left(U_{kl}^{\mathrm{A}} \otimes U_{k'l'}^{\mathrm{B}}\right) |\phi_{u,v}\rangle \\ &= \left\{ \left[\sum_{r=0}^{d-1} \mathrm{e}^{\frac{2\pi \mathrm{i} rk}{d}} |(r+l) \bmod d\rangle_{\mathrm{A}} \langle r| \right] \right. \end{aligned}$$

$$
\begin{aligned}
&\otimes\left[\sum_{r'=0}^{d-1}\mathrm{e}^{\frac{2\pi \mathrm{i} r'k'}{d}}\left|\left(r+l'\right) \bmod d\right\rangle_{\mathrm{B}}\langle r|\right]\Bigg\} \\
&\times\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{\frac{2\pi \mathrm{i} ju}{d}}|j\rangle_{\mathrm{A}\,\mathrm{B}}\langle(j+v) \bmod d| \\
=&\ \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{\frac{2\pi \mathrm{i} ju}{d}}|(j+l) \bmod d\rangle_{\mathrm{A}\,\mathrm{B}}\left\langle\left(j+l'\right) \bmod d\right| \\
=&\ \mathrm{e}^{-\frac{2\pi \mathrm{i} l(k+k')}{d}}\frac{1}{\sqrt{d}}\sum_{r=0}^{d-1}\mathrm{e}^{\frac{2\pi \mathrm{i} ru(k+k')}{d}} \\
&\times|r\rangle_{\mathrm{A}\,\mathrm{B}}\left\langle\left(r+v+l'-l\right) \bmod d\right| \\
=&\ M\left|\phi_{u+k+k',v+l-l'}\right\rangle, \qquad (6)
\end{aligned}
$$

where $M=\exp[-\frac{2\pi \mathrm{i} l(k+k')}{d}]$ is a complete phase of $\left|\phi_{u+k'+k,v+l'-l}\right\rangle$ without any physical effects. Therefore, one could conclude that

$$
\left(U_{kl}^{\mathrm{A}}\otimes U_{k'l'}^{\mathrm{B}}\right)|\phi_{u,v}\rangle_{\mathrm{AB}}=\left|\phi_{u+k'+k,v+l'-l}\right\rangle_{\mathrm{AB}}. \qquad (7)
$$

3. Proposed semi-quantum private comparison scheme

Suppose that two classical users Alice and Bob intend to compare the size relationship of their secrets under the aid of a semi-honest third party. 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 secrets of Alice and Bob are X and Y, respectively, where $X=(x_0,x_1,\ldots,x_{N-1})$, $Y=(y_0,y_1,\ldots,y_{N-1})$, Here $x_i,y_i\in\{00,01,\ldots,(h-1)(h-1)\}$, $i=0,1,\ldots,N-1$, $h=\frac{1}{2}(d+1)$. To prevent information leakage, classical participants need to pre-share a key sequence $k_{ab}=\left(k_{ab}^0,k_{ab}^1,\ldots,k_{ab}^{N-1}\right)$ with a secure SQKD protocol, where $k_{ab}^i\in\{00,01,\ldots,(h-1)(h-1)\}$. As given in Fig. 1, the detailed steps of the designed SQPC scheme are outlined as follows.

Step 1: TP prepares $4N$ d-dimensional Bell states in $|\phi_{u,v}\rangle$. Subsequently, the first particles of these Bell states are selected by TP to form sequence S_{A}, whereas the second particles are utilized to construct sequence S_{B}. Subsequently, TP sends sequence S_{A} (S_{B}) to Alice (Bob).

Step 2: When receiving the particles in S_{A} (S_{B}) from TP, Alice and Bob independently and randomly choose to apply either the CTRL operation or U_{kl}^{A} ($U_{k'l'}^{\mathrm{B}}$) operation. Note that once Alice (Bob) decides to execute U_{kl}^{A} ($U_{k'l'}^{\mathrm{B}}$) on the received particles, she (he) needs to record the value of R_a (R_b) based on the label kl ($k'l'$), where $R_a=\{r_{a_1}^j r_{a_2}^j\,|j=0,1,\ldots,2N-1\}$ ($R_b=\{r_{b_1}^j r_{b_2}^j\,|j=0,1,\ldots,2N-1\}$). The specific assignment rule is $R_a^j=r_{a_1}^j r_{a_2}^j=(d-k)\,l$ ($R_b^j=r_{b_1}^j r_{b_2}^j=k'l'$). After performing the above-mentioned operations on all particles in S_{A} (S_{B}), Alice (Bob) obtains and returns a fresh sequence S'_{A} (S'_{B}) to TP.

Step 3: When TP confirms that each qubit in S'_{A} (S'_{B}) has been received, he will request classical users to announce their selections in Step 2. According to the announced information, TP then carries out the respective functions as delineated in Table 1.

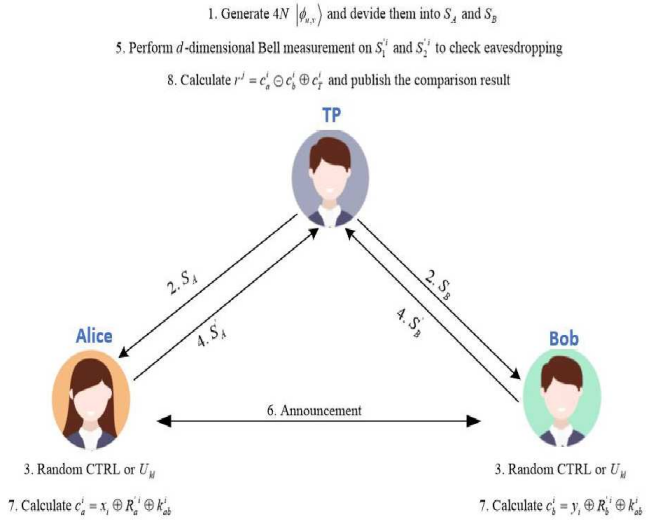


Fig. 1. Framework of the proposed SQPC scheme.

Table 1. Three cases based on participants' operations.

Case	Alice's operation	Bob's operation	TP's operation	Function
Case 1	CTRL	CTRL	d-dimensional Bell measurement	Checking eavesdropping
Case 2	U_{kl}^{A} (CTRL)	CTRL ($U_{k'l'}^{\mathrm{B}}$)		Checking eavesdropping
Case 3	U_{kl}^{A}	$U_{k'l'}^{\mathrm{B}}$		Comparison

Case 1: If both Alice and Bob select to perform CTRL operation on the received particles at the same positions, TP will measure S'_{A} and S'_{B} with d-dimensional 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 U_{kl}^{B} ($U_{k'l'}^{\mathrm{A}}$) operation on particles at the same position, TP will measure S'_{A} and S'_{B} with the d-dimensional Bell basis and require Bob (Alice) to promulgate U_{kl}^{A} ($U_{k'l'}^{\mathrm{B}}$) for eavesdroppers. In this scenario, the Bell measurement results and the corresponding U_{kl}^{A} ($U_{k'l'}^{\mathrm{B}}$) 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 d-dimensional Bell state is in $|\phi_{0,0}\rangle$ and the unitary operation implemented by Bob (Alice) is $U_{2,2}$, the corresponding measurement result should be $|\phi_{2,2}\rangle$ 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 U_{kl}^{A} and $U_{k'l'}^{\mathrm{B}}$ on the received particles at the same positions, respectively, TP will measure S'_{A} and S'_{B} with the d-dimensional Bell basis and send a "comparison" message containing these particles' current positions to Alice and Bob. Meanwhile, TP establishes a new variable $c_{\mathrm{T}}^{i} = (k'+k)(l'-l)$, whose value is obtained without any difficulty in comparing the initial Bell state $|\phi_{u,v}\rangle$ with the obtained measurement outcome $|\phi_{u+k'+k,v+l'-l}\rangle$.

Step 4: Upon receiving the "comparison" message from TP, Alice (Bob) extracts the corresponding values from R_a (R_b) based on the provided particle position indices. Then Alice (Bob) will rerecord these extracted values as $R'_a = \{r'^{i}_{a_1} r'^{i}_{a_2} | i = 0,1,\ldots,N-1\}$ $(R'_b = \{r'^{i}_{b_1} r'^{i}_{b_2} | i = 0,1,\ldots,N-1\})$ and compute $c_a^i = x_i \oplus R'^{i}_a \oplus k^i_{ab}$ $\left(c_b^i = y_i \oplus R'^{i}_b \oplus k^i_{ab}\right)$. Subsequently, Alice (Bob) delivers c_a^i $\left(c_b^i\right)$ to TP via the established authenticated classical channel.

Step 5: After obtaining c_a^i and c_b^i, TP calculates $r^i = c_a^i \ominus c_b^i \oplus c_{\mathrm{T}}^i$ and then establishes another variable c_r^i, where $r^i = \{r_1^1 r_2^1, r_1^2 r_2^2, \ldots, r_1^{N-1} r_2^{N-1}\}$ and $\ominus$ represents the subtraction modulo d. The relationship between c_r^i and $r_1^i r_2^i$ could be denoted as

$$c_r^i = \begin{cases} -1, & (h-1)(h-1) < r_1^i r_2^i \le (2h-2)(2h-2); \\ 0, & r_1^i r_2^i = 00; \\ 1, & 00 < r_1^i r_2^i \le (h-1)(h-1). \end{cases} \tag{8}$$

TP will publish c_r^i to Alice (Bob), and the size relation $f(x_i, y_i)$ of their privacies could be deduced by Alice (Bob) with c_r^i.

$$f(x_i, y_i) = \begin{cases} x_i < y_i, & c_r^i = -1; \\ x_i = y_i, & c_r^i = 0; \\ x_i > y_i, & c_r^i = 1. \end{cases} \tag{9}$$

4. Semi-quantum key distribution protocol

Semi-quantum key distribution (SQKD) provides a secure way to transmit keys between two classical participants with limited quantum abilities. Building upon this concept, the constructed SQPC protocol can be converted into an efficient SQKD protocol by modifying certain participants' operations, with the detailed steps outlined 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 the d-dimensional Bell measurement on particles S'_{A} and S'_{B}, then publish the corresponding measurement results. According to these results, Alice and Bob could detect eavesdroppers or obtain a raw key.

Case 1*: In the case that both Alice and Bob choose the CTRL operation, 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*: If either of the two users performs CTRL operation and the rest performs unitary operation, the Bell measurement result and the corresponding operation U_{kl}^{A} $(U_{k'l'}^{\mathrm{B}})$ executed by Alice (Bob) should conform to Eq. (5). The protocol will be terminated by both parties if the error rate exceeds the predefined threshold.

Case 3*: If both Alice and Bob apply unitary operations, each can deduce the other's operation by comparing the initial Bell states with the final measurement results, thereby easily obtaining the value of $k'l'$ (kl). Eventually, Alice and Bob will obtain a raw key according to the encoding rules illustrated in Table 2.

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

Table 2. Encoding rule.

Comparison of k and k'	Comparison of l and l'	Code
$k = k'$	$l = l'$	00
$k = k'$	$l \neq l'$	01
$k \neq k'$	$l = l'$	10
$k \neq k'$	$l \neq l'$	11

4.1. Correctness

From Eq. (7), $R'^{i}_a \ominus R'^{i}_b \oplus c_{\mathrm{T}}^i = (d-k)\,l \ominus k', l' \oplus (k'+k)(l'-l) = 00$ could be easily obtained by TP. Consequently, if TP has received c_a^i and c_b^i from the participants, r^i can be calculated as

$$\begin{aligned} r^i &= c_a^i \ominus c_b^i \oplus c_{\mathrm{T}}^i \\ &= \left(x_i \oplus R'^{i}_a \oplus k^i_{ab}\right) \ominus \left(y_i \oplus R'^{i}_b \oplus k^i_{ab}\right) \oplus c_{\mathrm{T}}^i \\ &= R'^{i}_a \ominus R'^{i}_b \oplus c_{\mathrm{T}}^i \oplus x_i \ominus y_i \\ &= x_i \ominus y_i. \end{aligned} \tag{10}$$

Namely, $r_1^i r_2^i = x_1^i x_2^i \ominus y_1^i y_2^i$.

If $r_1^i r_2^i = 00$, then $x_1^i x_2^i = y_1^i y_2^i$, i.e., $x_i = y_i$. If $00 < r_1^i r_2^i \le (h-1)(h-1)$, then $x_1^i x_2^i > y_1^i y_2^i$, i.e., $x_i > y_i$. If $(h-1)(h-1) < r_1^i r_2^i \le (2h-2)(2h-2)$, then $x_1^i x_2^i < y_1^i y_2^i$, i.e., $x_i < y_i$. Based on the above analysis, it is clear that Eqs. (8) and (9) are correct. Thus, the output result of the proposed protocol is accurate.

4.2. Examples

Several examples will be provided to further verify its correctness illustrated in Subsection 5.1. Assume that the initial d-dimensional Bell state generated by TP is $|\phi_{0,0}\rangle$ and $d = 13$. The secret integers of Alice and Bob are 30 and 20, respectively, i.e., $x_i = 30$ and $y_i = 20$. Additionally, Alice and Bob have prearranged a confidential key 12, that is to say, $k^i_{ab} = 12$. After Alice and Bob perform operations U_{45} and U_{56},

respectively, $R_a'^i = 95$ and $R_b'^i = 56$ will be obtained. Meanwhile, according to the initial Bell states and the corresponding measurement outcomes, $c_{\mathrm{T}}^i = 91$ could be easily determined. In Step 4, Alice (Bob) can calculate $c_a^i = 30 \oplus 95 \oplus 12 = 07$ $\left(c_b^i = 20 \oplus 56 \oplus 12 = 88\right)$ and deliver c_a^i $\left(c_b^i\right)$ to TP. Finally, based on Eqs. (8) and (9), $r^i = 07 \ominus 88 \oplus 91 = 10$, $c_r^i = 1$, and $x_i > y_i$ can be drawn. To further illustrate the comparison process, Table 2 displays the values of essential parameters.

Table 3. Relationship of parameters for several examples.

Initial state	d	x_i	y_i	U_{kl}^{A}	$U_{k'l'}^{\mathrm{B}}$	$R_a'^i$	$R_b'^i$	Measurement result	c_{T}^i	r^i	c_r^i	$f(x_i, y_i)$
$\|\phi_{1,3}\rangle$	13	25	23	45	56	95	56	$\|\phi_{10,4}\rangle$	91	02	1	$x_i > y_i$
	13	25	25	44	55	94	56	$\|\phi_{10,4}\rangle$	91	00	0	$x_i = y_i$
	13	25	29	66	86	76	86	$\|\phi_{2,3}\rangle$	10	09	−1	$x_i < y_i$
$\|\phi_{3,5}\rangle$	13	35	32	73	76	63	76	$\|\phi_{4,8}\rangle$	13	03	1	$x_i > y_i$
	13	35	35	77	77	67	77	$\|\phi_{4,5}\rangle$	10	00	0	$x_i = y_i$
	13	35	39	76	29	66	29	$\|\phi_{12,8}\rangle$	93	09	−1	$x_i < y_i$
$\|\phi_{3,5}\rangle$	15	35	32	73	86	83	86	$\|\phi_{3,8}\rangle$	03	03	1	$x_i > y_i$
	15	35	35	88	89	78	89	$\|\phi_{4,5}\rangle$	11	00	−1	$x_i = y_i$
	15	35	92	76	19	86	19	$\|\phi_{11,8}\rangle$	83	93	−1	$x_i < y_i$

5. Simulation on IBM quantum cloud platform

The IBM Quantum Cloud Platform provides an online, ideal simulation environment remotely accessible to IBM's prototype quantum processors. Next, under idealized conditions, 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 four-dimensional Bell state, in other words, $d = 4$, it can be expressed as

$$|\phi_{u.v}\rangle = \frac{1}{2}\sum_{j=0}^{3} \mathrm{e}^{\frac{\pi \mathrm{i} ju}{2}} |j\rangle |j \oplus v\rangle . \tag{11}$$

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

$$\begin{aligned}
&|00\rangle \to |0000\rangle , \quad |01\rangle \to |0001\rangle , \quad |02\rangle \to |0010\rangle , \\
&|03\rangle \to |0011\rangle , \quad |10\rangle \to |0100\rangle , \quad |11\rangle \to |0101\rangle , \\
&|12\rangle \to |0110\rangle , \quad |13\rangle \to |0111\rangle , \quad |20\rangle \to |1000\rangle , \\
&|21\rangle \to |1001\rangle , \quad |22\rangle \to |1010\rangle , \quad |23\rangle \to |1011\rangle , \\
&|30\rangle \to |1100\rangle , \quad |31\rangle \to |1101\rangle , \quad |32\rangle \to |1110\rangle , \\
&|33\rangle \to |1111\rangle .
\end{aligned} \tag{12}$$

Therefore, one can obtain

$$|\phi_{0,0}\rangle = \frac{1}{2}\left(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right). \tag{13}$$

Assume that the generated four-dimensional Bell state is $|\phi_{0,0}\rangle$ in Step 1, the corresponding quantum circuit can be designed as shown in Fig. 2.

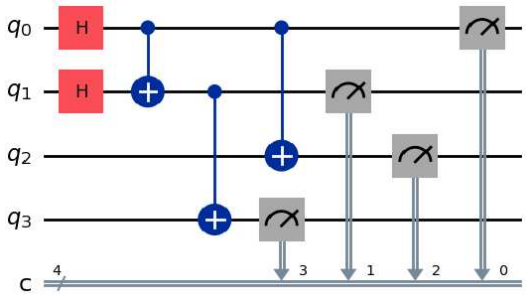


Fig. 2. Quantum circuit of quantum state for $|\phi_{0,0}\rangle$.

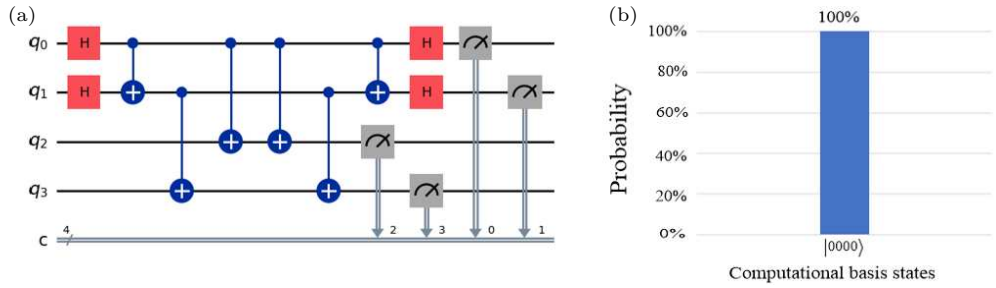


Fig. 3. Quantum circuit and measurement outcome. (a) Quantum circuit for both CTRL operations, (b) measurement outcome.

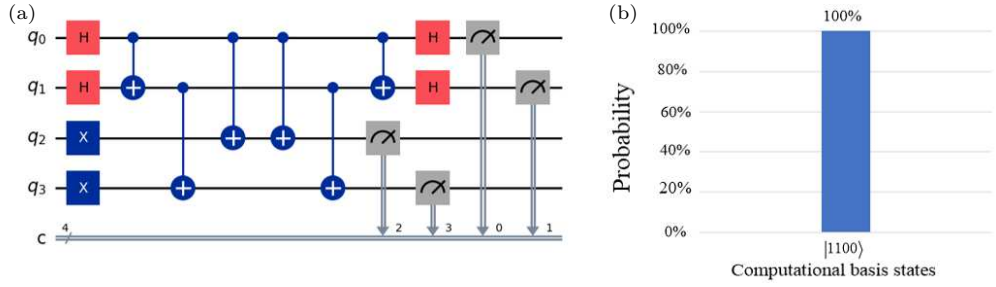


Fig. 4. Quantum circuit and measurement outcome. (a) Quantum circuit executing CTRL and U_{30} by Alice and Bob, respectively, (b) measurement outcome.

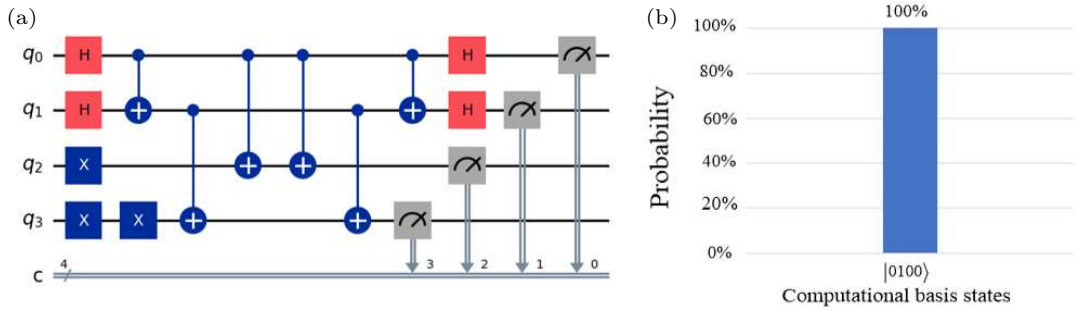


Fig. 5. Quantum circuit and measurement outcome. (a) Quantum circuit performing U_{30} and U_{20} by Alice and Bob, respectively, (b) measurement outcome.

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

$$\begin{aligned}
&|\phi_{0,0}\rangle \to |0000\rangle, \quad |\phi_{0,1}\rangle \to |0001\rangle, \quad |\phi_{0,2}\rangle \to |0010\rangle,\\
&|\phi_{0,3}\rangle \to |0011\rangle, \quad |\phi_{1,0}\rangle \to |0100\rangle, \quad |\phi_{1,1}\rangle \to |0101\rangle,\\
&|\phi_{1,2}\rangle \to |0110\rangle, \quad |\phi_{1,3}\rangle \to |0111\rangle, \quad |\phi_{2,0}\rangle \to |1000\rangle,\\
&|\phi_{2,1}\rangle \to |1001\rangle, \quad |\phi_{2,2}\rangle \to |1010\rangle, \quad |\phi_{2,3}\rangle \to |1011\rangle,\\
&|\phi_{3,0}\rangle \to |1100\rangle, \quad |\phi_{3,1}\rangle \to |1101\rangle, \quad |\phi_{3,2}\rangle \to |1110\rangle,\\
&|\phi_{3,3}\rangle \to |1111\rangle. \qquad (14)
\end{aligned}$$

Provided that the original Bell state generated by TP is $|\phi_{0,0}\rangle$, 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 in Fig. 3. Under conditions free from eavesdropping, the obtained measurement result was $|0000\rangle$, indicating that the outcome of Bell measurement was $|\phi_{0,0}\rangle$, as shown in Eq. (14). If one of the two users performs CTRL operation and the other executes U_{30} operation in Case 2, the corresponding quantum circuit and the measurement outcome are depicted in Fig. 4. The final measurement result obtained by TP was $|1100\rangle$ (i.e., $|\phi_{3,0}\rangle$) and is consistent with Eq. (5). In case the two unitary operations implemented by the participants are U_{30} and U_{20}, respectively, the quantum circuit was designed in Fig. 5(a) and the corresponding measurement outcome was $|0100\rangle$ (i.e., $|\phi_{1,2}\rangle$), as depicted in Fig. 5(b). Based on the measurement outcome and Eq. (7), Alice (Bob) can obtain c_a^i (c_b^i) while TP can acquire c_{T}^i, which enables TP to achieve the comparison of their secrets.

6. Security analyses

6.1. External attack

Suppose Eve is an external eavesdropper motivated by the desire to steal Alice's and Bob's private information without being detected. To this end, Eve may launch three possible attacks on the transmitted 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 in states identical to her measurement results and forwards these 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. Consequently, our protocol achieves a higher detection rate compared to prior schemes. When Alice and Bob select to perform operations CTRL and U_{nm} (U_{nm} and CTRL), respectively, TP could discover Eve with a probability of $1-1/d^2$. When both classical users select CTRL operation directly, the probability of discovering Eve is $1-1/d^2$. Therefore, it can be inferred that the probability of evading participants' detection is

$$p_1 = \frac{1}{4} + 3 \times \frac{1}{4} \times \frac{1}{d^2} = \frac{d^2+3}{4d^2}. \qquad (15)$$

In other words, when one qubit is attacked, the probability of introducing error by Eve is $1-\left(d^2+3\right)/4d^2$ substantially. Thus, the total rate that Eve would be detected is $1-\left[\left(d^2+3\right)/4d^2\right]^t$, if t particles are attacked. As illustrated in Fig. 6, the probability p 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

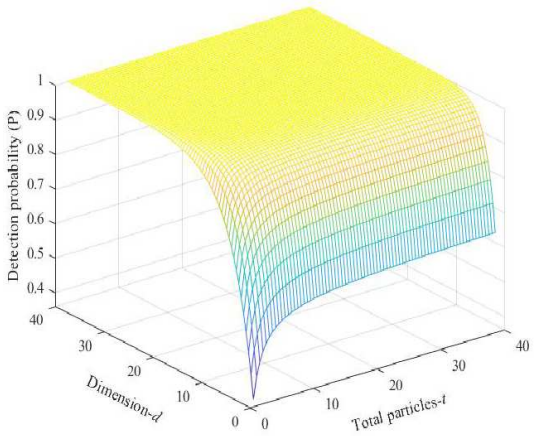


Fig. 6. Eavesdropping detection probability.

of detecting Eve approaches 1 when both t and d increase to 4. Therefore, it can be concluded that the suggested protocol could resist the intercept-measure-resend attack.

6.1.2. Entangle-measure attack

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

$$\begin{aligned} U_E|k\rangle|\varepsilon\rangle &= a_{k0}|0\rangle|\varepsilon_{k0}\rangle + a_{k1}|1\rangle|\varepsilon_{k1}\rangle + \cdots \\ &\quad + a_{k,d-1}|d-1\rangle\left|\varepsilon_{k,d-1}\right\rangle \\ &= \sum_{t=0}^{d-1} a_{kt}|t\rangle|\varepsilon_{kt}\rangle, \end{aligned} \tag{16}$$

$$\begin{aligned} U_E|F_k\rangle|\varepsilon\rangle &= U_E F|k\rangle|\varepsilon\rangle \\ &= U_E\left(\frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{kl}|l\rangle\right)|\varepsilon\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{kl}\left(U_E|l\rangle|\varepsilon\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{kl}\left(\sum_{j=0}^{d-1}a_{lj}|j\rangle\left|\varepsilon_{lj}\right\rangle\right) \\ &= \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{kl}\sum_{j=0}^{d-1}a_{lj}\left(\frac{1}{\sqrt{d}}\sum_{\zeta=0}^{d-1}\omega^{-\zeta j}\left|F_\zeta\right\rangle\left|\varepsilon_{lj}\right\rangle\right) \\ &= \frac{1}{d}a_{lj}\sum_{l,j,\zeta=0}^{d-1}\omega^{kl-\zeta j}\left|F_\zeta\right\rangle\left|\varepsilon_{lj}\right\rangle, \end{aligned} \tag{17}$$

where $\sum_{t=0}^{d-1}|a_{kt}|^2 = 1$ for $k = 0,1,\ldots,d-1$, $F_k = \frac{1}{\sqrt{d}}\sum_{l=0}^{d-1}\omega^{kl}|l\rangle$ and $\left|\varepsilon_{lj}\right\rangle$ is the pure auxiliary state. Whether Alice (Bob) executes operation CTRL or U_{nm}, 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 $a_{lj} = 0$, where $l \neq j$. In other words, Eqs. (16) and (17) can be reformulated as

$$U_E|k\rangle|\varepsilon\rangle = a_{kk}|k\rangle|\varepsilon_{kk}\rangle, \tag{18}$$

$$U_E|F_k\rangle|\varepsilon\rangle = \frac{1}{d}\sum_{j,m=0}^{d-1}\omega^{j(k-m)}a_{kk}|F_m\rangle|\varepsilon_{kk}\rangle. \tag{19}$$

Similarly, Eve must set $|F_k\rangle = |F_m\rangle$ to avoid her actions being detected, that is to say,

$$\sum_{j=0}^{d-1}\omega^{j(k-m)}a_{kk}|\varepsilon_{kk}\rangle = 0, \quad k \neq m. \tag{20}$$

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

$$\begin{aligned} U_E|\phi_{0,v}\rangle|\varepsilon\rangle &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}U_E|j\rangle|(j+v) \bmod d\rangle|\varepsilon\rangle \\ &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}a_{jj}\left|\varepsilon_{jj}\right\rangle|j\rangle|(j+v) \bmod d\rangle. \end{aligned} \tag{21}$$

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

$$a_{00}|\varepsilon_{00}\rangle = a_{11}|\varepsilon_{11}\rangle = \cdots = a_{d-1,d-1}\left|\varepsilon_{d-1,d-1}\right\rangle. \tag{22}$$

In accordance with Eq. (22), Eve cannot distinguish the auxiliary states $|\varepsilon_{00}\rangle, |\varepsilon_{11}\rangle, \ldots, \left|\varepsilon_{d-1,d-1}\right\rangle$. That is to say, Eve cannot gain any useful information from the ancillary states. Consequently, 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 seeks to manipulate the state of the traveling particles to deceive the participants into accepting false comparison outcomes without being detected. By performing unitary operation $U_{e_1e_2}$ on the transmitting particles, Eve can attain her goal of tampering with secret information. However, once Eve executes operation $U_{e_1e_2}$ on one particle in d-dimensional Bell state $|\phi_{u,v}\rangle$, the Bell state will be transformed into

$$\begin{aligned} U_{e_1e_2}|\phi_{u,v}\rangle &= \sum_{r=0}^{d-1}\mathrm{e}^{\frac{2\pi ire_1}{d}}|r\rangle|(r+e_2) \bmod d\rangle \\ &\quad \otimes\frac{1}{\sqrt{d}}\sum_{s=0}^{d-1}\mathrm{e}^{\frac{2\pi isu}{d}}|s\rangle_{\mathrm{A}}|(s+v) \bmod d\rangle_{\mathrm{B}} \\ &= \frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}\mathrm{e}^{\frac{2\pi ij(u+e_1)}{d}}|j\rangle_{\mathrm{A}}|(j+v+e_2) \bmod d\rangle_{\mathrm{B}} \\ &= |\phi_{u+e_1,v+e_2}\rangle. \end{aligned} \tag{23}$$

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 $|\phi_{u+e_1,v+e_2}\rangle$ instead of $|\phi_{u,v}\rangle$ as expected. Therefore, the existence of Eve can be easily detected by participants. In other words, the devised protocol can thwart this modification attack.

6.1.4. Double-CNOT attack

Eve performs the first controlled CNOT operation on the particles sent by TP to Alice or Bob. While Alice or Bob returns particles to TP, Eve performs the CNOT operation again. Since the execution of two CNOT operations leaves the particles and the encrypted message unchanged, Eve's attack will not be detected in this case. However, Eve cannot get any information or change the secrets of the participants by performing the double-CNOT attack. Therefore, the double-CNOT attack is ineffective against the protocol.

6.2. Internal attack

In general, the internal attack is more menacing than the external attack. In the inside attack, two types of participant attacks are considered: one is from dishonest Alice or Bob, and 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 just needs to know $R_a'^i$ to figure out Alice's privacy from c_a^i. Hence, Bob could launch any possible attack strategy to derive $R_a'^i$. Nevertheless, once Bob attempts to obtain r_a^i by performing an 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 Subsection 6.1. In conclusion, no matter what kind of attacks Bob launched, he is unable to access Alice's privacy without being detected. Similarly, it can be concluded that Alice could not dope out Bob's privacy either.

6.2.2. Attack from TP

Compared with other attacks, the 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 privacy of Alice and Bob. Except for colluding with other participants, TP could employ any possible attack strategy. In the devised protocol, the values of c_a^i and c_b^i are delivered to TP; besides, he could also obtain the information from S_{A} (S_{B}) and S'_{A} (S'_{B}). However, TP is still unable to extract the private information of Alice and Bob from c_a^i and c_b^i since the pre-shared key k_{ab}^i is out of his reach. Thus, TP can only conclude the size relation of x_i and y_i but cannot derive their precise values.

7. Comparison

The detailed comparisons among the presented protocol and those similar works in Refs. [32,36–38,43,44] are listed in Table 4. The designed scheme, similar to the protocols in Refs. [36–38], also could judge the size relation of two classical users' privacies. On the contrary, the SQPC protocol in Ref. [32] is only capable of determining the equality of the participants' privacies. Besides, it is well known that the qubit efficiency of SQPC protocols is denoted as $\eta = c/q$, where c denotes the number of compared privacies, while q is the overall number of particles prepared by participants. In the presented scheme, to compare $2n$-bit privacies, TP should prepare eight d-dimensional 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 $n/8$, which could be up to $1/2$ when $n = 4$. By contrast, in Refs. [36–38], the comparison process requires each participant to produce qubits, leading to a significant decrease in qubit efficiency.

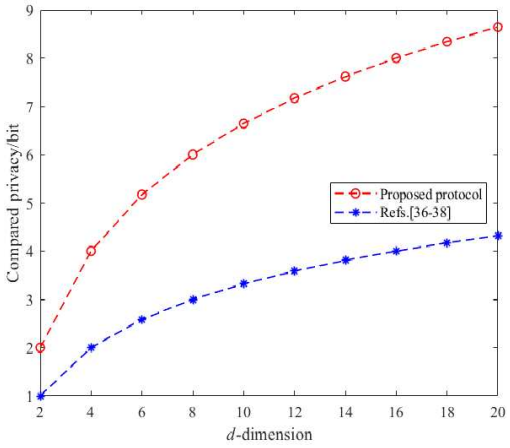


Fig. 7. Relationship between dimension and compared privacy.

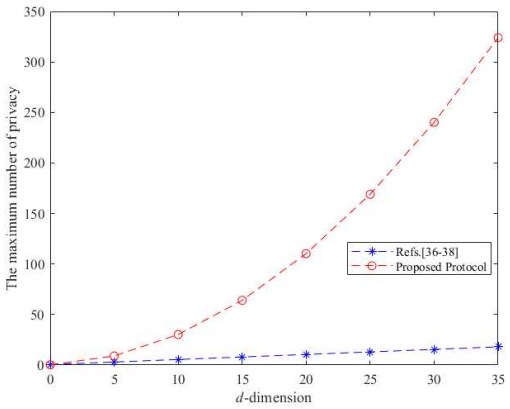


Fig. 8. Relationship between dimension and maximal privacy.

The proposed SQPC protocol exhibits a higher qubit efficiency than Refs. [32,36–38], as shown in Table 4. Furthermore, the proposed protocol and those in Refs. [36–38] 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 $2\log_2 d$-bit privacies with one qubit, whereas Refs. [36–38] only could compare $\log_2 d$-bit 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, our protocol scales to compare much larger private numbers than those in Refs. [36–38] as the dimension increases, as shown in Fig. 8. Consequently, if the participants intend to compare relatively larger private numbers, the proposed protocol has more significant advantages. Moreover, in Refs. [32,36,37], classical users need to possess the ability of measuring and preparing quantum states. In Ref. [37], although the classical users do not need to measure the qubits, they still should generate qubits. By contrast, the proposed protocol does not require classical users to prepare or measure any particles, which greatly reduces the difficulty of protocol

implementation. In Refs. [43,44], multiple participants can compare the size relationship of secret information by executing the protocol once. However, the protocols in Refs. [43,44] require the classical parties to measure and prepare new qubits, and the involvement of two semi-honest third-party TPs. In addition, their qubit efficiency is very low.

To guarantee protocol security, all the protocols listed in Table 4 need pre-shared secret keys between the classical participants. In the presented protocol, each participant refrains from disclosing any information about the particles, including the positions and the values. This approach effectively minimizes the risk of potential information leakage.

Table 4. Comparison among the designed protocol and the other typical SQPC ones. Here, d-D (d-dimensional), QR (quantum resource), CSQPC (category of SQPC), NMQCU (need of measuring qubits for classical users), NPQCU (need of preparing qubits for classical users), QE (qubit efficiency).

Protocols	[32]	[36]	[37]	Protocol 1[38]	Protocol 2[38]	[43]	[44]	Proposed protocol
QR	Single photon	d-D Bell state	d-D GHZ state	d-D single photon	d-D single photon	d-D single state	d-D Bell state	d-D Bell state
CSQPC	Equality	Size	Size	Size	Size	Size	Size	Size
NMQCU	Yes	Yes	Yes	No	No	Yes	Yes	No
NPQCU	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
QE	1/48	$1/24$	$n/16$	$n/24$	$n/12$	$1/32$	$1/24$	$n/8$
Secure	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

8. Conclusion

An efficient semi-quantum private comparison protocol is devised with d-dimensional Bell states, which could compare the size relation of two classical participants' privacies under the control of a semi-honest TP. It is not necessary for the classical parties to invoke measuring and preparing quantum states, thereby minimizing the waste of quantum resources and reducing the demands on quantum hardware. 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 resist various kinds of attacks, including outside attacks from attacker Eve and inside attacks launched by the participants.

Acknowledgment

Project supported by the National Natural Science Foundation of China (Grant No. 62161025).

References

[1] Bennett C H and Brassard G 2014 *Theor. Comput. Sci.* **560** 7
[2] Li Y, Cai W Q, Ren J G, Wang C Z, Yang M, Zhang L, Wu H Y, Chang L, Wu J C and Jin B 2025 *Nature* **640** 1
[3] Yu H, Sciara S, Chemnitz M, Montaut N, Crockett B, Fischer B, Helsten R, Wetzel B, Goebel T A and Kramer R G 2025 *Nat. Commun.* **16** 171
[4] Zhang J, Qin S J and Jin Z P 2025 *Quantum Inf. Process.* **24** 61
[5] Zhang Q, Zhong W, Du M M, Shen S T, Li X Y, Zhang A L, Zhou L and Sheng Y B 2024 *Phys. Rev. A* **110** 042403
[6] Lian J Y, Li X and Ye T Y 2023 *Phys. Scr.* **98** 035011
[7] Gong L H, Liu Y Y, Huang J H and Wang Y Z 2025 *Chin. J. Phys.* **94** 471
[8] Zhou Y Y, Wang Y P, Dai J Y and Gong L H 2025 *Adv. Quantum Technol.* **8** e00439
[9] Yao A C 1982 *Proc. 23rd Annu. Symp. Found. Comput. Sci.* November 3–5, 1982, Chicago, USA p. 160
[10] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[11] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[12] Lin J, Tseng H Y and Hwang T 2010 *Opt. Commun.* **284** 2412
[13] Liu B, Gao F, Jia H Y, Huang W, Zhang W W and Wen Q Y 2013 *Quantum Inf. Process.* **12** 887
[14] Tseng H Y, Lin J and Hwang T 2012 *Quantum Inf. Process.* **11** 373
[15] Wang J J, Dou Z, Chen X B, Lai Y P and Li J 2022 *Chin. Phys. B* **31** 050308
[16] Kou T Y, Che B C, Dou Z, Chen X B, Lai Y P and Li J 2022 *Chin. Phys. B* **31** 060307
[17] Hou M and Wu Y 2024 *Mathematics* **12** 3541
[18] Boyer M, Kenigsberg D and Mor T 2007 *Phys. Rev. Lett.* **99** 140501
[19] Zhao P, Zhong W, Du M M, Li X Y, Zhou L and Sheng Y B 2024 *Front. Phys.* **19** 51201
[20] Zhou S, Xie Q M and Zhou N R 2024 *Laser Phys. Lett.* **21** 065207
[21] Hu W, Zhou R G and Luo J 2022 *Chin. J. Phys.* **77** 1701
[22] Xing D, Wang Y F, Dou Z, Li J, Chen X B and Li L X 2023 *Chin. Phys. B* **32** 070308
[23] Houshmand M, Hassanpour S and Haghparast M 2024 *Opt. Quantum Electron.* **56** 759
[24] Tian Y, Zhang N Y J, Chang J Y and Li J 2024 *Phys. Scr.* **99** 095110
[25] Zhang X X, Zhou R G and Xu W S 2025 *Quantum Inf. Process.* **24** 1
[26] Gong L H, Li M L, Cao H and Wang B 2024 *Laser Phys. Lett.* **21** 055209
[27] Ye T Y and Lian J Y 2023 *Physica A* **611** 128424
[28] Gong L H, Ye Z J, Liu C and Zhou S 2024 *Laser Phys. Lett.* **21** 035207
[29] Chou W H, Hwang T and Gu J 2016 arXiv:1607.07961 [quant-ph]
[30] Ye T Y and Ye C Q 2018 *Int. J. Theor. Phys.* **57** 3819
[31] Lang Y F 2018 *Int. J. Theor. Phys.* **57** 3048
[32] Lin P H, Hwang T and Tsai C W 2019 *Quantum Inf. Process.* **18** 207
[33] Gong L H, Chen Z Y, Qin L G and Huang J H 2023 *Adv. Quantum Technol.* 2300097
[34] Li J, Wang Z, Yang J, Ye C Q, Che F T and Fu A Q 2025 *Int. J. Theor. Phys.* **64** 92
[35] Tian Y, Li J, Ye C, Chen X B and Li C 2022 *Int. J. Theor. Phys.* **61** 18
[36] Zhou N R, Xu Q D, Du N S and Gong L H 2021 *Quantum Inf. Process.* **20** 124
[37] Wang B, Liu S Q and Gong L H 2022 *Chin. Phys. B* **31** 010302
[38] Li Y C, Chen Z Y, Xu Q D and Gong L H 2022 *Int. J. Theor. Phys.* **61** 157
[39] Wang B, Gong L H and Liu S Q 2024 *Chin. Phys. B* **33** 110303
[40] Hu Y F, Gong L H and Zeng Q W 2025 *Quantum Inf. Process.* **24** 216
[41] Kong W B, Wang Y P, Gong L H and Dai J Y 2025 *Opt. Commun.* 132722
[42] Li H H, Gong L H and Zhou N R 2020 *Chin. Phys. B* **29** 110304
[43] Ye T Y and Lian J Y 2023 *Physica A* **611** 128424
[44] Lian J Y, Li X and Ye T Y 2023 *EPJ Quantum Technol.* **10** 10