Measurement device-independent multi-user semi-quantum private query protocol

Min Xiao[1,2*] and Anhua Peng[1]

[1]School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.
[2*]School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.

*Corresponding author(s). E-mail(s): xiaomin@cqupt.edu.cn;
Contributing authors: 2531741410@qq.com;

Abstract

In quantum private queries, the imperfection of measurement devices by users and database parties may be subjected to some side-channel attacks. In addition, the quantum capability of users may be limited in practice. We propose a multi-user semi-quantum private query protocol base on the single photon product state, in which many users can query different data items from the database simultaneously and each user is only required to perform single photon preparation on Z base and reflection. Furthermore, the proposed protocol is measurement device-independent, which removes all the detector side channels. The analysis shows that the protocol relaxes user quantum capability requirements and enhances security.

Keywords: Measurement device-independent, Semi-quantum, Multi-user quantum private query, Single photon

1 Introduction

Symmetrically private information retrieval(SPIR) [1] is a privacy-protected information retrieval, which allows users to hide their query information position and can't get additional data items during privacy retrieval, to achieve protection of user privacy and database security [2]. Quantum private query is a quantum cryptographic protocol that implements SPIR by means of quantum communication. Due to the

non-existence of unconditionally secure SPIR [3], quantum private queries relax the security requirements of SPIR, and allow users to access a limited amount of additional items, and user privacy is cheat-sensitive.

There are two methods to implement quantum private queries, which are based on oracle operation (unitary operation) or quantum key distribution(QKD). In 2008, Giovannetti et al. [4] proposed the first QPQ protocol (GLM protocol) based on unitary operation coding. The protocol encodes the database information to the unitary operation and applies it to the query state, and uses another superposition state for attack detection. The security analysis of this protocol is also given in the subsequent article [5]. In 2011, Olejnik et al. [6] proposed an improved protocol (O-protocol) based on the GLM protocol, reducing the communication complexity of the protocol. However, as the size of the database increases, the dimension of the unitary operation increases exponentially, which is difficult to implement. In the same year, Jakobi et al. [7] proposed the first QKD-based QPQ protocol (J-Protocol) based on the SARG04 protocol [8]. Compared with protocols based on unitary operations, it is more realizable, practical and loss-tolerant. Almost all subsequent QPQ protocols are implemented based on QKD.

In 2012, Gao et al. [9] proposed a protocol(G-protocol) whose security can be flexibly adjusted by introducing the angle parameter θ on the basis of J-protocol. Moreover, G-protocol has improved both in security and communication complexity. In 2013, Zhang et al. [10] proposed a QPQ protocol based on counterfactual QKD, pointing out that adding important detection devices to QKD devices can ensure the untrusted user privacy and database security. In 2014, Yang et al. [11] proposed a flexible QPQ protocol based on B92 [12], which improves the protocol by introducing entanglement on the basis of G-protocol. In 2015, Yang et al. [13] proposed a one state semi-quantum private query (SQPQ) protocol based on semi-quantum key distribution, which ensures user privacy and database security while reducing user quantum capability requirements. It is the first SQPQ protocol. SQPQ is QPQ protocol based on semi-quantum key distribution [14]. It can be described as follows. Any two computational basis $\{|0\rangle, |1\rangle\}$ of a two-level system can be defined as classical. If the party to the key agreement is classical, the protocol is said to be semi-quantum. Specifically, after receiving a qubit sent by the other party, a communicating party can only perform measurement and preparation operations on the classical basis, that is, either (1) measure the qubit with the classical $\{0, 1\}$ basis, (2) prepare a fresh qubit in the classical basis and send it, or let the qubit return to the channel undisturbed. In 2017, Zhao et al. pointed out that the security of the QKD-based QPQ protocol can be completely damaged by detector-blinding attacks [15], while the measurement device-independent methods [16–18] can solve the problem. It can be defined as: the security of a secret communication does not depend on a trusted measurement device. First proposed in QKD, MDI-QKD [16] achieves this goal by performing BSM in an untrusted third party. The key point is that the result of BSM does not reveal the quantum state information of the two sides of the communication. Benefiting from the idea of MDI-QKD, Zhao et al. [15] proposed loss-tolerant measurement device-independent QPQ. The protocol also has the characteristic of measurement device-independent protocol, which removes all the detector side channels while ensuring security. In 2019, Gao et al. [19] reviewed

the research progress of QPQ protocol and proposed a simple and effective method to detect external eavesdropper. In 2020, Ye et al. [20] proposed multi-user QPQ protocol (Ye-protocol) based on G-protocol, which added eavesdropping detection and honesty detection process to the database, and extended the protocol to allow multiple users to query different data items simultaneously. In the same year, Yang et al. [21] used GHZ state and entanglement swapping technology to propose a multi-user QPQ protocol for multi-user collaborative data query, which protects the user privacy and database security through real-time security detection. In 2021, Zhu et al. [22] performed a cryptographic analysis of the Ye-protocol and pointed out that adding a bidirectional authentication process can prevent man-in-the-middle attacks on it. In 2022, Wang et al. [23] proposed a multi-user QPQ protocol using the multi-particle W state to query the same data item through multi-user collaboration, and the protocol became more sensitive to the deception of the database holder as the number of users increased. In 2023, Basak [24] designed a semi-device independent multi-user QPQ protocol by means of multi-particle GHZ state verification and self-detection of the specific POVM operators, which ensures privacy and also allows different users to retrieve different data items.

Compared with the single-user QPQ protocol, the multi-user protocol can allow multiple users to retrieve at the same time, which is obviously more in line with the actual application scenario. This research development makes the QPQ protocol take a more practical step. However, the existing protocols do not consider the problem of insufficient user capacity and side channel in multi-user scenarios. Considering that SQPQ can solve the problem of insufficient quantum ability of users, and MDI-QPQ can remove all the side channels and make the protocol more secure and practical. Inspired by them, this paper proposes a measurement device-independent multi-user semi-quantum private query protocols. This protocol enables multiple semi-quantum users to query their own interested data items from the database at the same time, and eliminates all the detector side channels while ensuring the privacy of users and the database.

The paper is organized as follows: the proposed protocol is described in the Sect. 2, the correctness of the protocol is analyzed in the Sect. 3, the security of the protocol is analyzed in the Sect. 4, and the Sect. 5 is conclusion.

2 Proposed protocol

2.1 System model

As shown in Fig. 1, there are three participants in this protocol, namely a database holder Bob who sells data to users, n semi-quantum users $U_i(i = 1, 2, \ldots n)$ who want to buy data from the database, and a semi-trusted third party Charlie who assists in the execution of the protocol.

2.2 Security assumption

The security assumptions of the measurement device-independent multi-user SQPQ protocol are as follows:

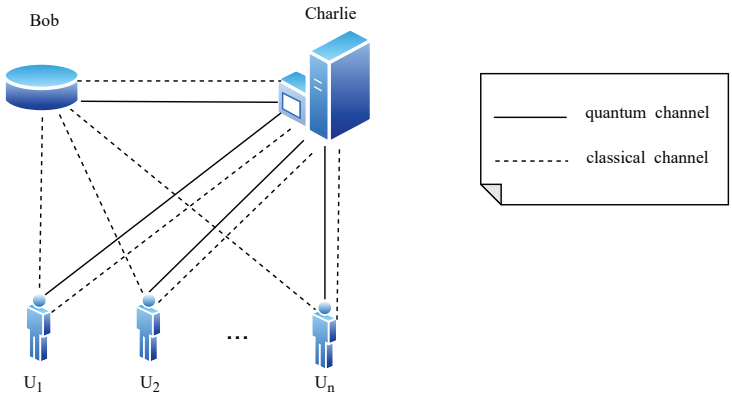

Fig. 1 System model

1. Charlie is a semi-trusted third party, he will honestly carry out the protocol steps, but he wants to get as much user privacy and database information as possible. Charlie will not conspire with Bob or users when the protocol is executed honestly.
2. Bob is not fully trusted, where the data item of the database is N, he always wants to know the user's retrieval address as much as possible to infer their private information. However, he will provide data honestly for the sake of the database's reputation.
3. Users $U_i (i = 1, 2, \ldots n)$ are untrusted, and always want more database information than they request.

2.3 Protocol description

Step 1: State Preparation

(1) Charlie prepares a sequence Φ of $l = \frac{2kN}{c}$(k is a security parameter, c is a constant coefficient representing the probability of successful BSM) product states, each randomly selected from $\{|+\rangle^{\otimes n}, |-\rangle^{\otimes n}\}$, where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. He then extracts the i-th qubit from each product state in Φ to obtain the sequence $S_C^i = \{s_C^j\}$ for each $i = 1, \ldots, n$ and $j = 1, \ldots, l$. Finally, Charlie sends each S_C^i to U_i and announces the quantum states of all qubits.

(2) Each U_i $(i = 1, \ldots, n)$ randomly selects to perform a CTRL or SIFT operation on the received sequence S_C^i, resulting in a new sequence $S_U^i = \{s_U^j\}$.

- **CTRL:** Sends the received qubit back to Charlie directly;
- **SIFT:** After receiving a qubit, generates a new qubit selected from $\{|0\rangle, |1\rangle\}$ with equal probability and sends it to Charlie.

(3) Bob prepares n random sequences of l length states, where each state is randomly selected from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, denoted as $S_B^i = \{s_B^j\}$ for each $i = 1, \ldots, n$ and $j = 1, \ldots, l$. Bob then sends all n sequences to Charlie.

Step 2: Bell Measurement

(1) Charlie receives the sequences from the users and Bob, then performs Bell state measurements (BSM) on corresponding qubits in S_U^i and S_U^i for each $i = 1, \ldots, n$. For each qubit pair $\{s_C^j, s_B^j\}$, the BSM operation is either successful or failed.

(2) Charlie announces all BSM events, including position strings $P^i = \{p^j | p^j \in \{0,1\}, j = 1 \ldots l\}$, where $p^j = 1$ indicates a successful measurement and $p^j = 0$ indicates a failed measurement, and the successful measurement results $R^i = \{r^j | j \in 1 \ldots l\}$, where $r^j \in \{00, 01, 10, 11\}$ corresponding to the Bell states $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$. Here, $l^* = cl$ represents the number of successful BSM numbers.

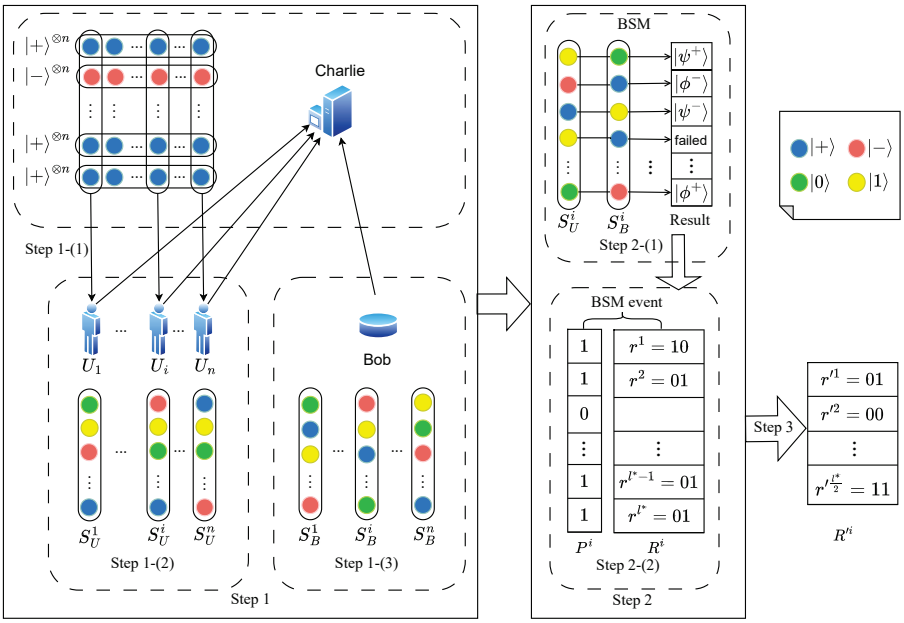

Fig. 2 The protocol procedure from Step 1 to Step 3

Step 3: Eavesdropping Detection Based on the measurement results, Charlie randomly selects $\frac{l}{2}$ positions D for eavesdropping detection by Bob and each $U_i (i = 1, \ldots, n)$. Specifically:

1. Bob and each U_i simultaneously announce the quantum states in the corresponding positions of S_B^i and S_U^i, then compare these announced states with the BSM results in R^i.
2. If the error rate exceeds a predefined threshold, it indicates eavesdropping, then the protocol is restarted; otherwise, the protocol continues.

It is important to note that this step not only detects eavesdropping in the channel but also verifies the honesty of the participants. If a party is dishonest, it will introduce additional errors in the measurement results, leading to detection. If some users and Bob have no successful BSM events in D, the protocol must be restarted, which only occurs when $c \leq \frac{1}{2}$. When $c > \frac{1}{2}$, there must be at least $(c-\frac{1}{2})l$ successful BSM events in D. Note that c is the probability that the BSM succeeds, determined by the BSM device. The effect of $c \leq \frac{1}{2}$ can be eliminated by using the BSM method from Ref. [25]. According to the coefficient of variation $C_v = \frac{1}{\sqrt{kN}}$, when kN is sufficiently large, the remaining successful measured qubit pairs for each user are very close to $\frac{l^*}{2} = kN$. The remaining successful BSM results are represented as $R'^i = \{r'^j\}$ for $j = 1, \ldots, \frac{l^*}{2}$ and $i = 1, \ldots, n$. Steps 1 to 3 are illustrated in Fig. 2.

Step 4: Key Negotiation Bob and each $U_i (i = 1, \ldots, n)$ use R'^i for key negotiation. Specifically, Bob announces a bit string $\Lambda^i = \{\lambda^j | j = 1, \ldots, \frac{l^*}{2}\}$ according to the following rule:

$$\lambda^j = \begin{cases} 0, & \text{if } s_B^j \in \{|0\rangle, |1\rangle\}, \\ 1, & \text{if } s_B^j \in \{|+\rangle, |-\rangle\}. \end{cases}$$

Step 5: Key Inference Each $U_i (i = 1, \ldots, n)$ infers the raw key based on their CTRL or SIFT operation, the bit string Λ^i announced by Bob, and the BSM results R'^i. In the case of honest protocol, the theoretical probabilities of the four Bell states $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$ can be derived based on the quantum states of the user and Bob, as shown in Table 1.

An example is given to illustrate how $U_i (i = 1 \ldots n)$ get a conclusive result in the honest protocol. If the measurement result is $|\phi^+\rangle$, U_i prepared the state $|0\rangle$, and only when Bob sent the state $|0\rangle$ and announced 0 will get the raw key bit 0. When Bob sent the state $|+\rangle$ or $|-\rangle$ and announced 1, U_i will not get a conclusive result. Although U_i and Bob send four random BB84 states essentially, and the state combinations of the four BSM results are different, it is not difficult to find that the analysis of other measurement results is similar by comparing Table 1. Then, the situations for users to obtain conclusive results are shown in Table 2. According to Table 2, it is not difficult to find when the states of the user and Bob are on the same basis, the user can get a conclusive result, then the probability of getting a conclusive result is $p_{con} = \frac{1}{2}$.

After the above steps, U_i and Bob share a raw key of $\frac{l^*}{2} = kN$ length, with Bob knowing all of the key and U_i only knowing some of them. Then, the raw key is divided into k substrings of length N, and then these substrings are added by bitwise to obtain a N bits final key $K^i (i = 1, 2 \ldots n)$.

Step 6: Database query Bob encrypts his database and $U_i (i = 1 \ldots n)$ gets the data item he wants based on a bit he known in K^i. For example, U_i knows the jth bit k_j^i in K^i and wants to get the ith item D_i in the database, he declares $s = j - i$, then Bob shifts K^i by s bits to get SK^i, then he encrypts the database with SK^i and sends the encrypted database to U_i. Finally, U_i can decrypts D_i by k_j^i.

Table 1 Quantum state theoretical probability of user and Bob when the BSM result is in $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^+\rangle\}$

	$\|\phi^+\rangle$				$\|\phi^-\rangle$				$\|\psi^+\rangle$				$\|\psi^-\rangle$			
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|0\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$\|1\rangle$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$
$\|-\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0

Table 2 The situations for U_i to obtain conclusive result, where the encoding rule is $0:\{|0\rangle,|+\rangle\}$, $1:\{|1\rangle,|-\rangle\}$, ? indicates a inconclusive raw key bit.

BSM result	The bit announced by Bob (Corresponding state)	U_i's state(State $\|0\rangle(\|1\rangle)$ corresponds to operation SIFT, otherwise CTRL)	Conclusive result	The raw key bit
$\|\phi^+\rangle$	0 ($\{|0\rangle,|1\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	Yes	0 (1)
	0 ($\{|0\rangle,|1\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	Yes	0 (1)
$\|\phi^-\rangle$	0 ($\{|0\rangle,|1\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	Yes	0 (1)
	0 ($\{|0\rangle,|1\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	Yes	1 (0)
$\|\psi^+\rangle$	0 ($\{|0\rangle,|1\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	Yes	1 (0)
	0 ($\{|0\rangle,|1\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	Yes	0 (1)
$\|\psi^-\rangle$	0 ($\{|0\rangle,|1\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	Yes	1 (0)
	0 ($\{|0\rangle,|1\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|0\rangle$ ($\|1\rangle$)	No	?
	1 ($\{|+\rangle,|-\rangle\}$)	$\|+\rangle$ ($\|-\rangle$)	Yes	1 (0)

3 Correctness

3.1 Correctness of Table 1

The qubit combination of user and Bob can be represented as equation (1), and the probability distribution in Table 1 can be obtained based on it. Take the measurement result $|\phi^+\rangle$ as an example, the state prepared by SIFT is $|0\rangle$, various possible cases are as follows:

(1) The state sent by Bob is $|0\rangle$, the BSM result get $|\phi^+\rangle$ or $|\phi^-\rangle$ with equal probability. Namely, $Pr(BSM = |\phi^+\rangle\,|U = |0\rangle, B = |0\rangle) = \frac{1}{2}$, where U and B denote the events of quantum states sent by U_i and Bob, respectively.

(2) The state sent by Bob is $|1\rangle$, the BSM result get $|\phi^+\rangle$ with none probability. Then $Pr(BSM = |\phi^+\rangle\,|U = |0\rangle, B = |1\rangle) = 0$.

(3) The state sent by Bob is $|+\rangle$ or $|+\rangle$, the BSM result get $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$ with equal probability. Then $Pr(BSM = |\phi^+\rangle\,|U = |0\rangle, B = |+\rangle) = Pr(BSM = |\phi^+\rangle\,|U = |0\rangle, B = |-\rangle) = \frac{1}{4}$.

3.2 Correctness of the proposed protocol

The analysis process for the remaining cases is similar to the above. The BSM result is $|\phi^+\rangle$ and U_i performs a SIFT operation, a conclusive result can only be obtained when Bob announces the bit value 0. In Step 5, we provided the method for users to obtain the conclusive key and the probability of obtaining the conclusive key. Then the average bits number of U_i's final key is $\overline{n} = N(p_{con})^k$. The probability that U_i knows none final key is $p_0 = [1-(p_{con})^k]^N$. It implies that the correctness of the proposed protocol is similar to the J-protocol [7] and G-protocol [9].

$$
\begin{aligned}
|00\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\phi^-\rangle) \quad & |0+\rangle &= \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle + |\psi^+\rangle + |\psi^-\rangle)\\
|01\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle + |\psi^-\rangle) \quad & |0-\rangle &= \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle - |\psi^+\rangle - |\psi^-\rangle)\\
|10\rangle &= \frac{1}{\sqrt{2}}(|\psi^+\rangle - |\psi^-\rangle) \quad & |1+\rangle &= \frac{1}{2}(|\phi^+\rangle - |\phi^-\rangle + |\psi^+\rangle - |\psi^-\rangle)\\
|11\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\phi^-\rangle) \quad & |1-\rangle &= \frac{1}{2}(|\psi^+\rangle - |\psi^-\rangle - |\phi^+\rangle + |\phi^-\rangle)\\
|++\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle + |\psi^+\rangle) \quad & |+0\rangle &= \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle + |\psi^+\rangle - |\psi^-\rangle)\\
|+-\rangle &= \frac{1}{\sqrt{2}}(|\phi^-\rangle - |\psi^-\rangle) \quad & |+1\rangle &= \frac{1}{2}(|\phi^+\rangle - |\phi^-\rangle + |\psi^+\rangle + |\psi^-\rangle)\\
|-+\rangle &= \frac{1}{\sqrt{2}}(|\phi^-\rangle + |\psi^-\rangle) \quad & |-0\rangle &= \frac{1}{2}(|\phi^+\rangle + |\phi^-\rangle - |\psi^+\rangle + |\psi^-\rangle)\\
|--\rangle &= \frac{1}{\sqrt{2}}(|\phi^+\rangle - |\psi^+\rangle) \quad & |-1\rangle &= \frac{1}{2}(|\phi^-\rangle - |\phi^+\rangle + |\psi^+\rangle + |\psi^-\rangle)
\end{aligned}
\tag{1}
$$

4 Security analysis

The proposed protocol allows all users and the database to avoid all the detector side channels, which means that any security issues related to the detector will be eliminated, but dishonest users and the database and semi-trusted Charlie want to get as much information as possible. Since the participants have more advantages than the external eavesdroppers, the attacks from the external eavesdropper can be regarded as the attacks conducted by the participants. In addition, existing QPQ protocols [26, 27] with authentication processes can resist some external attacks such as man-in-the-middle attacks, which is not the focus of this article. Therefore, we do not specifically consider the external attackers. Our primary concern is user privacy and database privacy.

4.1 Database privacy

4.1.1 Attacks from users

Fake state attack Users may perform a fake state attack, such as sending the state $|\varphi\rangle$ in step 1 to increase the probability of getting a certain measurement result. The state $|\varphi\rangle$ has the form:

$$|\varphi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle \tag{2}$$

where $\theta \in (0, \frac{\pi}{2})$. During the eavesdropping detection, U_i only knows the BSM results, but does not know Bob's state. U_i can only randomly select a state based on the BSM result to announce. According to Table 3, when the result is $|\phi^+\rangle$, the various states announced by U_i are as follows:

(1) $|0\rangle$ announced by U_i, then Bob's state is $|1\rangle$ with the probability $\frac{1}{2}\sin^2\theta$, but it is impossible in the case of honest protocol, so $|0\rangle$ announced by U_i has the probability $\frac{1}{2}\sin^2\theta$ being detected.
(2) Similarly, $|1\rangle$ announced by U_i has the probability $\frac{1}{2}\cos^2\theta$ cannot pass eavesdropping detection.
(3) $|+\rangle$ announced by U_i has the probability $\frac{1-\sin 2\theta}{4}$ cannot pass eavesdropping detection.
(4) $|-\rangle$ announced by U_i has the probability $\frac{1-\cos 2\theta}{4}$ cannot pass eavesdropping detection.

The four states sent by Bob with equal probability, then BSM result is also get four Bell states with equal probability. There is a probability of U_i announcing an impossible state with $\frac{1}{4}$. So, the probability of U_i passing eavesdropping detection is $P_a = (1 - \frac{1}{4})^{\frac{l^*}{2}} = (\frac{3}{4})^{kN}$, when kN is relatively large, the probability of U_i passing eavesdropping detection is close to 0.

Table 3 Comparison between the theoretical probability of the combination of U_i's cheat state and Bob's honest state when the BSM result is $|\phi^+\rangle$ and the theoretical probability in the case of honest protocol

	$\|\phi^+\rangle$			
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|\varphi\rangle$	$\frac{1}{2}\cos^2\theta$	$\frac{1}{2}\sin^2\theta$	$\frac{1+\sin 2\theta}{4}$	$\frac{1-\sin 2\theta}{4}$
$\|0\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
$\|1\rangle$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
$\|-\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$

Assuming that U_i is lucky enough to pass the eavesdropping detection, based on the BSM results and the bits announced by Bob, he wants to get the conclusive results. Taking measurement result $|\phi^+\rangle$ as an example, the probability distribution of the state combination of U_i and Bob is shown in Table 3. When 0 announced by Bob, in U_i's view, the probabilities of Bob's state being $|0\rangle, |1\rangle$ are $P_0 = \cos^2\theta$ and $P_1 = \sin^2\theta$, respectively. To obtain a conclusive result, U_i can only set $\theta = 0$ or $\frac{\pi}{2}$. At this point, U_i's state is $|0\rangle$ or $|1\rangle$. With θ being other values, according to Table 1 and Table 3, if U_i wants to get the raw key bit 0, then he has the probability $\cos^2\theta$ of getting the correct result, but there is also the probability $\sin^2\theta$ of Bob sending the state $|1\rangle$ so that getting the wrong result. When U_i wants to get the raw key bit 0, it has an error rate of $\cos^2\theta$. When 1 announced by Bob, from the perspective of U_i, the probabilities of Bob's state being $|+\rangle, |-\rangle$ are $P_+ = \frac{1+sin2\theta}{2}$ and $P_- = \frac{1-sin2\theta}{2}$, respectively. In order to obtain a conclusive result, U_i can only set $\theta = \frac{\pi}{4}$ or $\frac{3\pi}{4}$. Then the states of U_i are $|+\rangle$ or $|-\rangle$. When θ is set to other values, if U_i wants to obtain the raw key bit 0, there is an error rate of $\frac{1-sin2\theta}{2}$. Similarly, if U_i wants to obtain the raw key bit 1, there is an error rate of $\frac{1+sin2\theta}{2}$. In other cases, U_i cannot get exact results. These inconclusive results will cause U_i to get the raw key bit that is inconsistent with Bob, and finally get the wrong query result. It is reasonable to assume that even if U_i is lucky enough to pass the eavesdropping detection, there is no need to invade the database privacy by this attack strategy for wrong query answers.

Participant attack Participant attacks from dishonest users are generally more powerful [28]. $U_j(j = 1 \ldots n, j \neq i)$ may launch an attack on the sequence sent by Bob or U_i, then U_j is an external eavesdropper actually, which will be detected in Step 3. It is noted that each user in the proposed protocol is independent of each other, then the joint attack from multiple participants is not necessary because they cannot benefit from it and moreover there is a risk of detection in Step 3.

4.1.2 Attacks from Charlie

The semi-trusted third party, Charlie, although he will honestly implement the protocol and not collude with other participants, will attempt to obtain some raw key $K^i(i = 1 \ldots n)$ information based on BSM result and other publicly available information. Since the state sent by Bob is a random BB84 state, Charlie can only infer the key K^i according to his BSM result, and from Table 1, Charlie has no better strategy than random guessing.

4.2 User privacy

Both Bob and semi-trusted Charlie attempt to obtain the location of the user's query data item. They are a major security concern for users under user privacy without having to trust the measurement-device. Since the raw key obtained by each user is independent of each other, the privacy analysis of a particular user applies to all users, and the following analysis only needs to be carried out for user $U_i(i = 1, 2 \ldots n)$. Moreover, in order to prevent Trojan horse attacking, U_i can pass the signal through wavelength filter and the photon number separator (PNS) before he receives it.

4.2.1 Attacks from Bob

We suppose that the conditions for the participant's photon sources, channels, and detectors are perfect, which maximizes the probability Bob knows the position of data item $U_i(i = 1 \dots n)$ is interested in. Since all measurement operations are delegated to a semi-trusted third party Charlie, it is not feasible for Bob to cheat from the measurement side.

Fake initial state attack Based on the above analysis, although Bob can not cheat on the detector, it can also adopt a fake state attack similar to the users. However, Bob needs to be able to pass eavesdropping detection. In eavesdropping detection, the only information Bob knows is the BSM result, but he has to publish his state with n users at the same time. Different users at one detection position may have different BSM results, but he does not know what the states the users will announce, so he cannot exclude the possible states of these users. He can only announce one of the four states based on the BSM result, and he has the probability $\frac{1}{4}$ of choosing an impossible state that will cause the detection to fail. Then the probability of Bob passing the detection is $P_b = (1 - \frac{1}{4})^{\frac{nl^*}{2}} = (\frac{3}{4})^{nkN}$. As the number of users and kN increase, the probability of Bob passing the eavesdropping detection approaches 0.

Entangled state attack Bob wants to get the U_i's raw key bits by preparing the entangled state. Suppose Bob prepares entangled state $|\phi^+\rangle$,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{12} \tag{3}$$

Table 4 Comparison between the theoretical probability of the combination of U_i's honest state and Bob's cheat state when the BSM result is $|\phi^+\rangle$ and the theoretical probability in the case of honest protocol

	$\|\phi^+\rangle$			
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
$\|\phi^+\rangle_1$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$
$\|0\rangle$	$\frac{1}{2}$	0	$\frac{1}{4}$	$\frac{1}{4}$
$\|1\rangle$	0	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$
$\|+\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{2}$	0
$\|-\rangle$	$\frac{1}{4}$	$\frac{1}{4}$	0	$\frac{1}{2}$

then he sends qubit 1 to Charlie for BSM while keeping qubit 2 for himself. After Charlie announced the BSM results, Bob wanted to get the conclusive state Alice

sent based on the state qubit 2 was in. However, qubit 2 will collapse into four states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ with equal probability, and Bob cannot discriminate them perfectly. Then, in eavesdropping detection, Bob is unable to get beneficial information from the BSM results and cannot determine the states sent by U_i, he has no better strategy than to announce a state randomly based on the BSM result. According to Table 4, using a similar analysis method to the Sec. 4.1.1, the error rate of Bob with $\frac{1}{4}$ finally fails to pass the eavesdropping detection at a BSM position. This error rate cannot be ignored. The cheating behavior will be detected in Step 3 then cause the protocol to restart.

4.2.2 Attacks from Charlie

Since Charlie is semi-trust third party, he will honestly implement the protocol, but he wants to get the data items that U_i is interested in as much as possible according to his own measurement results and public information. Since the operation chosen by U_i is random, and according to the known BSM results, the states sent by U_i are equally probabilistic on X or Z basis, which is obviously the same as random guess. As long as users do not disclose their own random operations, then Charlie can not gain more advantage than random guessing based on the information he has.

4.3 Similar protocol comparison

Table 5 Comparison of the proposed protocol with similar works

Protocol	Resource states	Support multi-user retrieval	Support users retrieve different items	User capability requirement	Remove detector side channels
[13]	single photon	No	No	Semi-quantum capability	No
[15]	single photon	No	No	Full-quantum capability	Yes
[20]	Product States	Yes	Yes	Full-quantum capability	No
[21]	GHZ state	Yes	No	Full-quantum capability	No
[23]	W state	Yes	No	Full-quantum capability	No
[24]	GHZ state	Yes	Yes	Full-quantum capability	No
the proposed protocol	Product states	Yes	Yes	Semi-quantum capability	Yes

The comparison of the proposed protocol with similar works is shown in Table 5. It is not difficult to see that most multi-user QPQ protocols use high-dimensional entangled states as quantum resources, and these multi-user protocols don't take into account the detector side-channel problem. In MDI-QKD [16, 29, 30], all the detector

side channels are removed by performing BSM through an untrusted third party, while the legitimate communicating party only needs to ensure the classical information of the state prepared by itself is not leaked. The QPQ protocol proposed in this paper is based on MDI-QKD and thus also inherits this feature. Different from the implementation of Ref. [15], BSM is delegated to a semi-trusted third party Charlie in our protocol. As long as users do not disclose their specific random operations and Bob does not disclose the state sequences he sends, BSM cannot reveal the quantum state information of the user and Bob in the protocol. In this way, measurement device-independent is achieved by removing all detector side channels. In addition, the existing SQPQ protocols are limited to single-user scenarios. The protocol proposed in this paper eliminates the side channel of the detector while ensuring multiple users with only semi-quantum capabilities can query different data items.

5 Conclusion

In this paper, a measurement device-independent multi-user SQPQ protocol is proposed by using product states. While retaining the advantages of MDI-QPQ in the single user scenario, the protocol extends single user to multiple users enables multiple users to query different data items simultaneously, while reducing the quantum capability requirements of users, making the protocol more practical. We not only analyze the correctness of the proposed protocol, but also the user privacy and database privacy of the protocol. The analysis result shows that the proposed protocol can ensure the privacy of the user and the database, and eliminate all the detection end-side channels. In the future, we need to consider more realistic scenarios, such as making third parties untrusted and performing a more comprehensive security analysis of the protocol.

Data availability Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declarations

Conflict of interest All authors disclosed no relevant relationships.

Competing interests The authors declare no competing interests.

References

[1] Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. Journal of Computer and System Sciences **60**(3), 592–629 (2000)

[2] Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: Private information retrieval. J. ACM **45**(6), 965–981 (1998)

[3] Lo, H.-K.: Insecurity of quantum secure computations. Phys. Rev. A **56**, 1154–1162 (1997)

[4] Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries. Physical Review Letters **100**(23), 230502 (2008)

[5] Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries: Security analysis. IEEE Transactions on Information Theory **56**(7), 3465–3477 (2010)

[6] Olejnik, L.: Secure quantum private information retrieval using phase-encoded queries. Physical Review A **84**(2), 022313 (2011)

[7] 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. Physical Review A **83**(2), 022301 (2011)

[8] Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Physical Review Letters **92**(5), 057901 (2004)

[9] Gao, F., Liu, B., Wen, Q.-Y., Chen, H.: Flexible quantum private queries based on quantum key distribution. Optics Express **20**(16), 17411 (2012)

[10] Zhang, J.-L., Guo, F.-Z., Gao, F., Liu, B., Wen, Q.-Y.: Private database queries based on counterfactual quantum key distribution. Physical Review A **88**(2), 022334 (2013)

[11] Yang, Y.-G., Sun, S.-J., Xu, P., Tian, J.: Flexible protocol for quantum private query based on b92 protocol. Quantum Information Processing **13**(3), 805–813 (2014)

[12] Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)

[13] Yang, Y.-G., Zhang, M.-O., Yang, R.: Private database queries using one quantum state. Quantum Information Processing **14**(3), 1017–1024 (2015)

[14] Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Physical Review A **79**(3), 032341 (2009)

[15] Zhao, L.-Y., Yin, Z.-Q., Chen, W., Qian, Y.-J., Zhang, C.-M., Guo, G.-C., Han, Z.-F.: Loss-tolerant measurement-device-independent quantum private queries. Scientific Reports **7**(1), 39733 (2017)

[16] Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. **108**, 130503 (2012)

[17] Maitra, A.: Measurement device-independent quantum dialogue. Quantum Information Processing **16**(12), 305 (2017)

[18] Liu, B.-X., Huang, R.-C., Yang, Y.-G., Xu, G.-B.: Measurement-device-independent multi-party quantum key agreement. Frontiers in Quantum Science and Technology **2**, 1182637 (2023)

[19] Gao, F., Qin, S., Huang, W., Wen, Q.: Quantum private query: A new kind of practical quantum cryptographic protocol. Science China Physics, Mechanics & Astronomy **62**(7), 70301 (2019)

[20] Ye, T.-Y., Li, H.-K., Hu, J.-L.: Multi-user quantum private query protocol. International Journal of Theoretical Physics **59**(9), 2867–2874 (2020)

[21] Yang, H., Xiao, M.: Multi-user quantum private query. Quantum Information Processing **19**(8), 253 (2020)

[22] Zhu, D., Wang, L., Zhu, H.: Cryptanalysis of multi-user quantum private query protocol. International Journal of Theoretical Physics **60**(1), 284–292 (2021)

[23] Wang, H.-P., Zhou, R.-G.: Multi-user quantum private query using symmetric multi-particle w state. International Journal of Theoretical Physics **61**(3), 71 (2022)

[24] Basak, J.: Multi-user semi-device independent quantum private query. Quantum Information Processing **22**(7), 276 (2023)

[25] Gao, Z., Su, Z., Song, Q., Genevet, P., Dorfman, K.E.: Metasurface for complete measurement of polarization bell state. Nanophotonics **12**(3), 569–577 (2023)

[26] Xiao, M., Lei, S.: Quantum private query with authentication. Quantum Information Processing **20**(5), 166 (2021)

[27] Xiao, M., Zhao, M.: Multi-user quantum private query using bell states. Quantum Information Processing **23**(3), 81 (2024)

[28] Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: A simple participant attack on the brádler-dušek protocol **7**(4), 329–334 (2007)

[29] Primaatmaja, I.W., Lavie, E., Goh, K.T., Wang, C., Lim, C.C.W.: Versatile security analysis of measurement-device-independent quantum key distribution. Phys. Rev. A **99**, 062332 (2019)

[30] Curty, M., Xu, F., Cui, W., Lim, C.C.W., Tamaki, K., Lo, H.-K.: Finite-key analysis for measurement-device-independent quantum key distribution. Nature Communications **5**(1), 3732 (2014)