applied sciences

MDPI

Article

Quantum Privacy Query Protocol Based on GHZ-like States

Tingyu Li, Bai Liu * and Jun Zhang

School of Computer Science, Hubei University of Technology, Wuhan 430068, China
* Correspondence: liubai@hbut.edu.cn

Abstract: The rapid development of telemedicine technology has brought great convenience to people's lives. Alongside generating great convenience, protecting patients' privacy has become increasingly important. Therefore, to solve the above problems, this paper proposes a quantum privacy query protocol based on GHZ-like states. The protocol first utilizes existing diagnostic information for classification to encode symptom attributes. Then, the correlation after measurement using GHZ-like entangled states is utilized so that the querying party can only obtain a key message with the assistance of a third party. Through the above operation, the database cannot know the address of the message queried by the querying party, and the querying party is also unable to obtain more information. The protocol not only adds decoy factor detection but also adds the process of authentication while checking for illegal eavesdropping. It makes the protocol sufficiently resistant to joint attacks, participant attacks, and external system credit attacks. This database privacy query protocol ensures that the database service is more effective and its environment is more secure.

Keywords: two-way privacy protection; GHZ-like state; authentication; joint attacks

check for updates

Citation: Li, T.; Liu, B.; Zhang, J. Quantum Privacy Query Protocol Based on GHZ-like States. *Appl. Sci.* **2024**, *14*, 608. https://doi.org/10.3390/app14020608

Academic Editor: Christos Bouras

Received: 30 November 2023
Revised: 6 January 2024
Accepted: 6 January 2024
Published: 10 January 2024

Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Traditional medical diagnosis is based on a physician's medical knowledge, clinical insight, and the ability to integrate and analyze available information. However, experienced doctors will inevitably make mistakes. With the rapid progress of computer and network technology, medical-assisted diagnosis systems have also received significant attention and development [1]. Online medical assistance systems utilize computer technology and artificial intelligence to provide medical advice, diagnosis, and treatment recommendations. These systems, which are usually delivered via the internet or mobile apps, can provide a variety of medical information and support to patients, physicians, and healthcare professionals. Patients can enter their symptoms online, and the system will provide initial medical advice to help them understand a possible disease or health problem. Patients are then given information about diseases, medications, treatments, and health advice to help them better understand and manage their health conditions. According to the literature [2], which combines decision tree and Oblivious Transfer (OT) technology to achieve two-way privacy protection in medical-assisted diagnosis systems, one researcher proposed a decision tree indexing protocol, which can efficiently digitize the decision tree information, thus facilitating the use of OT protocol to protect the client's privacy [3] and at the same time ensuring that the client can only obtain the query related information and not other additional information. However, the security field still faces severe challenges. As technology continues to advance, the rapid development of quantum computing capabilities has become a focus of widespread concern. The rise of this emerging technology has raised significant concerns about information security. The power of quantum computing promises to break some of the classical encryption algorithms currently considered secure, including those widely used in the classical Oblivious Transfer protocol [4].

However, quantum algorithms are becoming increasingly sophisticated, and the security of these schemes based on complicated mathematical assumptions deserves reconsideration. Fortunately, quantum cryptography and quantum mechanical principles can solve

the security problems of classical SPIR schemes [5]. The protocol that deals with these problems using quantum cryptography and quantum mechanics can be called quantum private query (QPQ [6–8]). Quantum private query is a privacy protection technology involving quantum computing, whose goal is to protect the security of users and databases. In 2008, Giovannetti et al. [9] proposed the first QPQ protocol (GLM), and then the security of the protocol is demonstrated through experiments [10]. The GLM protocol has a substantial improvement in safety, and the complexity required for computation and communication shows an exponential decrease. Nevertheless, the GLM protocol is no longer applicable when the database data increases substantially. To accommodate the large databases, Jacobi et al. [11] proposed a QPQ protocol based on quantum key distribution (j-protocol). It is worth noting that in this protocol, the database knows all the keys while the user knows only part of the keys, so it is necessary to dilute the user's known key to almost 1 bit, and this dilution algorithm is called a post-processing algorithm [12]. To make the protocol more flexible, Gao et al. [13] introduced a new parameter θ in the j protocol to make it highly flexible. Quantum states in $\{|0\rangle, |1\rangle, \cos\ \theta|0\rangle + \sin\ \theta|1\rangle, \sin\ \theta|0\rangle - \cos\ \theta|1\rangle\}$ are used in this protocol to realize a more flexible j protocol. Although the security and communication efficiency of the protocol can be changed by adjusting the value of the parameter θ, the quantum resources are not easy to prepare. In 2015, Yang et al. [14] proposed another QPQ scheme using one quantum state. where the database owner sends only one quantum state to the user. This type of protocol requires expensive quantum resources and operations, so it is not very easy to implement. In 2016, Yan et al. [15] proposed a protocol based on two non-orthogonal states. This protocol resists external attacks by failing to accurately distinguish between these two non-orthogonal states. In 2018, Chang et al. [16] proposed a scheme based on EPR pairs and single photons, which is resistant to joint measurement attacks. However, most protocols have a security problem. When the querying party has multiple keys, it can launch a joint measurement attack on the database. So, we need to control the number of keys the querying party obtains strictly.

Therefore, a protocol for privacy queries based on GHZ-like states is now proposed. In our protocol, the number of keys obtained by Alice can be precisely controlled by Charlie, so it is sufficiently resistant to joint measurement attacks. Due to the entangled nature of GHZ-like states, the measurement of one of the quantum bits affects the state of all the remaining particles, so this substantial entanglement property will improve the security of our protocol. Then, our protocol resists attacks from dishonest users by secondary authentication. These designs will make our protocol much more secure.

The organization of this paper is described below. In Section 2, we present some preliminary work on our protocol. In Section 3, we propose a privacy query protocol based on the GHZ-like states. In Section 4, we provide a functional comparison and security analysis. Finally in Section 5, we give the conclusion.

2. Preliminaries

First, we describe the system model and the process of the protocol in detail in Section 2.1. In Section 2.2, we make some security assumptions and some security goals that our protocol needs to achieve. In Section 2.3, the generation process of the GHZ-like states and measurement bases we used is introduced.

2.1. System Model

The participants of the proposed quantum privacy query protocol based on GHZ-like states include Alice, Bob, hospital, and Charlie. In this protocol, Alice acts as a data searcher, Bob is the manager of the quantum database, the hospital provides the necessary data to the quantum database, and Charlie is responsible for creating entangled states and distributing entangled particles. The whole system is modeled in Figure 1.

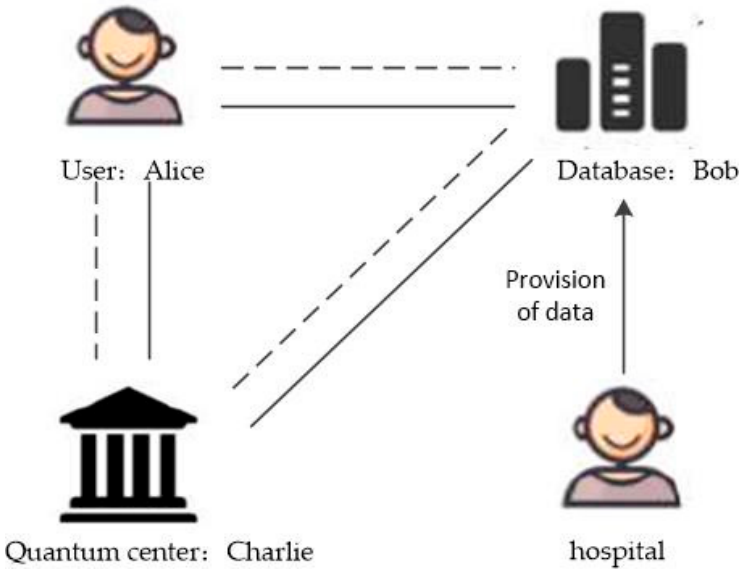


Figure 1. System model.

Quantum privacy query means protecting the security of the user and the database, while our protocol also needs to guarantee the data privacy of the data provider. We first segment the symptom information; then, we create indexes and provide the information to the quantum database. In order to protect the privacy of the data querier and the server, we propose the utilization of class GHZ states for privacy queries. First, Charlie constructs a series of GHZ-like states and distributes the quantum states to Alice and Bob. The user receives the quantum bits and processes them. Bob uses the particles he receives as his key Kb, and Alice obtains one of Bob's items as his key ka through the data he receives and a series of declarations. Alice obtains the data he needs through his key Ka. In this query, Alice can obtain only one key information with the help of Charlie, and Bob cannot know the address of the information queried by the searcher.

2.2. Security Assumptions and Security Objectives

First of all, Charlie is a semi-trustworthy third-party quantum server. Although it is said that Charlie will honestly follow the protocol flow, he is still curious about the privacy of the database and the users. We then assume that the database holder is imperfectly honest and wants information about the specific address that the user is querying. Finally, we assume that the user is not completely honest and that she is interested in obtaining more information about the database.

Based on the above assumptions, our scheme has to satisfy the following security objectives. We do not allow Charlie, external attackers, and user Alice to access more information about the database. Also, we do not allow database Bob, an external attacker, and Charlie to steal the address of the information queried by Alice.

2.3. Three-Particle GHZ-like State

A three-particle GHZ-like state is an abbreviation of three-particle GHZ states [17]. Three particle GHZ-like states can be obtained by using three-particle GHZ states and Hadamard operation [18]. The GHZ-like state is a quantum state with some unique properties that make it essential for applications in quantum information science. GHZ-like states usually include multiple quantum bits, where each quantum bit is in a superposition state, and these superposition states have certain phase relations with each other. Since GHZ-like states possess the property of substantial entanglement, the measurement of one of the quantum bits affects the state of all the remaining particles, and the security of privacy queries can be improved. Also, GHZ-like states possess non-confinement and non-cloning properties, so we can easily detect if an attacker has intercepted the information we send.

Overall, in our privacy query, the GHZ-like states provides a secure key transfer channel for the database and the querier.

The expression formula of the three-particle GHZ-like state is given as follows:

$$|\mathrm{GHZ-like}\rangle_{123} = \mathrm{H_1H_2H_3}|\mathrm{GHZ}\rangle_{123} = \frac{\sqrt{2}}{2}(|+++\rangle + |---\rangle)_{123} = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)_{123} \quad (1)$$

Here,

$$|\mathrm{GHZ}\rangle_{123} = \frac{\sqrt{2}}{2}(|000\rangle + |111\rangle)_{123} \quad (2)$$

$$\mathrm{H} = \frac{\sqrt{2}}{2}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|] \quad (3)$$

Two single-quantum measurement bases:

1. $\{|0\rangle, |1\rangle\}$ is the basis for a standard set of measurements, called $\mathrm{B_z}$, where

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)\ |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) \quad (4)$$

2. $\{|+\rangle, |-\rangle\}$ is the basis for the measurement of another set of standards, called $\mathrm{B_x}$, where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (5)$$

3. Quantum Privacy Query Based on the GHZ-like State

3.1. Creating Indexes

In this part, the hospital constructs an index of the data information and sends it to the quantum database. The data provider first generalizes the data thoroughly to realize the gradual segmentation of the data. Then, the data provider sends all the segmentation schemes and their corresponding probabilities of selected schemes to the quantum database. As shown in Table 1, we divide each symptom into n attributes, and for each attribute data, we have values 0 and 1. The first one is the processing of continuous type numerical data. The patient's temperature attribute TEMP is a continuous numerical data type, and its value domain is [36, 41]. We subdivided Temp into the intervals of [35, 37.8] and (37.8, 41], so we can consider that attribute TEMP has two values: Temp takes the value of 0 when Temp is [35, 37.8]; Temp takes the value of 1 when Temp is (37.8, 41]. The second is the processing of discrete numerical data and textual data. The patient's headache attribute Headaches is textual data, and the value of attribute Headaches is {yes, no}, where we set the value of yes to 1 and no to 0. Thus, the patient can obtain the value of each bit of the binary according to the form of the questionnaire used by the system, etc. Finally the binary number is converted to the index Index according to Equation (6).

$$\mathrm{Index} = 2^0 \times \mathrm{Index}_1 + \cdots + 2^{n-1} \times \mathrm{Index}_n \quad (6)$$

Table 1. Index construction of data information.

	Headaches	**Temp**	**Sniffle**	...	**Diarrhea**	**Vomiting**
000...01	0	0	0	...	0	1
000...10	0	0	0	...	1	0
...	...	...	...	...	...	...
111...10	1	1	1	...	1	0
111...11	1	1	1	...	1	1

3.2. Quantum Privacy Query

Step 1. First, Charlie generates N GHZ-like states and enough non-orthogonal states. These non-orthogonal states are randomly in one of these four states: $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

The GHZ-like states are shown below:

$$|\text{GHZ-like}\rangle_{123} = \frac{1}{2}(|000\rangle + |011\rangle + |110\rangle + |101\rangle)_{123} \tag{7}$$

The footer 123 represents particle 1, particle 2 and particle 3, respectively.

We can also represent the GHZ-like states as a sequence C:

$$C : C_1(1), C_1(2), C_1(3); C_2(1), C_2(2), C_2(3); \ldots; C_n(1), C_n(2), C_n(3) \tag{8}$$

Step 2. First, Charlie generates and announces a binary number R of $r_1 r_2 r_3 \ldots r_n$, where $r_i (1 \leq i \leq n)$ is $C_i(1) \oplus C_i(2) \oplus C_i(3)$. Charlie randomly inserts enough decoy photons $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into the sequence of particles, each randomly in one of four states. Charlie then retains particle 1 in sequence C, assigns particle 2 to Bob, and assigns particle 3 to Alice.

Step 3. When all the particles are released, Alice and Bob publicly announce which particle positions were not successfully received. Then, the three participants will remove the particles from this position together. Alice and Bob will not lie during this step because this step does not reveal any private information, and lying does not benefit Alice and Bob in any way. Then, in order to check whether the entangled particles are safely distributed and the particle releases are listened to, non-orthogonal particles are used for security checking. This is performed as follows: firstly, in Step 2, Charlie randomly inserts enough decoy photons $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ when distributing the particles of sequence C, and each particle is randomly in one of the four states. Secondly, Charlie tells Alice and Bob about the positions of the decoy photons inserted in sequence C and the prepared measurement bases. Then, Alice and Bob use Charlie's information to measure these decoy photons and tell Charlie about the measurement results of these decoy photons. Finally, Charlie determines whether there is a listener or not by comparing the initial state of the decoy photon inserted at the beginning with the measurement results of Bob and Alice. If the error rate is higher than the threshold, there is a listener, and the protocol is terminated, returning to Step 2 and starting again; otherwise, the subsequent protocol continues.

Step 4. Next, Alice, Bob, and Charlie measure the sequence of particles in their hands by the binary number R: $r_1 r_2 r_3 \ldots r_{\mathrm{n}}$, where $r_i (1 \leq i \leq n)$, as shown in Table 2, and record the measurement. At the same time, the particle measured by Charlie is called sequence S1; similarly, the particle retained by the server is called sequence S2; and the particle owned by Alice is called sequence S3.

Table 2. Specific measurement basis.

$r_i = 0$	Z-basis
$r_i = 1$	X-basis

Step 5. At this point, Charlie chooses a GHZ-like state at random, joining Charlie to choose the ith GHZ-like state, and then he secretly tells Alice about this bit and his measurements about this bit.

Step 6. As shown in Table 3, by Charlie secretly telling Alice the above information, Alice can infer the bits of the relative location Bob. Firstly, when the ith bit of the binary number R is 0, the measurement base used is the Z measurement base. If Charlie secretly tells Alice it is $|1\rangle$, Bob and Alice have opposite results, so Alice can infer Bob's measurement result according to her own measurement result. If Charlie secretly tells Alice it is $|0\rangle$, Bob and Alice have the same results, so Alice can infer Bob's measurement result according to her own measurement result. Secondly, when the ith bit of the binary number R is 1, then the measurement base used is the X measurement base. Bob and Alice have the same

result, and Alice can infer Bob's measurement result based on her own measurement result. Alice uses the inferred Bob's measurement result for this state as her own key Ka, and Bob writes down all her measurements as the key Kb.

Table 3. The effect of Charlie's measurements on Alice's and Bob's states.

Measurement Basis	$C_i(1)$	$C_i(2)$	$C_i(3)$
Z-basis	1	1	0
		0	1
	0	1	1
		0	0
X-basis	1	1	1
	0	0	0

Step 7. By the above steps, Bob knows the whole key information while Alice only knows the key information of the *i*th bit sent by Charlie secretly. At this point, Bob uses the shared information to Alice to encode the measurement base for authentication. In the shared data, bit 1 corresponds to measurement base B_x, and bit 0 corresponds to measurement base B_z. Alice generates a set of entangled states, as shown in Equation (9).

$$\left|\Psi_{12}^{+}\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1\langle 1|_2 + |1\rangle_1|0\rangle_2) \tag{9}$$

For each entangled pair, Alice keeps the first particle and sends the other particle to Bob, then Alice measures her own particle using B_z, and after the measurement, the Bell state collapses to $|0\rangle_1$ or $|1\rangle_0$. Bob measures the received particle using a measurement base corresponding to the shared information. Bob then encrypts the estimated information and the information about the particle into a ciphertext and sends the ciphertext to Alice, who decrypts the ciphertext and verifies Bob's identity by comparing the measured information. Finally, Alice sends the decryption result of the ciphertext to Bob, and if the decryption result is correct, then Bob has verified Alice's identity.

Step 8. In the privacy query phase, Alice can measure the information about Bob in bit *i* because Charlie secretly told Alice about the *i*th bit. At this point, Alice knows the key for the *i*th bit k_i, but she wants the *j*th bit k_j of the database. So, Alice will announce the number $s = i - j$. Bob will shift the key kb by s. Then, Bob encrypts the database by the latest key and sent it to Alice. Finally, Bob announces N bits $c_n = x_n \oplus k_{n+s}$, and then Alice can go through $c_j = x_j \oplus k_i$ and thus obtain the information x_j she wants to obtain.

The quantum privacy query based on the GHZ-like states scheme is introduced in detail in the previous section. The role of our protocol is to perform medically assisted diagnosis. First, users can generate an index based on their symptom attributes. Then, they can perform our quantum privacy query. Finally, they will be able to obtain detailed information on disease progression prediction and treatment plan development. For clarity, we describe a schematic to explain the proposed quantum privacy query based on GHZ-like states scheme, as shown in Figure 2.

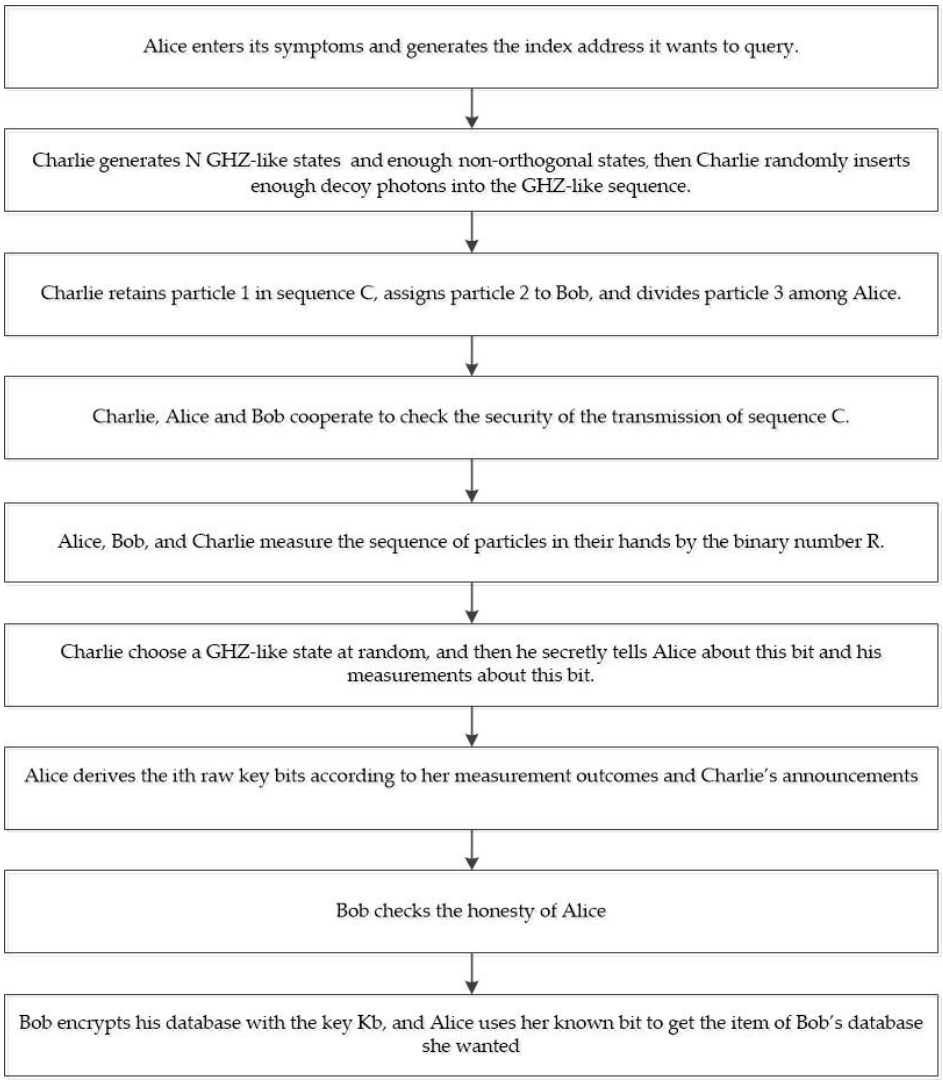


Figure 2. The schematic figure of the proposed quantum privacy query based on the GHZ-like states.

4. Functional Comparison and Security Analysis

In the previous sections, we focused on the content of our protocol and the detailed process with flowcharts. Now, we analyze the functional aspects and security aspects of the protocol. First, we compare the functions of our protocol with some privacy query schemes. Then, we proved that our protocol can resist various attacks.

4.1. Functional Comparison

The references [2,19–21] implement different privacy query schemes. In ref. [2], the privacy protection protocol based on OT is designed for protecting Bob's privacy database, so the user does not know any information other than the type of disease which is corresponding to her symptoms. In addition, the protocol protects the privacy of user Alice, so Bob does not know the address of the specific data which is queried by Alice. But with the development of quantum computing, the traditional encryption algorithms are no longer secure. So, the quantum privacy query came up. There are two main methods for quantum key distribution in quantum privacy query: single particle distribution and entangled state distribution. When we use single-particle distribution for quantum privacy queries, users can still attack our protocol through joint measurements. So, some studies in the literature use EPR for quantum privacy queries, such as the ref. [19], and the user can use specific algorithms and iterative steps to obtain the final key. However, the ratio of the original

keys known by Alice to the whole original key is surprisingly as high as 1/6. So, even if entangled states are used, the number of the key known by Alice is not controlled to 1. In our protocol, we use the entangled nature of GHZ-like states so that Alice can infer the original key from Charlie's statement and the secret messages. In this process, we control the number of keys Alice obtains by controlling the number of bits Charlie sends secretly. Therefore, our protocol is free from JM attacks and has a significant security improvement. In ref. [20], the protocol utilize w-state for privacy query. It can also evade JM attack, but the use of spurious entangled photons by dishonest third parties may pose a threat to the database and the privacy of the user. In comparison, GHZ-like states are easier to fabricate and remain robust for specific noise and interference. So, GHZ-like states are more suitable for quantum privacy queries. In realizing these QKD protocols, we must take into account the key rate, the quantum production cost, and the quantum robustness. What is more important is whether the protocols resist various security attacks.

Compare with the above protocols that our protocol has four functions advantages (in Table 4). Firstly, our protocol uses quantum states which can withstand attacks from quantum computers, just like in the literature [19,20]. Secondly, our protocol adds the detection of illegal eavesdroppers in Step 3. Thirdly, we precisely control the number of keys obtained by the querier in Step 5, which not only sufficiently resists participant's attacks and improves the security but also improves the efficiency of our efficiency of the protocol. Finally, we add authentication in Step 7, which makes our protocol sufficiently resistant to external attackers and improves the security of our protocol to a certain extent. This process not only protects the privacy of user Alice but also protects the privacy of database Bob, so Bob does not know the specific address of the data queried by Alice.

Table 4. Protocol comparisons.

Protocols	Using Quantum States	Quantum Resource	Authentication	Number of Keys for the Querier
Ref. [2]	No	No	No	No
Ref. [19]	Yes	EPR	No	1/6 of the total key number
Ref. [20]	Yes	W states	Unsafe	1
ours	Yes	GHZ-like states	Yes	1

4.2. Security Analysis

To ensure the security of quantum private queries, we need to consider database security and user privacy security. This section analyzes external eavesdropper security, participant attack security, database privacy, and user privacy, respectively. First, we have no need to consider the joint measurement attack because Charlie can precisely control the number of keys obtained by Alice without post-processing. Second, we have no need to consider Charlie's launching entangled auxiliary particles attack [22,23], but we need to consider an attack by an external attacker emitting entangled auxiliary particles. The specific steps of launching an entangled auxiliary particles attack follow. Charlie entangles the prepared auxiliary particles into Bob's particle sequence through the local Missy operation and tries to obtain measurements about Bob by measuring his own additional particles later. However, we perform a secondary authentication in Step 7 in [24], so Charlie still does not have private information and data in the database. In general, we only analyze attacks on the privacy of Alice and Bob. So, our protocol also has the possibility of attacks on auxiliary systems and attacks within the participants during the query process. We will analyze these two aspects of security.

4.2.1. Security against an Outside Eavesdropper

As shown in Figure 3, we assume that an external attacker can intercept the particles Charlie distributes to Bob and Alice and then entangle the particles Charlie distributes

to Bob and Alice with $|E\rangle = \{|E_1\rangle, |E_2\rangle, |E_3\rangle, \ldots, |E_i\rangle, \ldots\}$. We assume an attack on the particles as follows:

$$U|0\rangle|E_i\rangle = \chi_1|0\rangle|e_{00}\rangle + \chi_2|1\rangle|e_{01}\rangle \tag{10}$$

$$U|1\rangle|E_i\rangle = \chi_3|0\rangle|e_{10}\rangle + \chi_4|1\rangle|e_{11}\rangle \tag{11}$$

$$U|+\rangle|E_i\rangle = \frac{1}{2}[|+\rangle(\chi_1|e_{00}\rangle + \chi_2|e_{01}\rangle + \chi_3|e_{10}\rangle + \chi_4|e_{11}\rangle) + |-\rangle(\chi_1|e_{00}\rangle - \chi_2|e_{01}\rangle + \chi_3|e_{10}\rangle - \chi_4|e_{11}\rangle)] \tag{12}$$

$$U|-\rangle|E_i\rangle = \frac{1}{2}[|+\rangle(\chi_1|e_{00}\rangle + \chi_2|e_{01}\rangle - \chi_3|e_{10}\rangle - \chi_4|e_{11}\rangle) + |-\rangle(\chi_1|e_{00}\rangle - \chi_2|e_{01}\rangle - \chi_3|e_{10}\rangle + \chi_4|e_{11}\rangle)] \tag{13}$$

where $a, b, c, d \in [0, 1]$ and $\chi_1^2 + \chi_2^2 = \chi_3^2 + \chi_4^2 = 1$, $|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle$ are the states that the attacker has to distinguish. If the attacker wants to avoid the security check in step 3, then it must satisfy Equations (14)–(16).

$$\chi_2 = \chi_3 = 0 \tag{14}$$

$$\chi_1|e_{00}\rangle - \chi_2|e_{01}\rangle + \chi_3|e_{10}\rangle - \chi_4|e_{11}\rangle = 0 \tag{15}$$

$$\chi_1|e_{00}\rangle + \chi_2|e_{01}\rangle - \chi_3|e_{10}\rangle - \chi_4|e_{11}\rangle = 0 \tag{16}$$

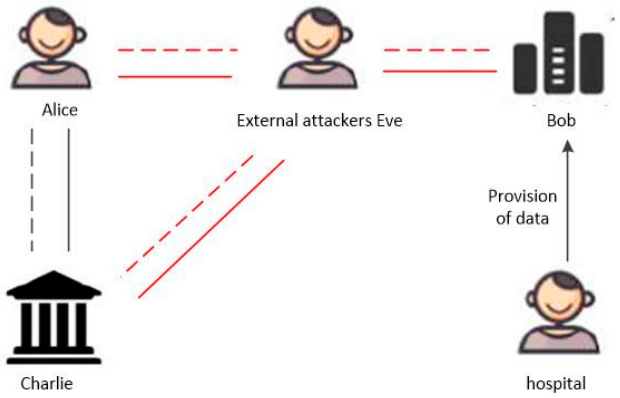


Figure 3. External attacker attack.

From the above equation, we can conclude that $\chi_1|e_{00}\rangle = \chi_4|e_{11}\rangle$; if the attacker wants to avoid the security check in step 3 completely, he cannot distinguish between the two states, $|e_{00}\rangle$ and $|e_{11}\rangle$. So, our protocol can still detect the attack through auxiliary particles.

4.2.2. Security against Participant Attack

In this section, we will discuss the attacks of dishonest participants. Based on our security assumptions and security goal analysis, the untrustworthy user Alice and the database Bob are the primary sources of danger for our protocol, and Charlie is a semi-trustworthy third-party quantum server with no private information. The database is imperfectly honest, and he wants information about the specific address that the user is querying. The user is not completely honest and is interested in obtaining more information about the database. However, the database and user initiate the attack when Charlie distributes the particles of sequence C; then, the database and user will be treated as external eavesdroppers.

1. The first type of participant attack (Database: Bob)

As shown in Figure 4, we analyze that Bob attacks Alice to obtain the address information of the data Alice wants. At this point, Bob must know where Alice knows the

key to accurately deduce the information about the data Alice intends to obtain. Next, we discuss all the attacks that Alice can and will launch. Firstly, Bob is not the generator and distributor of sequence C, so Bob cannot perform the entanglement measurement and the attack of the auxiliary system. Then, the key information that Alice knows is the random bit of information told by Charlie secretly, and Bob is unable to know the specific information in this step. Moreover, Alice is unable to intercept and retransmit the particles in the sequence C sent by Charlie, because the interception retransmission will change the state of the entangled state. There is no way to escape the detection of the decoy particle in step 3 when intercepting the retransmission. Therefore, these attacks are ineffective.

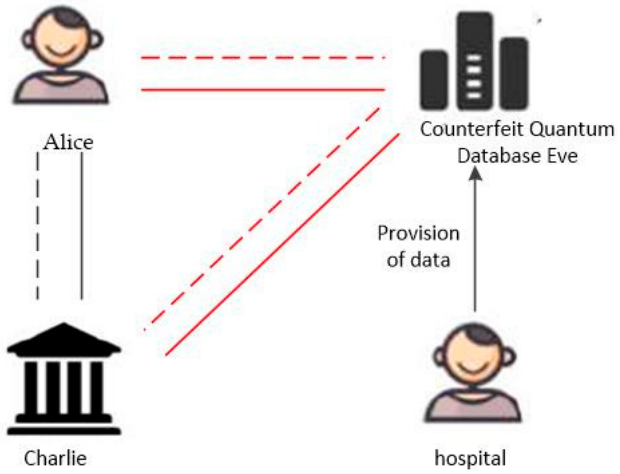


Figure 4. The first type of participant attack (database: Bob).

2. The second type of participant attack (Database: Bob)

As shown in Figure 5, we analyze Alice attacking Bob to obtain more information about the database. Next, we discuss all the attacks that Bob can and will launch. As with the analysis in the previous section, Alice is also incapable of intercepting retransmissions, entanglement measurement, and the attack of the auxiliary system. In our protocol, if Charlie is not secretly telling the measurement base of the *i*th bit and his measurement result, Alice is unable to infer Bob's *i*th measurement, and Alice is also unable to learn the measurement result of any of Bob's other bits. With the above analysis, our protocol is sufficiently resistant to participant attacks.

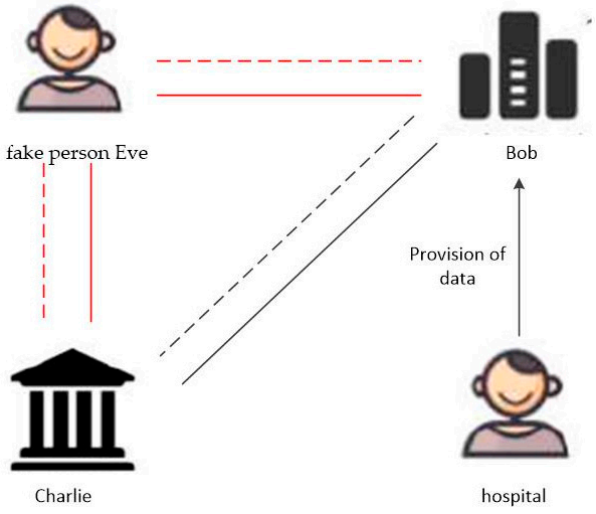


Figure 5. The second type of participant attack (user: Alice).

5. Conclusions

We propose a quantum privacy query protocol based on the GHZ-like states, which solves the following problems. The role of our scheme is to perform medically assisted diagnosis. Bob encrypts the information when he sends it to Alice. Alice uses the obtained key to decrypt the required information. This scheme enables the patient to acquire detailed information about the prediction of disease progression and the development of a treatment plan. In this paper, we propose a quantum privacy query protocol based on GHZ-like states. Compared with the existing QPQ protocols, this protocol has the following differences: first, in our security analysis, we do not consider the joint measurement attack because Charlie can precisely control the number of keys obtained by Alice without post-processing. In Step 3, we add the detection of the decoy factor. The consistency of detection results can help our protocol ascertain whether there is a third-party attack or not. In Step 7, we add authentication. After both the communicating parties have obtained the key, the role of authentication is to prevent unauthorized users or devices from participating in the communication. These are used to enhance the security of the protocol. Moreover, the database and the user's privacy can be sufficiently protected. The performance of our protocol is greatly improved. Then, GHZ, as the largest entangled state, will increase the efficiency and reliability of the quantum information processing process, and it is easy to fabricate and realize. GHZ-like states are easier to fabricate than GHZ states and consume fewer quantum gates. In the actual process of quantum privacy query, the quantum state may be affected by certain noises and interferences, and the GHZ-like states can still maintain its entanglement properties in such an environment. There are still many improvements in the study of quantum privacy queries in this paper, and we need to design a more practical QPQ protocol in combination with practical scenarios.

At the same time, we also need to improve the following questions in the subsequent research. This study can only realize the query of the same data address by multiple users, so how to realize that separate users can retrieve different data addresses at the same time is of great research significance. Based on our single-quantum privacy query, we can go on to explore the entanglement properties of the four-particle GHZ-like states to apply into the multi-user quantum privacy query. Then, our protocol can only retrieve one data address, and in reality, the data are stored in blocks. We need to improve the protocol to make the user retrieve more data information at one time under the security situation. More data information can be obtained. Finally, there is still some improvement in the communication efficiency of our protocol. Future research in quantum privacy querying should improve security while also improving the efficiency of the program to make it better. Of course, we also hope to achieve higher breakthroughs in the subsequent areas.

Author Contributions: This article was prepared through the collective efforts of all the authors. Conceptualization, B.L. and T.L.; methodology, B.L. and T.L.; validation, B.L., T.L. and J.Z.; formal analysis, J.Z.; investigation, J.Z.; resources, B.L.; data curation, J.Z.; writing—original draft preparation, T.L.; writing—review and editing, B.L.; visualization, J.Z.; supervision, B.L.; project administration, B.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China (62002105) and The Key Research and Development Program of Hubei (2021BEA163).

Data Availability Statement: The authors confirm that the data supporting the findings of this study are available within the article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Tang, H.; Huang, H.; Liu, J.; Zhu, J.; Gou, F.; Wu, J. AI-Assisted Diagnosis and Decision-Making Method in Developing Countries for Osteosarcoma. *Healthcare* **2022**, *10*, 2313. [CrossRef] [PubMed]
2. Chen, L.L.; Chen, L.X.; Mu, Y. Two-Way Privacy Protection Method in Medically Assisted Diagnosis System. *J. Cryptologic Res.* **2021**, *8*, 167–182.
3. Naor, M.; Pinkas, B. Efficient oblivious transfer protocols. *SODA* **2001**, *1*, 448–457.

4. Stroh, L.; Horová, N.; Stárek, R.; Puthoor, I.V.; Mičuda, M.; Dušek, M.; Andersson, E. Noninteractive XOR quantum oblivious transfer: Optimal protocols and their experimental implementations. *PRX Quantum* **2023**, *4*, 020320. [CrossRef]
5. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by bothparties. In Proceedings of the 1993 IEEE 34th Annual Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993.
6. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; pp. 175–179.
7. Shi, R.H.; Li, Y.F. Quantum private set intersection cardinality protocol with application to privacy-preserving condition query. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 2399–2411. [CrossRef]
8. Khan, A.; Khalid, U.; Ur Rehman, J.; Shin, H. Quantum anonymous private information retrieval for distributed networks. *IEEE Trans. Commun.* **2022**, *70*, 4026–4037. [CrossRef]
9. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef]
10. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries: Security analysis. *IEEE Trans. Inf. Theor.* **2010**, *56*, 3465–3477. [CrossRef]
11. 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* **2011**, *83*, 022301. [CrossRef]
12. Gao, F.; Qin, S.; Huang, W.; Wen, Q. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 70301. [CrossRef]
13. Gao, F.; Liu, B.; Wen, Q.Y.; Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Express* **2012**, *20*, 17411–17420. [CrossRef]
14. Yang, Y.G.; Zhang, M.O.; Yang, R. Private database queries using one quantum state. *Quantum Inf. Process.* **2015**, *14*, 1017–1024. [CrossRef]
15. Yan, C.; Shibin, Z.; Guihua, H.; Zhiwei, S.; Lili, Y.; Jinxin, X. Quantum private query protocol based on two non-orthogonal states. *Entropy* **2016**, *18*, 163.
16. Gao, X.; Chang, Y.; Zhang, S.B.; Yang, F.; Zhang, Y. Quantum private query based on bell state and single photons. *Int. J. Theor. Phys.* **2018**, *57*, 1983–1989. [CrossRef]
17. Frantzeskakis R, Liu C, Raissi Z, et al. Extracting perfect GHZ states from imperfect weighted graph states via entanglement concentration. *Phys. Rev. Res.* **2023**, *5*, 023124. [CrossRef]
18. Rahman, A.U.; Ji, Z.X.; Zhang, H.G. Demonstration of entanglement and coherence in GHZ-like state when exposed to classical environments with power-law noise. *Eur. Phys. J. Plus* **2022**, *137*, 440. [CrossRef]
19. Yan, C.; Jin, X.X.; Gao, X.; Shibin, Z.; Li, L.Y. Quantum private query protocol based on EPR pairs. *Chin. J. Electron.* **2018**, *27*, 256–262.
20. Zhou, R.G.; Hua, Y. Quantum private query using W state. *Int. J. Theor. Phys.* **2021**, *60*, 2531–2542. [CrossRef]
21. Nurhadi, A.I.; Syambas, N.R. Quantum Key Distribution (QKD) Protocols: A Survey. In Proceedings of the 2018 4th International Conference on Wireless and Telematics (ICWT), Nusa Dua, Indonesia, 12–13 July 2018; pp. 1–5.
22. Sood, S.K. Quantum Computing Review: A Decade of Research. *IEEE Trans. Eng. Manag.* **2023**, 1–15. [CrossRef]
23. Pereg, U.; Deppe, C.; Boche, H. Communication with unreliable entanglement assistance. *IEEE Trans. Inf. Theory* **2023**, *69*, 4579–4599. [CrossRef]
24. Shi, B.S.; Li, J.; Liu, J.M.; Fan, X.F.; Guo, G.C. Quantum key distribution and quantum authentication based on entangled state. *Phys. Lett. A* **2001**, *281*, 83–87. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.