Quantum Information Processing (2021) 20:166
https://doi.org/10.1007/s11128-021-03099-9

Quantum private query with authentication

Min Xiao[1] · Shumei Lei[2]

Received: 2 September 2020 / Accepted: 8 April 2021 / Published online: 3 May 2021

Abstract

The quantum privacy query (QPQ) is the quantum version of private query, which refers to that a user (Alice) to purchase data from a database owner (Bob) under the condition of ensuring the privacy of both parties. Specifically, Alice should not access data other than those she bought, and Bob cannot know what data Alice has obtained. The existing QPQ protocols focus on privacy protection and ignore other attacks from outside attackers, such as impersonation, man-in-the-middle and tampering. Undoubtedly, these attacks can destroy the QPQ process. In this paper, we present a secure QPQ protocol that can resist external active attacks. By designing an identity authentication mechanism and integrating it into the existing quantum key distribution-based QPQ protocol, the proposed protocol implements mutual identity authentication in the oblivious key agreement phase to resist impersonation and "man-in-the-middle" attacks. Besides, the mutual authentication process also generates a shared key between Alice and Bob to achieve the data source authentication and integrity protection against tampering attack in the data retrieval phase. The security analysis demonstrates that the proposed protocol not only retains the privacy protection strength of the original QPQ protocol, but also has strong resistance to external attacks.

Keywords Quantum private query · Quantum identity authentication · Quantum message authentication · External attack

✉ Min Xiao
xiaomin@cqupt.edu.cn

Shumei Lei
1291923916@qq.com

[1] School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

[2] College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

1 Introduction

Private query is a practical issue in cryptography, in which a user purchases data from a database provider, each item is a valuable and sensitive message in database. Therefore, this task needs to meet two basic security requirements: (1) Bob should not know what item is purchased by Alice (user privacy); (2) Alice should not be able to access additional items other than the one she is interested in (database privacy). Early-stage, Gertner et al. [1] described the above problem as symmetric privacy information retrieval (SPIR), which is an extension of private information retrieval(PIR) [2] that can only guarantee user's privacy. Later, Lo et al. [3] proved that the SPIR was not absolutely secure even in the quantum environment, and this task could not be ideally realized.

Classical cryptography which is secured by computational assumptions may be vulnerable to quantum computing, while quantum cryptography solves this problem and it can introduce information-theoretic security. Recently, quantum cryptography has brought new possibilities to the SPIR problem, namely quantum private query (QPQ). Particularly, compared with the classical SPIR protocols, the QPQ protocols not only reduce the communication and computing complexity but also can be implemented securely with current technology.

In 2008, Giovannetti et al. [4] proposed the first QPQ protocol, which encodes the entire database into unitary operations, called oracle, and this oracle is performed on the two query states sent by Alice, one qubit contributes to the data query and the other relevant superposition state gives her a chance to detect Bob's cheating. Subsequently, Martini et al. [5], Giovannetti et al. [6] respectively conducted a QPQ experiment based on linear optics and QPQ security analysis, and an improved scheme based on phase-coded query was proposed by Olejnik [7]. Compared with the previous SPIR schemes, these QPQ protocols have an exponential decrease in communication complexity and computing complexity. Nevertheless, the oracle-based QPQ schemes are difficult to implement in practice, i.e., with the expansion of the database, the corresponding unitary operation dimension is also larger; these protocols are not secure any more if the quantum channel cannot tolerate loss.

In light of the above, in 2011, Jakobi et al. [8] initially used asymmetric quantum key distribution [9] to design a QPQ protocol (J-protocol), which can easily implement with current technology. On account of the protocol's characteristics of practical feasibility, transmission loss tolerance and scalability to large databases, J-protocol has attracted wide attentions, and different improvement schemes have emerged, such as a more flexible and controllable version of the J-protocol [10], improvement of post-processing [11,12], without a failure probability [13], enhancement of user privacy and database security [14,15], noise tolerance [16–18], real-time security check [19], resisting joint-measurement attack [20], adopting new quantum sources [21–23] and multi-user query [24]. The security of these J-protocol-like schemes is based on a cheating-sensitive strategy, that is, Alice will find the attack of dishonest Bob with a nonzero probability.

In terms of security, the existing QPQ protocols mainly focus on privacy of database and user and ignore the active attacks from external adversaries (Eve). However, in a practical scenario, there may be the following cases: (1) Eve may impersonate

Alice to communicate with Bob and obtain profit from the illegally obtained data, or Eve impersonates Bob to communicate with Alice and provides fake data to cheat money; (2) Eve may directly intercept and forge or tamper with the data that Bob returned to Alice, causing Alice to obtain a wrong item; (3) Eve may sneak into the communication between Alice and Bob and negotiate the oblivious key with them respectively to eavesdrop on the data that Alice bought from Bob. Obviously, these active attacks from external adversaries can destroy the QPQ process and thus the effective measures must be taken to prevent them. In 2019, Gao et al. [25] pointed out the necessity of defending against external adversaries in QPQ, they also introduced a simple and effective procedure to detect external eavesdroppers by estimating the error rate of part of the raw key based on the declarations of Alice and Bob. However, the emerging question of their method is how to estimate the threshold value of the error rate, and it mainly focuses on external eavesdropping attacks but ignores a "man-in-the-middle" attack.

Different from Gao et al's method, we combine QPQ with quantum authentication in this task. In a realistic QPQ environment, a user and a database owner do not trust each other, we believe it is reasonable that Alice and Bob should not share an initial secret. Due to this, the introduction of a trusted third party(TTP) becomes inevitable. Therefore, there are some quantum authentication protocols that introduce TTP. Zeng et al. [26] first proposed the identity verification in QKD via the assistance of TTP which only assisted in generating authentication key for participants. Ljunggren et al. [27] also proposed some schemes of authority-based user authenticated QKD on jammable public channels between communicators. Later, some specific quantum applications, such as quantum direct communication (QDC) [28], blind quantum computation (BQC) [29], etc. also gradually concerned about participants' identity authentication via TTP's assistances. In addition, message authentication which ensures data source authentication and integrity protection is also indispensable. In 2001, Marcos et al. [30] proposed a quantum authentication method of classical messages, which selected an entanglement state as the authentication key to implement quantum message authentication code (QMAC). Xin et al. [31] proposed an embodied version of QMAC via a shared key and two public unitary operations.

This work is to reinforce the security of the existing QKD-based QPQ protocol by integrating authentication mechanism, the contributions are as follows.

(1) In the oblivious key agreement phase, a two-way identity authentication is implemented to resist impersonation and man-in-the-middle attacks and generate a shared key between data user Alice and database owner Bob.

(2) In the data retrieval phase, the data sending process from Bob to Alice is accompanied by quantum message authentication based on the above shared key to achieve the data source authentication and integrity protection against tampering attacks .

(3) The proposed protocol not only retains the privacy protection strength of the original QPQ protocol, but also has strong resistance to external attacks.

The rest of this article is arranged as follows. In Sect. 2, we will briefly review the J-protocol. In Sect. 3, the specific process of QPQ protocol with authentication is given. Section 4 is contributed to provide security analysis of the proposed scheme. Finally, a summary is given in Sect. 5.

2 Review of J-protocol

J-protocol is the first QKD-based QPQ protocol. Suppose that Bob possesses a database of N items, and Alice wants to purchase one of them, the process of J-protocol includes the following eight phases.

(1) Bob sends a long random string of qubits in states $(|0\rangle, |1\rangle, |+\rangle, |-\rangle)$ to Alice. Here, $|0\rangle$ and $|1\rangle$ represent bit 0, while $|+\rangle$ and $|-\rangle$ code for 1.

(2) For each qubit received by Alice, she measures it randomly in basis Z or X.

(3) Alice announces which instances she has detected successfully, and both sides should disregard all of the lost photons.

(4) For each qubit that Alice has successfully measured, Bob announces a pair of states, one of which is the quantum state he has been sent and the other is randomly selected from the other basis. For instance, Bob will declare $\{|+\rangle, |0\rangle\}$ or $\{|+\rangle, |1\rangle\}$ at random if the sent state is $|+\rangle$.

(5) Alice deduces her measurement results in step 2. According to her measurement results and Bob's declaration, Alice can obtain the sent bit with a certain probability. Alice and Bob now share a raw key K^r which is known completely to Bob and partly to Alice.

(6) Alice and Bob divide the raw key into k substrings of length $N(k$ is a security parameter, N is the number of items in the database), and these strings are added bitwise, obtaining the final key K^f with length N. So far, Bob knows the the whole key K^f and Alice knows it roughly 1 bit.

(7) After step 6, the protocol has to restart if Alice is left with no known bit.

(8) Bob encodes the database and Alice decodes it to get the data she needs. If K^f has been established correctly, assume Alice knows the jth bit K^f_j and wants the ith item of the database X_i. She then announces a shift value $s = j - i$ so that Bob can shift K^f by s and send N bits $C_n = X_n \oplus K^f_{n+s}$ to Alice, where Alice can read $C_i = X_i \oplus K^f_j$ and thus obtain X_i .

3 The proposed scheme

In this section, the J-protocol is used as an example of the basic QKD-based QPQ protocol to illustrate our scheme. In fact, our proposed scheme is also applicable to other similar QPQ protocols.

3.1 The security assumptions and goals

(1) TTP is fully trusted. There is a significant assumption in the proposed protocol, TTP and Alice share at some instant a secure channel(where the transmitted information is privacy and integrity), the same is true for TTP and Bob. Note that the channel is open only once, it merely used for Alice and Bob to secretly register their identities with the TTP. There is no such secure channel between Alice and Bob. TTP, his role is to simply perform unitary operations according to communicators' identity and publish what operations he has done in the procedure of authentication.

(2) The data user Alice is untrusted. She always wants more information than she bought, and she is an authorized user of the database, but may be impersonated.

(3) The database owner Bob is semi-trusted. He sells real data to users for her reputation, but he is interested in user preferences. He is a legitimate database owner, but may be impersonated.

Our goals are to guarantee the privacy of user and database under cheat-sensitive strategy and the security of all communication processes against external active attacks.

A QPQ protocol can be divided into two phases, the oblivious key agreement phase and data retrieval phase. In different phases, the purpose of authentication is different. In the first phase, the two-way identity authentication is needed, and in the second phase, the message authentication is implemented.

3.2 The oblivious key agreement with identity authentication

Assume that Bob possesses a database $\left\{x_1, x_2, \ldots, x_Q\right\}$ of Q items, and Alice wants to purchase one of them.

Step 1: Registration with TTP. Bob and Alice send TTP their random generated identities $ID_B = \left\{id_1^B, id_2^B, \ldots, id_{\mathrm{N}}^B\right\}$ and $ID_A = \left\{id_1^A, id_2^A, \ldots, id_{\mathrm{N}}^A\right\}$ $\left(id_i^* \in \{0, 1\}, * \in \{\mathrm{B}, \mathrm{A}\}, i = 1, 2, \ldots, N\right)$ $(N > Q)$ to secretly register the system via the secure channel.

Step 2: Bob prepares qubits. Bob randomly chooses a subset $V = \{v_1, v_2 \ldots v_{\mathrm{N}}\}$ from the position set $P = \{1, 2, \ldots, M\}$ and prepares a random sequence of M qubits. The qubits in the position V will be used for authentication and the shared key agreement, called $AUTH$ qubits; For the remaining $M - N$ positions, the prepared qubits will be used for the oblivious key agreement, called $QUERY$ qubits. The two types qubits are selected from BB84 states ($|0\rangle, |1\rangle, |+\rangle, |-\rangle$) according to following rules. For the $AUTH$ qubits, Bob randomly chooses $|0\rangle$ or $|1\rangle$ if $id_i^B = 0$, otherwise he chooses $|+\rangle$ or $|-\rangle$. The $QUERY$ qubits are completely random. Afterward, Bob sends all the qubits to TTP sitting midway between Bob and Alice.

Step 3: TTP performs unitary operations. Bob publishes the positions of $AUTH$ qubits after TTP received all the qubits. TTP applies an unitary operation $U = \{X, I\}$ on each $AUTH$ qubit as follows, $U_i = X$ if $id_i^A = id_i^B$; if not $U_i = I$. Note that TTP will not measure them, otherwise he may be considered as an attacker. Subsequently, TTP sends all the qubits to Alice.

Step 4: Alice measures qubits. Alice measures each received $QUERY$ qubit randomly in basis Z or X. Besides, for each received $AUTH$ qubit, Alice measures it in Z basis if $id_i^A = 0$; or else she measures it in X basis. Alice announces which instances she has detected successfully, and both sides should disregard all of the lost qubits.

Step 5: Identity authentication. For $AUTH$ qubits, Alice and Bob respectively select a different position subset A and B of size l, and exchange the information of quantum states according to the rules of BB84, that is, if the quantum state is $|0\rangle$ or $|+\rangle$, declares 0, otherwise, claims 1. Afterward, TTP declares what he has done on each $AUTH$ qubit.

At this point, Alice and Bob can achieve the following goals.

(1) Implementing two-way identity authentication and obtaining a shared key

Table 1 gives a specific explanation of the identity authentication process and shows that there is a definite correlation between the quantum state prepared by Bob and Alice's measurement result at the position where they both have the same identity bit (i.e., $id_i^A = id_i^B$). That is, if $id_i^A = id_i^B = 0$, the quantum state that Bob prepares is $|0\rangle$ (or $|1\rangle$), after TTP performs the unitary operation X, the measurement result of Alice should be $|1\rangle$ (or $|0\rangle$); if $id_i^A = id_i^B = 1$, the quantum state that Bob prepares is $|+\rangle$ (or $|-\rangle$) and the measurement result of Alice should be $|+\rangle$ (or $|-\rangle$).

The identity authentication can be performed based on the definite correlation. Next, we will explain how Bob authenticates Alice (Alice authenticates Bob in the same way).

a) For Alice and the selected set A, Bob first finds out the positions where TTP's operation is X (i.e., $id_i^A = id_i^B$);

b) Bob compares the initial quantum states in these positions and Alice's declarations one by one, and if all the results are correct, Bob authenticate Alice successfully, other wise, as long as there is an incorrect result, the authentication falls. For example, if the initial quantum state is $|0\rangle$ (or $|1\rangle$), Alice's declaration must be 1 (or 0); if the initial quantum state is $|+\rangle$ (or $|-\rangle$), Alice's declaration must be 0 (or 1).

In addition, for the unannounced $AUTH$ states in the positions where TTP performed the unitary operation X (i.e., $id_i^A = id_i^B$), Alice can infer the initial states that Bob prepared and Bob can also infer the measurement results of Alice. Based on the shared secret, Alice and Bob can share a key, denoted as K_s, which will be used to protect the oblivious key agreement process and calculate the quantum message authentication code in data retrieval phase. As shown in Table 1, if at some positions where TTP's operation is X, Alice's measurement results are $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, she can infer the initial quantum states of these positions are $\{|1\rangle, |0\rangle, |+\rangle, |-\rangle\}$ and the shared key can be 1001.

After the end of the authentication process, Alice and Bob can also deduce each other's identities ID_B and ID_A according to TTP's operations. ID_A, ID_B and K_s are used together to calculate message authentication key in the data retrieval phase.

(2) Obtaining the oblivious retrieval key

After the successful identity authentication, Alice and Bob implement a security oblivious retrieval key agreement process by running step 4 to step 8 of J-protocol and encrypting Bob's announcement in step 4 with the shared key K_s. So far, Bob and Alice can obtain the final retrieval key K^f with length Q, which is known completely to Bob and roughly 1 bit to Alice.

3.3 The data retrieval with message authentication

Bob encrypts the database of Q items into $C = \left\{c_1, c_2, \ldots, c_i, \ldots, c_Q\right\}$ by bitwise adding K^f shifted by $s = j - i$ (suppose Alice knows the jth bit key and wants the ith bit of the database), that is, $c_q = x_q \oplus K_{q+s}^f$, K_{q+s}^f is the qth bit of key K^f shifted by s . Different from J-protocol, the proposed protocol adds a message authentication process which references to the quantum message authentication code (QMAC) pattern in Ref. [30,31] to ensure the integrity of data returned by Bob. The detail retrieval process with message authentication is as follows.

Table 1 Specific identity authentication process

(id_i^A, id_i^B)	Qubits sent by Bob	TTP's operation and results	Alice's measurement bases and results	Alice's declaration	Bob's declaration
(0, 0)	$\|0\rangle$	X,$\|1\rangle$	Z,$\|1\rangle$	1	0
	$\|1\rangle$	X,$\|0\rangle$	Z,$\|0\rangle$	0	1
(0, 1)	$\|+\rangle$	I,$\|+\rangle$	$Z, \|0\rangle\ or \|1\rangle$	$0\ or\ 1$	0
	$\|-\rangle$	I,$\|-\rangle$	$Z, \|0\rangle\ or \|1\rangle$	$0\ or\ 1$	1
(1, 0)	$\|0\rangle$	I,$\|0\rangle$	$X, \|+\rangle\ or \|-\rangle$	$0\ or\ 1$	0
	$\|1\rangle$	I,$\|1\rangle$	$X, \|+\rangle\ or \|-\rangle$	$0\ or\ 1$	1
(1, 1)	$\|+\rangle$	X,$\|+\rangle$	X,$\|+\rangle$	0	0
	$\|-\rangle$	X,$-\|-\rangle$	X,$\|-\rangle$	1	1

Table 2 Generation of $|a_i\rangle$

c_i s_i	0	1
0	$\|a_i\rangle = \|\varphi_0\rangle$	$\|a_i\rangle = \|\varphi_1\rangle$
1	$\|a_i\rangle = \|\psi_0\rangle$	$\|a_i\rangle = \|\psi_1\rangle$

Table 3 Generation of $|t_i\rangle$

s_{i+1}	$\|t_i\rangle$
0	$U_0\,\|a_i\rangle$
1	$U_1\,\|a_i\rangle$

Table 4 Measurement basis of $|t_i\rangle$

s_i s_{i+1}	0	1
0	$\{U_0\,\|\varphi_0\rangle\,, U_0\,\|\varphi_1\rangle\}$	$\{U_0\,\|\psi_0\rangle\,, U_0\,\|\psi_1\rangle\}$
1	$\{U_1\,\|\varphi_0\rangle\,, U_1\,\|\varphi_1\rangle\}$	$\{U_1\,\|\psi_0\rangle\,, U_1\,\|\psi_1\rangle\}$

Step 1: Authentication key calculation. According to TTP's declaration in step 5 of Sect. 3.2, Alice and Bob could accurately deduce the other party's identity strings ID_B and ID_A with N bits (note that the legal participants' identity strings should be updated after each communication), they have also obtained a shared key K_s less than N bits. Alice and Bob extend K_s to N bits key $K_s^{'}$ using the shared key orderly and repeatedly. Then, the N bits message authentication key is $k = ID_A \oplus ID_B \oplus K_s^{'} = \{s_1, s_2, \ldots, s_i, s_{i+1}, \ldots, s_N\}$ ($\oplus$ is modular 2 arithmetic).

Step 2: quantum message authentication code (QMAC) generation. As in Ref. [31], Bob and Alice publicly select two unitary quantum operations U_0, U_1 in advance, which must satisfy the following conditions.

Suppose $|v\rangle$ is an arbitrary quantum states.

(1) $|U_0|\,v\rangle\left\langle v\left|U_0^{+} + U_1\right|v\right\rangle\!\left\langle v\left|U_1^{+}\right| \neq 0\right.$.

(2) Let an attacker cannot find a unitary operation U_e to make $\left\langle v\left|U_i^{+}U_eU_i\right|v\right\rangle = 0, i = 0, 1$.

(3) $\left\langle v\left|U_0^{+}U_1\right|v\right\rangle \neq 0$.

According to the message authentication key k and the two unitary operations U_0, U_1, Bob transforms the encrypted database $C = \left\{c_1, c_2, \ldots, c_i, \ldots, c_Q\right\}$ into Q pairs of qubits $\left\{(|a_1\rangle, |t_1\rangle), (|a_2\rangle, |t_2\rangle), \ldots, (|a_i\rangle, |t_i\rangle), \ldots, \left(\left|a_Q\right\rangle, \left|t_Q\right\rangle\right)\right\}$, where each data bit c_i is associated with a pair of qubits $(|a_i\rangle, |t_i\rangle)$, the first qubit is the quantization of c_i, the later is the relevant tag, Tables 2 and 3 show the specific method, In Table 2, Where $(|\varphi_0\rangle, |\varphi_1\rangle, |\psi_0\rangle, |\psi_1\rangle)$ are arbitrary quantum states, and $\langle\varphi_0 \mid \varphi_1\rangle = 0$, $\langle\psi_0 \mid \psi_1\rangle = 0$.

Step 3: Verification and Obtaining query data. For better security, Alice will verify each pair of received qubits $(|a_i\rangle, |t_i\rangle)$, even if she only buy one bit of the database. Only when all the pairs have passed the verification, can Alice accept the data item that she buys. The verification process is as follows.

(1) Decoding the first qubit $|a_i\rangle$ to gain the original classical query message ciphertext c_i. According to her key bit s_i and Table 1, if $s_i = 0$ ($s_i = 1$), Alice measures $|a_i\rangle$ under $\{|\varphi_0\rangle, |\varphi_1\rangle\}$ ($\{|\psi_0\rangle, |\psi_1\rangle\}$) basis and if the measurement result is $|\varphi_0\rangle$ ($|\psi_0\rangle$), gets $c_i = 0$, else if concludes $c_i = 1$.

(2) Checking the validity of the qubit $|t_i\rangle$. According to the key bit s_i and s_{i+1}, Alice performs an measurement on $|t_i\rangle$ using the orthogonal basis chosen from Table 4 and judges whether the equation $|t_i\rangle_{\text{measure}} = U_{S_{i+1}} |a_i\rangle_{\text{measure}}$ is true, where $|t_i\rangle_{\text{measure}}$ and $|a_i\rangle_{\text{measure}}$ are the measurement results of $|t_i\rangle$ and $|a_i\rangle$, respectively. If the result is true, the message authentication is successful, otherwise, the authentication fails. After Alice successfully verifies $(|a_i\rangle, |t_i\rangle)$, she gets the correct c_i and decrypts it by calculating $x_i = c_i \oplus K_j^f$ to obtain the data item x_i that she wants to buy.

4 Security analysis

The proposed protocol is a security enhanced version of QKD-based QPQ protocol by integrating the identity and message authentication into the existing protocol. Therefore, the proposed protocol has the same level of privacy of database and user as the existing protocol. In this section, we mainly analyze the security of the proposed protocol against external attacks, including impersonation, man-in-the-middle and tampering attacks.

4.1 Security of the oblivious key agreement phase

4.1.1 Impersonation attack

A. Eve impersonates Alice

The unauthorized Eve wants to impersonate the authorized Alice for accessing to Bob's data. Suppose that Eve knows how the protocol works. By public information, Eve can exactly knows which particles are $AUTH$ qubits. There are three possible attack strategies for Eve.

(1) Eve intercepts all the particles sent to Alice and replaces Alice for identity authentication and oblivious key agreement.

When Eve receives each $AUTH$ qubit from Bob via TTP's associated manipulation, to make the agreement looks normal, he needs to publish a bit string R corresponding to a position subset A' and claim that it is the measurement results of $AUTH$ qubits on A'. Since Eve does not know Alice's identity ID_A, he can only determine the value of the bit string R randomly. Let the size of set A' be H. In probability, half of TTP's operations should be X, that is, in $\frac{H}{2}$ positions, the corresponding bit values of ID_A and ID_B should be equal. Obviously, at every such position, the probability that Eve successfully passes the Bob's detection is $\frac{1}{2}$. Eve can bypass the identity authentication only if Bob's detection is successful at all $\frac{H}{2}$ positions. Therefore, the probability that Eve succeed is $\left(\frac{1}{2}\right)^{\frac{H}{2}}$ and as long as H is large enough, Eve cannot carry out the impersonation attack without being detected.

(2) Eve only intercepts the $QUERY$ qubits, sends fake $QUERY$ qubits to Alice, and then takes over the session after Alice is successfully authenticated.

Since Eve exactly knows which particles are $AUTH$ qubits, he cleverly intercepts only $QUERY$ qubits and regenerates fake $QUERY$ qubits to Alice. In such a situation, the identity authentication would be successful. However, Eve has no the shared key K_s and thus he cannot get any information about the encrypted Bob's announcement of the states of the $QUERY$ qubits in step 4 of J -protocol. Therefore, from Eve's point of view, the states of the $QUERY$ qubits are completely random and the oblivious key keeps secret from him. Furthermore, because Alice does not receive the correct $QUERY$ qubits, the J-protocol will go wrong and restart.

(3) Eve intercepts all the qubits. He keeps $QUERY$ qubits for himself and sends fake $QUERY$ qubits to Alice, while sends the $AUTH$ qubits that have been measured or entangled to Alice. That is, Eve carries out measurement-and-resend attack or entangle-and-measurement attack on the $AUTH$ qubits.

Obviously, the purpose that Eve carries out the attack strategy is to expect some information about Alice's identity ID_A and impersonate Alice for the oblivious key agreement. Because Eve does not have information about the initial states of the $AUTH$ qubits, he can only measure the intercepted these qubits with randomly selected bases. Consequently, the measurement-and-resend attack causes Alice to receive the false authentication qubits, which breaks the association between and loaded on the authentication quantum by TTP, and each one-way authentication will fail with a probability of $1-\left(\frac{1}{2}\right)^{\frac{H}{2}}$ and the protocol will abort.

The identities ID_A and ID_B are randomly selected and used only once and Eve has no information about ID_A and ID_B, thus from Eve's view of point, the identity authentication process is essentially similar to BB84. As in Ref. [32], it shows that entangle-and-measurement attack would not occurs successfully for BB84. Therefore, Eve cannot obtain Alice's identity information and the attack strategy degenerates into the strategy (2).

Overall, the identity authentication mechanism of the proposed protocol can prevent unauthorized users from accessing database by impersonating an authorized user.

B. Eve impersonates Bob

If Eve can successfully impersonate Bob, he may sell the fake data to users for money or other purposes. Like impersonating Alice, Eve can use similar strategies to impersonate Bob. Since Eve has no knowledge about Bob's identity ID_B and the states of $AUTH$ qubits are determined by ID_B, compared with impersonation Alice, Eve will not have more advantages if he impersonates Bob.

4.1.2 "Man-in-the-middle" attack

The malicious Eve sits midway between Alice and Bob, he attempts to simultaneously establish communications with Alice and Bob for obtaining the retrieval key K_r^{AE},K_r^{BE} respectively. After that, Eve not only can impersonate Alice to unauthorizedly obtain data from the database provider but also impersonate Bob to provide fake information to the data purchaser.

Eve can establish the retrieval key with the participants only if he is authenticated by both Alice and Bob. The effective strategy by which Eve can pass the mutual authentication is that knows ID_A and ID_B. Actually, the identity strings of Alice and Bob ID_A and ID_B merely leaked out to legal participants. Alice and Bob can deduce the identity of the opposite side according to their own identity and TTP's declarations which are based on the correlation of the identity of legal participants. In other words, Eve can never obtain the information of ID_A and ID_B only according to existing public information(TTP's unitary operations and the encoding of quantum states in Sect. 3.2 step 5). Besides, the analyses in Sect. 4.1.1 demonstrate that Eve cannot carry out the impersonation attack without being detected. On the other hand, on account of legal participants' identity strings will be updated after each communication, the information of ID_A and ID_B has no advantage for legal participants in the next communication. Consequently, the proposed protocol can prevent "man-in-the-middle" attack.

4.2 Security of the data retrieval phase

In the proposed protocol, a data purchaser can verify the source and integrity of message of database owner by the shared key K_s and two publicly selected unitary quantum operations U_0, U_1. The security of the oblivious key agreement phase assures that only Alice and Bob know the shared key K_s. The security of the message authentication has been proved in Ref. [30,31] if the two public selected unitary operations U_0, U_1 satisfy the conditions listed in step 2 of Sect. 3.3.

5 Conclusion

In this paper, we propose a security enhanced version of QKD-based QPQ protocol by integrating the identity and message authentication into the existing protocol. Compared with the original QPQ protocol, the presented protocol cannot only remain the same level of privacy but also resist identity impersonation, "man-in-the-middle", message forging and tampering attacks from external malicious adversaries. The restrictions of this scheme are the introduction of TTP, and the secure channel assumption between TTP and participants. In the future work, we can consider entangled resources to solve the above problems.

References

1. Gertner, Y., Ishai, Y., Kushilevitz, E., Malkin, T.: Protecting data privacy in private information retrieval schemes. J. Comput. Syst. Sci. **60**(3), 592–629 (2000)
2. Chor, B., Goldreich, O., Kushilevitz, E., Sudan, M.: Private information retrieval. In: Proceedings of Foundations of Computer Science, pp. 41–50 (1995)
3. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A. **56**(2), 1154–1162 (1997)
4. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries. Phys. Rev. Lett. **100**(23), 230502 (2008)
5. Martini, F.D., Giovannetti, V., Lloyd, S., Maccone, L., Nagali, E., Sansoni, L., Sciarrino, F.: Experimental quantum private queries with linear optics. Phys. Rev. A. **80**(1), 010302 (2009)
6. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum private queries: security analysis. IEEE Trans. Inf. Theory **56**(7), 3465–3477 (2010)
7. Olejnik, L.: Secure quantum private information retrieval using phase-encoded queries. Phys. Rev. A. **84**(2), 022313 (2011)
8. Jakobi, M., Simon, C., Gisin, N., Bancal, J.D., Branciard, C., Walenta, N., Zbinden, H.: Practical private database queries based on a quantum-key-distribution protocol. Phys. Rev. A. **83**(2), 773–781 (2011)
9. Scarani, V., Acin, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**(5), 057901 (2004)
10. Gao, F., Liu, B., Wen, Q.Y.: Flexible quantum private queries based on quantum key distribution. Opt. Express. **20**(16), 17411–17420 (2012)
11. Panduranga Rao, M.V., Jakobi, M.: Towards communication-efficient quantum oblivious key distribution. Phys. Rev. A. **87**(1), 012331 (2013)
12. Gao, F., Liu, B., Huang, W., Wen, Q.Y.: Postprocessing of the oblivious key in quantum private queries. IEEE. J. Sel. Top. Quant. **21**(3), 6600111 (2015)
13. Liu, B., Gao, F., Huang, W., Wen, Q.Y.: QKD-based quantum private query without a failure probability. Sci. China Phys. Mech. Astron. **58**(10), 100301 (2015)
14. Maitra, A., Goutam, P., Sarbani, R.: Device-independent quantum private query. Phys. Rev. A. **95**(4), 042344 (2017)
15. Wei, C., Cai, X., Liu, B.: A generic construction of quantum-oblivious-key-transfer-based private query with ideal database security and zero failure. IEEE Trans. Comput. **67**(1), 2–8 (2018)
16. Chan, P., Lucio-Martinez, I., Mo, X.: Performing private database queries in a real-world environment using a quantum protocol. Sci. Rep. **4**(23), 5233 (2014)
17. Yang, Y., Liu, Z., Chen, X., Zhou, Y., Shi, W.: Robust QKD-based private database queries based on alternative sequences of single-qubit measurements. Sci. China Phys. Mech. Astron. **60**(12), 120311 (2017)
18. Wei, C.Y., Cai, X.Q., Wang, T.Y., Qin, S.J., Gao, F., Wen, Q.Y.: Error tolerance bound in QKD-based quantum private query. IEEE J. Sel. Areas Commun. **38**(3), 517–527 (2020)
19. Yang, Y.G., Sun, S.J., Tian, J., Xu, P.: Secure quantum private query with real-time security check. Opt. Int. J. Light Electron Opt. **125**(19), 5538–5541 (2014)
20. Wei, C.Y., Wang, T.Y., Gao, F.: Practical quantum private query with better performance in resisting joint-measurement attack. Phys. Rev. A. **93**(4), 042318 (2016)
21. Xiao, M., Zhang, D.F.: Practical quantum private query with classical participants. Chin. Phys. Lett. **36**(3), 030301 (2019)
22. Gao, X., Chang, Y., Zhang, S.: Quantum private query based on bell state and single photons. Int. J. Theor. Phys. **57**(7), 1983–1989 (2018)
23. Zheng, T., Zhang, S., Gao, X.: Practical quantum private query based on Bell state. Mod. Phys. Lett. A **34**(24), 1950196 (2019)
24. Yang, H., Xiao, M.: Multi-user quantum private query. Quantum Inf. Process. **19**, 253 (2020)
25. Gao, F., Qin, S.J., Huang, W., Wen, Q.Y.: Quantum private query: a new kind of practical quantum cryptographic protocol. Sci. China Phys. Mech. Astron. **62**(7), 70301 (2019)
26. Zeng, G., Zhang, W.: Identity verification in quantum key distribution. Phys. Rev. A. **61**(2), 022303 (2000)
27. Ljunggren, D., Bourennane, M., Karlsson, A.: Authority-based user authentication in quantum key distribution. Phys. Rev. A. **62**(2), 022305 (2000)

28. Lee, H., Yang, H.J., Lim, J.: Quantum direct communication with authentication. Phys. Rev. A. **73**(4), 042305 (2005)
29. Li, Q., Li, Z., Chan, W.H.: Blind quantum computation with identity authentication. Phys. Lett. A **382**(14), 938–941 (2018)
30. Marcos, C., David, J.S.: Quantum authentication of classical messages. Phys. Rev. A. **64**(6), 062309 (2001)
31. Xin, X., Li, F.: Quantum authentication of classical messages without entangled state as authentication key. Int. J. Multimed. Ubiquitous Eng. **10**(8), 199–206 (2015)
32. Slutsky, B.A., Rao, R.R., Sun, P.C., Fainman, Y.: Security of quantum cryptography against individual attacks. Phys. Rev. A. **57**(4), 2383–2398 (1998)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.