Responses to the Comments

We do appreciate for all the comments from reviewers and the handling editor. These comments are all valuable and helpful for revising and improving our manuscript, as well as the important guiding significance to our researches. We have studied comments careful and have made correction which we hope meet with approval. We have revised the paper based on the comments to significantly improve the writing. Here, we provide a detailed explanation of the revisions, with the modified content highlighted in red.

Reviewer #1:

Comment 1: In the Introduction, this paper only sees that they list many protocols of predecessors, lacking their own summary or thinking, so that the title of the article can be introduced in the next step. At the same time, some keywords often mentioned in the article, such as semi-quantum QPQ, independent of measurement equipment, etc., also lack relevant explanations or definitions.

Response: Thank you very much for this valuable advice. First , we have revised the third paragraph of the introduction to explain the keywords SQPQ and MDI. The revisions are as follows, with the changes in red:

"*2012, Gao et al. 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. 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. proposed a flexible QPQ protocol based on B92, which improves the protocol by introducing entanglement on the basis of G-protocol. In 2015, Yang et al. 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. 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, while the measurement device-independent methods 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 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. 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."

Then, a summary of previous protocols was added in the third and fourth paragraphs of the introduction, and the specific modifications were as follows, where the red font is the revised content:

"*In 2019, Gao et al. reviewed the research progress of QPQ protocol and proposed a simple and effective method to detect external eavesdropper. In 2020, Ye et al. 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. 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. 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. 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 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."

Comment 2: In Section 2.2, there is a problem with the role definition of database Bob. Even if Bob is untrustworthy, in order to protect user privacy, the protocol's provisions for Bob should also prevent Bob's malicious behavior. How can Bob in the text obtain the user's private information?

Response: Thank you very much for your valuable modification suggestion. We have corrected the description of Bob's role in 2.2. Since Bob may provide data honestly for the sake of reputation, but he is also interested in user privacy, here Bob is defined as not fully trusted. The specific changes are as follows.

"*Bob is not fully trusted (untrusted, previously), 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 (he may obtain the user's retrieval address and infer their private information by some malicious behaviors, previously). However, he will provide data honestly for the sake of the database's reputation.*"

Comment 3: There is an error in (3) in 2.3 Step 1

Response: Thank you very much for pointing out this error, we have revised the error in (3) in 2.3 Step 1.The revision is as follow.

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

Comment 4: The definitions of various symbols in the text are too complicated and too many, affecting the perception, such as SBi, Ri', etc. In Step 3 of 3.2, how do different values of c affect the BM measurement results? After all, the text says that the probability of obtaining a deterministic result is pc=0.5.

Response: Thank you very much for pointing out these valuable suggestions.

First, we have simplified the symbolic representation and description in the protocol description. We don't list the changes here but they are highlighted in red.
Second, in Step 1 (1) of Section 2.3, we have noted the meaning of c, which I would like to explain in detail for you. c is a constant coefficient that represents the probability of BSM success, which is related to the specific BSM device used in the implementation of the protocol. Meanwhile, in Step 3 of Section 2.3, we have described the impact of different c values on the protocol and proposed a solution to eliminate the effects of c values being too small. We have also modified the symbolic

representation of the subscript and constant coefficient c to avoid any misunderstandings caused by the fact that the subscript and constant coefficient c are the same for $p_c = 0.5$. The specific modification has also been highlighted in red in Step 3 of Section 2.3 in revised paper.

Comment 5: The format in Tables 1, 3, and 4 is not standardized. Table 5 mentions a removal of the detector side channel to achieve an effect that is independent of the measurement device. The text also lacks relevant explanations in this regard.

Response: Thank you very much for pointing out the important issues. We have standardized Tables 1, 3, and 4, and explained the effect of achieving measurement device independence proposed in Table 5 in 4.3. The revision is as follows, where the red font is the revised content.

"*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 [1][5][6] , 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., 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.*"

Comment 6: It is recommended to use more data analysis to reflect the advantages of the protocol in this article.

Response: I would like to express my sincere gratitude for your valuable suggestion. In the first section of the security analysis, we explained the impact of external eavesdroppers on the protocol. Here, it is necessary to explain again that the eavesdropping attack of external eavesdroppers will be detected as a participant attack. Furthermore, existing QPQ protocols with authentication processes [2][3] can resist some external attacks such as man-in-the-middle attacks. By adding an authentication process before the proposed protocol, we can achieve the same effect. However, this is

not the focus of this paper, so we only analyzed the impact of external eavesdropping without specifically analyzing external attacks. Specifically, the modifications are as follows:

"**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 theparticipants. In addition, existing QPQ protocols [2][3] 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."

In section 4.1.1, we added an analysis of participant attacks, and in section 4.3, we explained how to achieve measurement device independence in the protocol comparison. Specifically, the modifications are as follows:

"***4.1.1Attacks from users***

Participant attack *Participant attacks from dishonest users are generally more powerful[4].* $U_j(j=1,...,n, j\neq i)$ *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."

References:

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

[2]. Xiao, M., Lei, S.: Quantum private query with authentication. Quantum Information Processing 20(5), 166 (2021) 16

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

[4]. Gao, F., Qin, S.-J., Wen, Q.-Y., Zhu, F.-C.: A simple participant attack on the br´adler-du˘sek protocol 7(4), 329–334 (2007)

[5]. 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)

[6]. 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)

Reviewer #2:

Comment 1: In step 1(1), Charlie sends the sequences to each user U_i and then announces the states of them immediately, it is puzzling. She can announce the information about the states and ask the user to prepare the states according to her announcement and the user's choices of CTRL/SIFT. Such operation is simpler and can avoid two-way quantum communications as well as corresponding loopholes induced by two-way quantum communications.

Response: Thank you very much for your valuable suggestion. Allow us to explain it to you. We have carefully studied some semi-quantum QPQ protocols in the single-user scenario [1][2], which only require one quantum state for the initial state and then perform similar CTRL/SIFT operations based on the initial state. Inspired by these protocols, we hereby announce the quantum state only to enable users to obtain precise state information, and then perform random CTRL/SIFT operations to form new sequences for key negotiation. Since the initial state sequence and the new sequence formed by subsequent operations are not related, announcing precise state information will not have a significant impact on subsequent key negotiation. Furthermore, the protocol also includes a eavesdropping detection step to reduce the impact of this behavior.

Comment 2: In step1(3), Bob prepares quite a lot of identical quantum states and sends them to Charlie. It is also dangerous when the man-in-the-middle attack is considered. The attacker can intercept multiple copies of the identical quantum states and uses them to obtain the accurate state of each carrier qubit, and then instead he/she prepares the correct states accordingly and sends them to Charlie. This attack can steal the whole database and cannot be detected.

Response: Thank you very much for raising this issue. We has already modified the description of this part. In step 1(3), Bob prepares n random (previously identical) state sequences. This modification prevents an eavesdropper from intercepting multiple copies to obtain the exact quantum state of each qubit. The specific modifications are as follows.

"*Bob prepares* n *random sequences of* $j=1,...,l$ *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* $i=1,...,n$

and $j = 1, ..., l$. *Bob then sends all* n *sequences to Charlie.*"

References:

[1]. Yang, Y.-G., Zhang, M.-O. & Yang, R. Private database queries using one quantum state. Quantum Inf Process 14, 1017–1024 (2015).

[2]. Ye, T.-Y., Li, H.-K. & Hu, J.-L. Semi-Quantum Private Query Protocol Without Invoking the Measurement Capability of Classical User. Int J Theor Phys 59, 2044–2051 (2020).