A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment

Wenjie Liu,1,2,3 Peipei Gao,2 Zhihao Liu,3,4 Hanwu Chen,3,4 and Maojun Zhang5,6

1Jiangsu Engineering Centre of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing, China
2School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China
3School of Computer Science and Engineering, Southeast University, Nanjing, China
4Key Laboratory of Computer Network and Information Integration (Southeast University), Ministry of Education, Nanjing, China
5School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin, China
6College of Computer Science and Information Technology, Guangxi Normal University, Guilin, China

Correspondenceshould be addressed to Wenjie Liu; wenjiel@163.com and Maojun Zhang; zhang1977108@sina.com

Received 16 August 2018; Accepted 26 February 2019; Published 1 April 2019

Guest Editor: Yuan Yuan

Copyright © 2019 Wenjie Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cloud computing is a powerful and popular information technology paradigm that enables data service outsourcing and provides higher-level services with minimal management effort. However, it is still a key challenge to protect data privacy when a user accesses the sensitive cloud data. Privacy-preserving database query allows the user to retrieve a data item from the cloud database without revealing the information of the queried data item, meanwhile limiting user’s ability to access other ones. In this study, in order to achieve the privacy preservation and reduce the communication complexity, a quantum-based database query scheme for privacy preservation in cloud environment is developed. Specifically, all the data items of the database are firstly encrypted by different keys for protecting server’s privacy, and in order to guarantee the clients’ privacy, the server is required to transmit all these encrypted data items to the client with the oblivious transfer strategy. Besides, two oracle operations, a modified Grover iteration, and a special offset encryption mechanism are combined together to ensure that the client can correctly query the desirable data item. Finally, performance evaluation is conducted to validate the correctness, privacy, and efficiency of our proposed scheme.

1. Introduction

Cloud computing is a powerful computing paradigm that enables ubiquitous access to shared infrastructure resources and higher-level services. It has shown the remarkable advantage in load balancing, data access control, and resources sharing, for database management [1]. Benefiting from the cloud paradigm, an increasing number of individuals and groups choose to put their massive data (including private part) into the cloud.

In recent years, database outsourcing has become an important component of cloud computing [2], where data owners outsource data management to a service provider (i.e., cloud database), and this mode is also called Database-as-a-Service (DaaS) [3]. Cloud database provides users with capabilities to store and process their data in the cloud, which has the advantages of scalability and high availability that users can access data anytime, anywhere and anyway. However, all the data of data owner is stored in the cloud environment, and some sensitive data (e.g., health records, financial transactions, and personal information) is at risk of being compromised. So, security and privacy have become the major challenges which inhibit the cloud computing wide acceptance in practice [4].

The privacy preservation is the main concern of cloud application, such as service recommendation [5–7], service quality prediction [8, 9], database query [10–16], etc. As an important research branch, the privacy-preserving database query (PPDQ) aims to protect database security and clients’ privacy, while ensuring the correctness of database query. To be specific, any user can query data items from the cloud database without revealing its information, but his/her access to other data items is not permitted. There are a variety of techniques or methods for guaranteeing the privacy...
preservation of database query, such as homomorphic encryption (HE) [10, 11], attribute-based encryption (ABE) [12–14], searchable encryption (SE) [15, 16], etc. Searchable encryption is a cryptographic system which offers secure search functions over encrypted data, which is considered to be a more effective technique to solve the problem of PPDQ. In 2000, Song et al. [15] proposed the first searchable encryption scheme based on symmetric key cryptography (SKC). Since then, other various SE schemes have been continuously proposed, such as public key cryptography-(PKC-) based searchable encryption [17], secure ranked search over encrypted cloud data [18], and so on.

As we all know, the security of classic cryptography protocols, including most private query schemes (also named privacy-preserving database query schemes), is based on mathematical complexity, and its security is based on the fact that computing power is limited. However, with the prevalence of new distributed computing models (especially cloud computing), a normal user is given the super computing power far beyond a single computer. Therefore, these cryptography protocols based on computational complexity are facing serious challenges.

On the other hand, quantum computing demonstrates the superior parallel computing power that the classical paradigm cannot match. For instance, Shor’s algorithm [19] solves the problem of integer factorization in polynomial time, and Grover’s algorithm [20] has a quadratic speedup to the problem of conducting a search through some unstructured database. Therefore, most classic cryptography protocols, including PPDQ schemes, are very vulnerable to the powerful quantum computer. Fortunately, quantum mechanics also provides a security mechanism against quantum attacks, and it holds the potential unconditional security based on some physical properties, such as noncloning theorem, uncertainty principle, quantum entanglement, etc. With the application of quantum mechanics in the field of information processing, some research findings have been proposed, including quantum key distribution [21, 22], quantum secret sharing [23, 24], quantum key agreement [25, 26], quantum direct communication [27, 28], quantum steganography [29], quantum teleportation and state preparation [30–32], quantum sealed bid auction [33, 34], delegating quantum computation [35], and quantum machine learning [36, 37].

With the above observations, the security of classic database query schemes is facing the dual challenge of cloud computing and quantum computing, while quantum mechanics has been proven to be an effective method for solving such problem. In this study, in order to implement the privacy-preserving database query in cloud environment, we utilize some physical properties of quantum mechanics to design a quantum-based database query scheme for privacy preservation (QBDQ) in cloud environment and conduct its performance evaluation to show our scheme is feasible, secure, and efficient. To be specific, our main contributions include the three following aspects.

1) We present a systematic framework for privacy preservation cloud database query scheme in the cloud environment.

2) A feasible QBDQ is designed through oblivious transfer, the offset encryption mechanism, oracle operation, and the modified Grover iteration to achieve the privacy preservation for the cloud database query and reduce its communication complexity.

3) The performance evaluation is conducted to verify the performance of our proposed QBDQ scheme, such as correctness, security, and efficiency.

The rest of this paper is organized as follows. In Section 2, we introduce the basic knowledge of quantum computing, while the framework of the privacy-preserving database query in cloud environment is presented. In Section 3, the problem of privacy-preserving database query in cloud environment is defined, and then the proposed QBDQ is elaborated step by step. Section 4 conducts the performance evaluation from the aspects of correctness, security, and efficiency. After that, Section 5 summarizes the related work on cloud database queries, SE, and quantum private queries. Finally, the conclusion of the paper and the prospect for future work are presented in Section 6.

2. Preliminaries

In this section, the basic knowledge of quantum computing is introduced firstly. Then, we introduced the principle of oblivious transfer (OT). And finally, a cloud computing framework for privacy preservation is designed.

2.1. Quantum Computing

2.1.1. Quantum Bit. The classic bit is the smallest unit in the classic computer, and its value is either 0 or 1. Unlike classical computers, the smallest unit of quantum computers is qubit (quantum bit), which is the quantum analog of the classic bit. A qubit is a unit vector in a two-dimensional complex Hilbert space, and its Dirac notation is represented as follows:

\[ |φ⟩ = α |0⟩ + β |1⟩ , \]

where \( α \) and \( β \) are the probability amplitudes of the state \( |φ⟩ \) and \( |α|^2 + |β|^2 = 1 \). Since the vectors \( |0⟩ \) and \( |1⟩ \) are basis states and can be represented as

\[ |0⟩ = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \]

\[ |1⟩ = \begin{pmatrix} 0 \\ 1 \end{pmatrix} , \]

the qubit \( |φ⟩ \) can be expressed in vector form \( |φ⟩ = (α β) \). In addition, the single qubit can be extended to multiple qubits; for example, an n-qubit system can exist in any superposed basis states

\[ |φ⟩ = α_0 |0⟩ + α_1 |1⟩ + \cdots + α_{2^n-1} |2^n-1⟩ . \]

Here, \( ∑_{i=0}^{2^n-1} |α_i|^2 = 1 \). Quantum states \( |0⟩, |1⟩, \ldots, |2^n-1⟩ \) form a complete orthonormal basis in Hilbert space.
2.1.2. Unitary Operator. In a closed quantum system, the evolution of the system is characterized by a series of unitary operators; that is,

\[ |\varphi\rangle' = U |\varphi\rangle, \]

where \(UU^\dagger = U^\dagger U = I\) and \(U^\dagger\) is the transpose conjugate of \(U\). Each unitary operator corresponds to a quantum gate. Similar to a logic gate in classical calculations, the quantum gate can be represented in matrix form, and the quantum gate over a qubit is represented by a \(2 \times 2\) unitary matrix. For instance, Pauli-\(X\), Pauli-\(Z\), and the Hadamard gate \(H\) are important quantum operators over one qubit described in

\[ X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \]
\[ Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \]
\[ H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \]

2.1.3. Quantum Measurement. The quantum state is in a superposition state, and it must be measured to collapse to a basis state to obtain a result. Assuming that the quantum state is \(|\varphi\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} \alpha_i |i\rangle\) before measurement operator, quantum measurements are described by a collection \(\{M_i\}\) of measurement operators which satisfy the completeness equation

\[ \sum_{i=0}^{N-1} M_i^\dagger M_i = I, \]

where \(i\) indicates the possible outcome of the measurement. The quantum state is measured by the measurement basis \(|i\rangle\), then the probability that result \(i\) occurs is given by

\[ p(i) = \langle \varphi | M_i^\dagger M_i |\varphi\rangle, \]

and the postmeasurement state is

\[ \frac{M_i |\varphi\rangle}{\sqrt{\langle \varphi | M_i^\dagger M_i |\varphi\rangle}}. \]

2.2. Oblivious Transfer. In cryptography, an oblivious transfer (OT) strategy is a type of strategy in which a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred. The first form of oblivious transfer was introduced by Rabin [38]. In this form, the sender sends a message to the receiver with probability \(1/2\), while the sender remains oblivious as to whether or not the receiver received the message. OT is a basic strategy in the field of cryptography and has a wide range of applications. In general, the OT strategy involves two parties, the sender and the receiver, and satisfies the following characteristics:

(i) Whether the queried data can be obtained is entirely dependent on probability, rather than sender or receiver. That is, neither the sender nor receiver can affect the execution of the strategy.

(ii) After the execution of the strategy, the sender could not know whether the receiver got the data he wanted to query.

\(k\)-out-of-\(n\) (\(OT_{k:n}^{\dagger}\) \((k<n)\)) is the general form of all OT strategies. That is, the sender has \(n\) secrets, and the receiver can only get \(k\) secrets. The \(OT_{k:n}^{\dagger}\) strategy consists of two parties, the sender with \(n\) secret data \((d_0, d_1, \ldots, d_{n-1})\), and the receiver with \(k\) indices \((i_1, i_2, \ldots, i_k)\). The strategy meets the following requirements:

(i) Correctness. After executing the strategy, the receiver can obtain all of the \(d_i\) correctly.

(ii) Receiver’s Security. When the receiver queries the data from the sender, the database cannot know the receiver’s query items.

(iii) Sender’s Security. The receiver cannot get more data items from the sender except queried data items.

2.3. The Framework of Privacy-Preserving Database Query in Cloud Environment. We first consider the framework model of privacy-preserving cloud database query system, which consists of two main entities (clients and cloud server) as illustrated in Figure 1.

As shown in Figure 1, there are \(n\) clients and a cloud database server, and every client sends a query request to the cloud server and gets the query result from the cloud server finally. In this framework, we suppose all the clients and server are semihonest: they are curious about cheating the privacy of other’s, but honest to carry out the operations in the scheme. Here, two kinds of entity can be defined as follows.

Client is the entity that wants to query items from the database in the cloud server and can be the connected users.
or the individual user with mobile constrained devices such as smartphones, PDA, TPM chip, etc.

Cloud server is the entity which provides data services and computational resources to the clients dynamically.

In this paper, we take three parties as an example, i.e., the client Alice, client Bob, and the cloud server Charlie, to demonstrate the process of the privacy-preserving database query using quantum mechanics.

3. A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment

In this section, we first define the privacy-preserving database query problem and quantum-based privacy-preserving database query problem in cloud environment. To address this issue, a QBDQ scheme is proposed in detail. Before we introduce the relevant content, the key notations and descriptions used in this section are listed in Table 1.

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>The number of items in cloud server’s database</td>
</tr>
<tr>
<td>D</td>
<td>The cloud server’s database, $D = {D_0, D_1, \ldots, D_{N-1}}$</td>
</tr>
<tr>
<td>$D_i$</td>
<td>The $i$-th data in $D$</td>
</tr>
<tr>
<td>$n$</td>
<td>The number of index qubits used to encode index of data items $n = \lceil \log N \rceil$</td>
</tr>
<tr>
<td>m</td>
<td>The number of qubits used to encode data $D_i$</td>
</tr>
<tr>
<td>$p$</td>
<td>The index of client Alice’s query data</td>
</tr>
<tr>
<td>$D_p$</td>
<td>The data item Alice wants to query from $D$</td>
</tr>
<tr>
<td>q</td>
<td>The index of client Bob’s query data</td>
</tr>
<tr>
<td>$D_q$</td>
<td>The data item Bob wants to query from $D$</td>
</tr>
<tr>
<td>$\Delta s_A$</td>
<td>The offset value of Alice</td>
</tr>
<tr>
<td>$\Delta s_B$</td>
<td>The offset value of Bob</td>
</tr>
<tr>
<td>$K$</td>
<td>The encryption key sequence belongs to Charlie, $K = {K_0, K_1, \ldots, K_{N-1}}$.</td>
</tr>
<tr>
<td>$O_K$</td>
<td>The oracle operation to encode Charlie’s key sequence $K$</td>
</tr>
<tr>
<td>$O_D^A$</td>
<td>The oracle operation to encode Alice’s query result $D_p$</td>
</tr>
<tr>
<td>$O_D^B$</td>
<td>The oracle operation to encode Bob’s query result $D_q$</td>
</tr>
<tr>
<td>$O_p$</td>
<td>The oracle operation which conditionally changes the sign in the amplitudes of the query item $D_p$ ($D_q$)</td>
</tr>
<tr>
<td>$O_q$</td>
<td>The oracle operation which perform a conditional phase shift of $-1$ with every computational base state except $</td>
</tr>
</tbody>
</table>

3.1. Some Definitions. In order to clearly illustrate our scheme, we first define the problem to be solved.

Definition 1 (database query problem for privacy preservation in cloud environment). In the cloud environment, the cloud server has a collection of sensitive data $D = \{D_0, D_1, \ldots, D_{N-1}\}$, and each client wants to query a data item $D_i$ ($0 \leq i \leq N - 1$) from the cloud server without revealing which item is queried. During the retrieving process, the client cannot gain any other data item except $D_i$.

Definition 2 (database query scheme for privacy preservation in cloud environment). Each client inputs the index of query item $i$ ($0 \leq i \leq N - 1$), and cloud server inputs sensitive dataset $D = \{D_0, D_1, \ldots, D_{N-1}\}$. After executing this scheme, the client outputs the queried data item $D_i$. In addition, the scheme should satisfy the following:

(i) Correctness. The client successfully obtains the correct data item he(she) wants to query (i.e., $D_i$).

(ii) Clients’ Privacy. During the retrieving process, the cloud server cannot get any private information about the query index of the client.

(iii) Cloud Server’s Privacy. Clients cannot get any other data items from the cloud server except $D_i$.

3.2. A Quantum-Based Database Query Scheme for Privacy Preservation in Cloud Environment. For the sake of simplicity, we take three parties (one cloud server Charlie, and two clients Alice, Bob) as an example to describe our scheme. Suppose Charlie has a private database $D$ with $N$ items $\{D_0, D_1, \ldots, D_{N-1}\}$ and an encryption key sequence $K = \{K_0, K_1, \ldots, K_{N-1}\}$, and Alice and Bob want to, respectively, query an item, the $p$-th item $D_p$, and the $q$-th item $D_q$ ($0 \leq p, q \leq N - 1$), from server. The scheme consists of five steps as follows (also shown in Figure 2).

Step 1. Charlie prepares an $(n+m)$-qubit state $|\psi_K\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle \otimes |K_i\rangle$, where $n = \lceil \log N \rceil$, $m = \lceil \log(\max[k_i] + 1) \rceil$, and then he applies an oracle operation $O_K$ (its schematic circuit is sketched in Figure 3) on $|\psi_K\rangle$ referring to the sequence $K = \{K_0, K_1, \ldots, K_{N-1}\}$. Here, $O_K$ is defined as follows:

$$O_K: \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |0\rangle \otimes |K_i\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle \otimes |K_i\rangle,$$

where $|i\rangle$ denotes the index of the data item and $|K_i\rangle$ is the encryption key originally assigned to encrypt the $i$-th data item. After the above operation, we can get the state, namely,
Client B (Bob)

Alicecanobtain 𝐾announce the offset 𝐴asameas Alice, Bobalsoperformsthesameoperations and the measurement result is also prepares another state

Alicewithoblivioustransferstrategy. Similarto Alice, Charlie

Step 2. After receiving the same way and sends it to Bob.

Step 3. Having received the offsets 𝐴and 𝐵, and obtains the new key sequence 𝐴and 𝐵,

\[ 𝐾^A = \{ K^A_i \mid 0 ≤ i ≤ N - 1 \} \]
\[ 𝐾^B = \{ K^B_i \mid 0 ≤ i ≤ N - 1 \} . \]

Then, Charlie encrypts every data items respectively with its new corresponding keys 𝐾^A and 𝐾^B as follows:

\[ D^A_i = D_i \oplus K^A_i, \quad 0 ≤ i ≤ N - 1 \]
\[ D^B_i = D_i \oplus K^B_i, \quad 0 ≤ i ≤ N - 1. \]

After that, Charlie prepares two states \( |\psi_D\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩ ⊗ |0⟩^{\oplus m} \), \( |\psi_D\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩ ⊗ |0⟩^{\oplus m} \) and applies the oracle operation \( O^a_D \), \( O^b_D \) as

\[ O^A_D : \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ |0⟩^{\oplus m} → \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ |D^A_i⟩ \]
\[ O^B_D : \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ |0⟩^{\oplus m} → \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ |D^B_i⟩ \]

and gets the final states \( |\psi''\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩ |D^A_i⟩ \), \( |\psi''\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩ |D^B_i⟩ \). Finally, Charlie sends \( |\psi''\rangle \), \( |\psi''\rangle \) to Alice and Bob, respectively, with oblivious transfer strategy.

Step 4. After receiving \( |\psi''\rangle \) from Charlie, Alice performs the modified Grover iteration on it to obtain the target state \( |p⟩ |D^A_p⟩ \). Figure 4 describes the detailed process of modified Grover iteration, which consists of at most \([ (\pi/4) \sqrt{2^{nm}} ]\)
times application of a quantum subroutine, called the G operator. The whole process of G operator (also shown in Figure 5) can be subdivided into four steps as follows.

Step 4.1. Alice applies the oracle operation \( O_s \) on \( |\phi^s⟩ \), which conditionally changes the sign of the amplitudes of the query item

\[
O_s: \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ \left| D^A_i \right> \rightarrow \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right>
\]  

(14)

Here, we call the resultant state \( O_s|\phi''⟩ \), i.e., \( O_s|\phi''⟩ = (1/\sqrt{N}) \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right> \), and \( f(i) \) is the judgment function defined by

\[
f(i) = \begin{cases} 
1, & \text{if } i \text{ is the query address (i.e., } i = p) \\
0, & \text{else (i.e., } i \neq p) 
\end{cases}
\]

(15)

Step 4.2. The Hadamard transformation \( H^{\otimes(n+m)} \) is applied on \( O_s|\phi''⟩ \),

\[
\frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right> \rightarrow H^{\otimes(n+m)} \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right>
\]

(16)

Step 4.3. Alice applies conditionally phase transfer \( O_p \) on the state \( H^{\otimes(n+m)} O_s|\phi''⟩ \),

\[
O_p: H^{\otimes(n+m)} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right> \rightarrow (-1)^{\sigma_{i,D_s}} H^{\otimes(n+m)} \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i⟩ \left| D^A_i \right>
\]

(17)

where the function \( \sigma_{i,D_s} \) is defined as follows:

\[
\sigma_{i,D_s} = \begin{cases} 
1, & i = 0, D_s = 0 \\
0, & \text{else.}
\end{cases}
\]

Step 4.4. The Hadamard transformation \( H^{\otimes(n+m)} \) is applied again on \( O_p H^{\otimes(n+m)} O_s|\phi''⟩ \) and obtains the state

\[
|\xi⟩ = H^{\otimes(2n+m)} O_p H^{\otimes(n+m)} O_s \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i⟩ \left| D^A_i \right>
\]

(19)

Alice applies the above Grover iteration \( [(\pi/4)\sqrt{2^{m+n}}] \) times and finally obtains the target state \( |p⟩ \left| D^A_p \right> \).

Similar to Alice, Bob also applies the modified Grover iteration on the received state \( |\psi''⟩ = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩ \left| D^A_i \right> \) and obtains the target query state \( |q⟩ \left| D^B_q \right> \).

Step 5. Alice and Bob measure the last \( m \)-qubit of state \( |p⟩ \left| D^A_p \right>, |q⟩ \left| D^B_q \right> \) and extract the classic information of query result \( D^A_p, D^B_q \), respectively.

In addition, in order to check eavesdropping in the quantum channel, we can use decoy-photon technology. That is, the sender randomly inserts several decoy photons into the qubit sequence, where every decoy photon is prepared randomly with either Z-basis \{\{0\},\{1\}\} or X-basis \{(1/\sqrt{2})\{0\} + \{1\}\}, \{(1/\sqrt{2})\{0\} - \{1\}\}, and transmits them to the receiver. After confirming that the receiver has received the transmitted sequence, the sender announces the positions of the decoy photons and the corresponding measurement basis. The receiver measures the decoy photons according to the sender’s announcements and tells the sender his (her) measurement results. Then, the sender compares the measurement results from the receiver with the initial states of the decoy photons in the transmitted sequence and calculates the error rate. If the error rate is higher than the threshold determined by the channel noise, they cancel this scheme and restart; else they continue the next step.

It is worth mentioning that we adopted the OT strategy and offset encryption mechanism in our scheme. In Step 3, the OT strategy is utilized to transfer Charlie’s data to Alice and Bob. As we know, the transmitted state \( |\psi⟩ \) is a superposition state which encapsulates all the encrypted data items \( |D_j⟩ \mid 0 \leq i \leq N-1 \). So, the process of Charlie sending \( |\phi'_f⟩, |\psi'⟩ \) to Alice and Bob can be viewed as the oblivious transfer mechanism. The use of OT strategy ensures that information about Charlie cannot be leaked. In addition, our scheme also applied the offset encryption mechanism. The offsets \( \Delta D_A, \Delta D_B \) can be computed by using the index of the query data items and the keys determined by clients’ measurement. Charlie updates the encryption keys according to these offsets and then encrypts data with these updated keys, respectively. The combination of OT strategy and offset mechanism allows Alice and Bob obtain the correct data they want to query, while Charlie cannot get their queried data, which guaranteed the privacy of client. At the same time, data encryption makes the data items into ciphertext, and neither the eavesdropper nor the clients can directly obtain the data item, thus ensuring the data security of the cloud server.

4. Performance Evaluation

Our proposed QBDQ scheme in cloud environment tends to ensure the correctness of query result, protect the privacy of clients and servers in cloud, and also improve the efficiency during querying the cloud database. Therefore, we take three
parties (i.e., clients Alice and Bob; cloud server Charlie) as an example and estimate the overall performance of the proposed scheme in terms of correctness analysis, security analysis, and the efficiency analysis.

4.1. Correctness Analysis. Now, we analyze the correctness of the proposed scheme. Without loss of generality, suppose that the server Charlie has a database of 16 items \( D = \{5, 9, 6, 12, 2, 11, 16, 5, 10, 7, 15, 6, 11, 6, 9\} \), and he holds the corresponding encryption key sequence \( K = \{14, 8, 3, 4, 7, 1, 11, 6, 12, 13, 0, 5, 9, 10\} \). Since \( N = 16 \), the max value in \( K \) is 15, \( n = \lceil \log N \rceil = \lceil \log 16 \rceil = 4 \), \( m = \lceil \log(15 + 1) \rceil = 4 \). Here, we take Alice as an example to analyze the procedures of our QBDQ scheme as follows (suppose Alice wants to query the 9th item of the database).

In Step 1, Charlie prepares an initial state \( |\psi_K\rangle = (1/4)\sum_{i=0}^{15} |i\rangle \otimes |0000\rangle \) and performs an oracle operation \( O_K \) on it to encode his encryption keys,

\[
|\phi^v\rangle = \frac{1}{4} \left( |0\rangle |K_0\rangle + |1\rangle |K_1\rangle + |2\rangle |K_2\rangle \right)
\]

\[
+ |3\rangle |K_3\rangle + |4\rangle |K_4\rangle + |5\rangle |K_5\rangle + |6\rangle |K_6\rangle \\
+ |7\rangle |K_7\rangle + |8\rangle |K_8\rangle + |9\rangle |K_9\rangle + |10\rangle |K_{10}\rangle \\
+ |11\rangle |K_{11}\rangle + |12\rangle |K_{12}\rangle + |13\rangle |K_{13}\rangle \\
+ |14\rangle |K_{14}\rangle + |15\rangle |K_{15}\rangle + |16\rangle |K_{16}\rangle \right) = \frac{1}{4} \left( |0000\rangle + |1100\rangle + |2200\rangle + |3300\rangle \right)
\]

\[
(20)
\]

Then, he sends the resultant state \( |\phi^v\rangle \) to Alice. In Step 2, Alice performs projective measurement on the first four qubits (i.e., index qubits) of \( |\phi^v\rangle \) in the computational basis \{0000, 0001, \ldots, 1111\}. Suppose the random measurement result is \( |12\rangle \) (i.e., \( \lambda_A = 12 \)), then the remaining qubits (i.e., the key qubits) collapse to the state \( |K_A\rangle = |0000\rangle \), which means \( K_A = 0000 \). But the data Alice wants to query is the ninth data \( D_8 \), so she computes the difference between \( \lambda_A \) and the desirable query index \( q, \Delta s = (\lambda_A - q) = 4 \), and sends \( \Delta s \) to Charlie. After receiving \( \Delta s \), Charlie updates the key sequence \( K \) through the formulation \( K_i = K_{(i + \Delta s) \mod N} \), then \( K_A^t = \{7, 1, 11, 6, 15, 2, 12, 13, 0, 5, 9, 10, 14, 8, 3, 4\} \). He uses \( K_A^t \) to encrypt every data items: \( D_i^A = D_i \oplus K_i^A \), that is, \( \{2, 8, 13, 10, 13, 9, 7, 11, 5, 15, 14, 5, 8, 3, 5, 13\} \). Then, in Step 3, Charlie prepares another state \( |\psi_D\rangle = (1/4)\sum_{i=0}^{15} |i\rangle \otimes |0000\rangle \) and applies the oracle operation \( O_D \) to embed the encrypted data items \( D_i^A \):

\[
|\phi''\rangle = \frac{1}{4} \left( |10\rangle |D_0\rangle + |11\rangle |D_1\rangle + |2\rangle |D_2\rangle \right)
\]

\[
+ |3\rangle |D_3\rangle + |4\rangle |D_4\rangle + |5\rangle |D_5\rangle + |6\rangle |D_6\rangle \\
+ |7\rangle |D_7\rangle + |8\rangle |D_8\rangle + |9\rangle |D_9\rangle + |10\rangle |D_{10}\rangle \\
+ |11\rangle |D_{11}\rangle + |12\rangle |D_{12}\rangle + |13\rangle |D_{13}\rangle \\
+ |14\rangle |D_{14}\rangle + |15\rangle |D_{15}\rangle \right)
\]

\[
(21)
\]

Then, he sends the state \( |\phi''\rangle \) to Alice.

Further, Alice performs modified Grover iteration on \( |\phi''\rangle \) up to \( R = \lceil \pi/4 \sqrt{2^{t+m}} \rceil = \lceil \pi/4 \sqrt{2^8} \rceil = 13 \) times (actually, the number of iterations is 6), then she can obtain the encrypted query item \( |p\rangle D_p^A = |5\rangle |8\rangle \) with a high possibility, and measures it to get \( D_p^A = 5 \). Alice uses the obtained key \( K_A^t = 0000 \) to decrypt the ninth item

\[
D_8 = D_8^t \oplus K_A^t = 0101 \oplus 0000 = 0101.
\]

Therefore, regardless of what measurement result Alice has obtained, she can finally obtain the query data correctly.

Figure 6 shows the entire execution process of Alice querying Charlie's database in a simplified way. At the same time, it also sketched the execution of the other user Bob (assuming it queries the fifth data).

4.2. Security Analysis

4.2.1. Privacy Analysis. Cloud Server’s Privacy. Suppose the client Alice is dishonest, and she wants to obtain more information about Charlie’s database. In Step 1 of our
The schematic graph of the execution process of Alice and Bob in our QBDQ scheme, assuring they query the 9-th and 5-th items, respectively.

scheme, the server Charlie sends the quantum state $|\phi\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i⟩|K_i⟩$ to client Alice through oblivious transfer strategy. Since all the information about the key sequence $K$ is encoded in the state $|\phi\rangle$, so Alice cannot extract the key form $|\phi\rangle$ directly. Here we suppose the whole system of quantum state $|\phi\rangle$ consisted of two subsystems, i.e., the $n$-qubit quantum subsystem $C$ (index qubits $|i⟩$) and the $m$-qubit subsystem $D$ (key qubits $|K_i⟩$). If Alice makes a projective measurement on the received state $|\phi\rangle$, she will get the resultant state $|i⟩|K_i⟩$ for any $i$ with the probability of $1/N$. The whole system can be represented by the quantum ensemble $\epsilon = \{p_i, \rho(i)\}$, here $p_i = 1/N$.

Here we get the upper limit of information that Alice can get from Charlie's is determined by the Holevo bound [38],

$$H(A : B) \leq S(\rho) - \frac{1}{N} \sum_{i=0}^{N-1} S(\rho(i))$$

Here $S(\rho)$ denotes Von Neumann entropy of quantum state $\rho$, $H(B:A)$ means the information Alice can get about Charlie’s key information (including the address $i$ and according keys $K_i$), and we have

$$\rho(i) = |i⟩ ⟨K_i| K_i⟩ |i⟩.$$
\[ S(\rho) = S\left( \frac{1}{N} \sum_{i=0}^{N-1} |i \rangle \langle K_i | K_i \langle i \rangle \right) = n + m. \tag{25} \]

and \( S(\rho(i)) = S(|i \rangle \langle K_i | K_i \langle i \rangle) = 0; \) therefore,

\[ H(A : B) \leq n + m. \tag{26} \]

Then, Alice can only get \( n \)-bit of address information (i.e., \( i \)) and the corresponding \( m \)-bit key (i.e., \( K_i \)) by measuring \( \rho \).

In addition, she will certainly lose the chance to get her key \( K_i \). This means Alice cannot extract more than one key from Charlie.

Besides, in Step 3, Charlie uses the offset key \( K_i^A = K_i^{A,\Delta A} \) to encrypt the data items, and sends its encoded state \( |\phi''\rangle = (1/\sqrt{N}) \sum_{i=0}^{N-1} |i\rangle |D_i^B\rangle \) to Alice with oblivious transfer strategy. Alice’s privacy of query index \( i \) is protected by the oblivious transfer strategy. For example, the transmitted state \( |\phi''\rangle \) Alice received is a superposition state, i.e., \( |\phi''\rangle = (1/\sqrt{N})(|0\rangle |D_0^A\rangle + |1\rangle |D_1^A\rangle + \cdots + |N-1\rangle |D_{N-1}^A\rangle) \), which encapsulates all the query data \( |D_i^A\rangle \) \( 0 \leq i \leq N-1 \) including the desirable one \( D_{i^*}^A \). Alice obtains the query item \( D_{i^*}^A \) through the Grover iteration and the previously obtained key \( K_{i^*} \). Suppose Bob is also dishonest, he has the same situation with Alice.

**Client’s Privacy.** If Charlie is dishonest, he may try to obtain Alice’s private query index \( p \) during the communication process. However, Alice only sends one classical message \( \Delta s = \lambda_A - p \) to cloud server Charlie in Step 2, and Charlie does not know the encryption key which chosen by Alice, thus he cannot obtain any useful information about the data Alice wants to search. As same as Alice, Bob only sends a classical offset message \( \Delta s = \lambda_B - p \) to Charlie, which prevents Charlie from obtaining his information.

### 4.2.2. Channel Security Analysis

The security of the quantum channel is guaranteed by the decoy-photon checking technology. The process of eavesdropping detected done by the two neighbor participants in our scheme is essentially equivalent to that in the BB84 scheme [36], which has been proved to be unconditionally secure. To be specific, the decoy qubits, which are randomly inserted into target qubits, are generated by randomly chosen from \([0\], [1], [+], [-]\). After one participant sends the mixed decoy qubits and encrypted target qubits to quantum center, he will ask quantum center to measure them with the same bases these qubits were produced. For any outside eavesdropper, the bases used by participants are all random; the eavesdropper cannot produce the same qubits like decoy qubits before quantum center receives the qubits. Just like the situation in the BB84 scheme, if any outside eavesdropper exists in the process of our scheme, the eavesdropping actions will be found by the two participants.

The outside eavesdropper cannot get the shared key because eavesdropper cannot distinguish target qubits form decoy qubits, and he can only choose one set of orthogonal basis to measure it, so the eavesdropper will certainly change the states of the qubit, and then he will be discovered. We assume that eavesdropper will do intercept-resend attack.

Eavesdropper applies operation \( U_E \) and auxiliary system \( |E\rangle \) which satisfies the following conditions:

\[ U_E |0\rangle |E\rangle = a |0\rangle |E_{00}\rangle + b |1\rangle |E_{01}\rangle, \tag{27} \]
\[ U_E |1\rangle |E\rangle = c |0\rangle |E_{00}\rangle + d |1\rangle |E_{11}\rangle. \tag{28} \]

Here, \( |a|^2 + |b|^2 = 1 \) and \( |c|^2 + |d|^2 = 1 \). If the eavesdropper wants to extract the encode information precisely, then \( U_E \) must satisfy

\[ U_E |+\rangle |E\rangle = \frac{1}{\sqrt{2}} (a |0\rangle |E_{00}\rangle + b |1\rangle |E_{01}\rangle + c |0\rangle |E_{10}\rangle + d |1\rangle |E_{11}\rangle), \tag{29} \]
\[ U_E |-\rangle |E\rangle = \frac{1}{\sqrt{2}} (a |0\rangle |E_{00}\rangle + b |1\rangle |E_{01}\rangle - c |0\rangle |E_{10}\rangle + d |1\rangle |E_{11}\rangle), \tag{30} \]
\[ U_E |y\rangle |E\rangle = \frac{1}{\sqrt{2}} (a |0\rangle |E_{00}\rangle + b |1\rangle |E_{01}\rangle + ic |1\rangle |E_{10}\rangle - id |1\rangle |E_{11}\rangle), \tag{31} \]
\[ U_E |-y\rangle |E\rangle = \frac{1}{\sqrt{2}} (a |0\rangle |E_{00}\rangle + b |1\rangle |E_{01}\rangle - ic |1\rangle |E_{10}\rangle + id |1\rangle |E_{11}\rangle). \tag{32} \]

From (29)–(32) we can obtain that

\[ a |E_{00}\rangle - b |E_{01}\rangle + c |E_{10}\rangle - d |E_{11}\rangle = 0, \tag{33} \]
\[ a |E_{00}\rangle + b |E_{01}\rangle - c |E_{10}\rangle - d |E_{11}\rangle = 0, \tag{34} \]
\[ a |E_{00}\rangle + ib |E_{01}\rangle + ic |E_{10}\rangle - id |E_{11}\rangle = 0, \tag{35} \]
\[ a |E_{00}\rangle - ib |E_{01}\rangle - ic |E_{10}\rangle + id |E_{11}\rangle = 0, \tag{36} \]
we can get that \( a = d = 1, b = c = 0, \) and \( |E_{00}\rangle = |E_{11}\rangle, \) then we get

\[ U_E |0\rangle |E\rangle = |0\rangle |E_{00}\rangle, \tag{37} \]
\[ U_E |1\rangle |E\rangle = |1\rangle |E_{11}\rangle, \tag{38} \]

and we can summarize that eavesdropper would not be found only when decoy qubits and target qubits are \([0\], [1]\), which is impossible. So there is no way for the eavesdropper to know the secret key.
4.3. Efficiency Analysis. As we know, quantum-based schemes have greater information capacity than classic ones. In order to evaluate the efficiency of our QDBQ scheme more objectively, we choose some of the most representative quantum schemes as comparison objects, for example, Jakobi et al’s quantum private query (QPQ) scheme (J11 for short) [39], Gao et al’s QPQ scheme (G12) [40], and Rao et al’s QPQ scheme (R13) [41].

To evaluate the efficiency of quantum communication schemes, there are mainly two indicators: the communication complexity (i.e., the number of transmitted qubits), and the consumption of exchanged classic messages (i.e., the number of exchanged classic bits).

4.3.1. Communication Complexity. The communication complexity, i.e., the number of quantum bits (qubits) transmitted in the communication process, is one of the key indicators of the efficiency for communication scheme. In J11 and G12 schemes, the cloud server (Charlie) sends $k \times N$ qubits to the client (Alice), where $k$ is the number of divided substrings. These $k$ substrings are added bitwise in order to reduce Alice’s information on the key to roughly one bit (i.e., $\pi = N^{(1/4)^k} \approx 1$), so $k = \log \sqrt{N}$. In summary, $N \times \log \sqrt{N}$ qubits are transmitted in J11 and J12 schemes, and its communication complexity is $O(N \log N)$. But in the R13 scheme, the number of qubits that need to be exchanged is reduced to $O(N)$, so the communication complexity is $O(N)$.

In our QBDQ scheme, Charlie firstly transmits a $([\log N] + m)$-qubit state $|\psi \rangle$ for sending the encryption keys in Step 1, and the $([\log N] + m)$-qubit state $|\psi \rangle$ containing every encrypted data $D_i (0 \leq i \leq N - 1)$ is transmitted to Alice (Bob) in Step 3. Considering that each data item the cloud server holds is an only one-bit message in J11, G12 and R13 schemes, here we let $m = 1$. Therefore, the transmitted qubits are $2(\log N + 1)$, so its communication complexity is $O(\log N)$.

To be more intuitive, we calculate the numbers of transmitted qubits in different database capacities for the J11, G12, R13, and our QBDQ schemes (see Table 2) and show the comparison results among them in Figure 7. As shown in this figure, J11 and G12 schemes have the same qubits consumption, R13 scheme reduces the consumption, and our QBDQ scheme has the lowest qubits consumption. That is, our scheme has the lowest communication complexity among them.

4.3.2. Consumption of Exchanged Classic Messages. For a communication scheme, it should also consider the consumption of the exchanged classic messages. In the J11, J12, and R13 schemes, $N \times 1$ bits of encrypted data, considering each data item is a one-bit message (i.e., $m = 1$), is transmitted from the cloud server to the client, so their exchanged classic messages are all $O(N)$ bits. In our scheme, Alice (Bob) returns a classical message $\Delta s$, i.e., a $([\log N] \times m)$-bit classic message, to Charlie in Step 2. Since $m = 1$, the exchanged message is just $O(\log N)$ bits.

Table 3 lists the numbers of transmitted qubits in different database capacities for the J11, G12, R13, and our QBDQ schemes, while Figure 8 gives a more intuitive comparison between our QBDQ scheme and the other QPQ schemes (J11, G12, and R13 schemes). Obviously, our scheme needs less consumption of exchanged classic messages than other QPQ protocols.

In summary, Table 4 lists the comparison among our QBDQ scheme and the other three QPQ schemes clearly. As shown in Table 4, our scheme achieves a great reduction on both the communication complexity and the consumption of exchanged classic messages. Besides, our QBDQ scheme just needs to perform quantum measurement two times, which is obviously less than the other ones.
Table 2: Numbers of transmitted qubits in different database capacities for J11, G12, R13, and our QBDQ schemes.

<table>
<thead>
<tr>
<th>Database size</th>
<th>Transmitted messages (qubit)</th>
<th>Database size</th>
<th>Transmitted messages (qubit)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>24</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td>64</td>
<td>16</td>
<td>4</td>
</tr>
<tr>
<td>24</td>
<td>120</td>
<td>24</td>
<td>5</td>
</tr>
<tr>
<td>32</td>
<td>160</td>
<td>32</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>240</td>
<td>40</td>
<td>6</td>
</tr>
<tr>
<td>48</td>
<td>288</td>
<td>48</td>
<td>6</td>
</tr>
<tr>
<td>56</td>
<td>336</td>
<td>56</td>
<td>6</td>
</tr>
<tr>
<td>64</td>
<td>384</td>
<td>64</td>
<td>6</td>
</tr>
<tr>
<td>72</td>
<td>504</td>
<td>72</td>
<td>7</td>
</tr>
<tr>
<td>80</td>
<td>560</td>
<td>80</td>
<td>7</td>
</tr>
<tr>
<td>88</td>
<td>616</td>
<td>88</td>
<td>7</td>
</tr>
<tr>
<td>96</td>
<td>672</td>
<td>96</td>
<td>7</td>
</tr>
<tr>
<td>104</td>
<td>728</td>
<td>104</td>
<td>7</td>
</tr>
<tr>
<td>112</td>
<td>784</td>
<td>112</td>
<td>7</td>
</tr>
<tr>
<td>120</td>
<td>840</td>
<td>120</td>
<td>7</td>
</tr>
<tr>
<td>128</td>
<td>896</td>
<td>128</td>
<td>7</td>
</tr>
<tr>
<td>136</td>
<td>1088</td>
<td>136</td>
<td>8</td>
</tr>
<tr>
<td>144</td>
<td>1152</td>
<td>144</td>
<td>8</td>
</tr>
<tr>
<td>152</td>
<td>1216</td>
<td>152</td>
<td>8</td>
</tr>
<tr>
<td>160</td>
<td>1280</td>
<td>160</td>
<td>8</td>
</tr>
<tr>
<td>168</td>
<td>1344</td>
<td>168</td>
<td>8</td>
</tr>
<tr>
<td>176</td>
<td>1408</td>
<td>176</td>
<td>8</td>
</tr>
<tr>
<td>184</td>
<td>1472</td>
<td>184</td>
<td>8</td>
</tr>
<tr>
<td>192</td>
<td>1536</td>
<td>192</td>
<td>8</td>
</tr>
<tr>
<td>200</td>
<td>1600</td>
<td>200</td>
<td>8</td>
</tr>
</tbody>
</table>

Table 3: Exchanged classic messages in different database capacities for J11, G12, R13, and our QBDQ schemes.

<table>
<thead>
<tr>
<th>Database size</th>
<th>Exchanged messages J11/G12/R13</th>
<th>Database size</th>
<th>Exchanged messages J11/G12/R13</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>QBDQ</td>
<td></td>
<td>QBDQ</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
<td>8</td>
<td>3</td>
</tr>
<tr>
<td>16</td>
<td>16</td>
<td>4</td>
<td>96</td>
</tr>
<tr>
<td>24</td>
<td>24</td>
<td>5</td>
<td>104</td>
</tr>
<tr>
<td>32</td>
<td>32</td>
<td>5</td>
<td>112</td>
</tr>
<tr>
<td>40</td>
<td>40</td>
<td>6</td>
<td>120</td>
</tr>
<tr>
<td>48</td>
<td>48</td>
<td>6</td>
<td>128</td>
</tr>
<tr>
<td>56</td>
<td>56</td>
<td>6</td>
<td>136</td>
</tr>
<tr>
<td>64</td>
<td>64</td>
<td>6</td>
<td>144</td>
</tr>
<tr>
<td>72</td>
<td>72</td>
<td>7</td>
<td>152</td>
</tr>
<tr>
<td>80</td>
<td>80</td>
<td>7</td>
<td>160</td>
</tr>
</tbody>
</table>

Table 4: Comparison among our QBDQ scheme and the other QPQ schemes.

<table>
<thead>
<tr>
<th>Schemes</th>
<th>Communication complexity (qubit)</th>
<th>Exchanged message (bit)</th>
<th>Measurement times</th>
</tr>
</thead>
<tbody>
<tr>
<td>J11</td>
<td>$O(N \log N)$</td>
<td>N+1</td>
<td>$kN$</td>
</tr>
<tr>
<td>G12</td>
<td>$O(N \log N)$</td>
<td>N+1</td>
<td>$kN$</td>
</tr>
<tr>
<td>R13</td>
<td>$O(N)$</td>
<td>N+1</td>
<td>N</td>
</tr>
<tr>
<td>Ours</td>
<td>$O(\log N)$</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

5. Related Work

Cloud database services are typically run on cloud computing platforms, and access to cloud databases is provided as a service, which takes care of scalability and availability of the database, and it makes the underlying software-stack transparent to the user.

Benefit from cloud computing technologies and devices, more and more data owners are motivated to outsource their data to cloud servers for great convenience in data management, and cloud database query has attracted the attention of scholars. Cloud database query was firstly proposed by Chor et al. [42], where the privacy of the server cannot be guaranteed, which means that sensitive data (e.g., health records, financial transactions) stored in cloud database is threatened by information leaks. Therefore, how to preserve the privacy of sensitive data in the process of cloud database query has become an important topic. In order to solve the problem, many methods are proposed to guarantee the privacy preservation of database query [12–18]; one of the most popular methods is SE.
SE is a special kind of private query, which enables the user to store the encrypted data to the cloud and execute keyword search over ciphertext. Since Song et al. [15] proposed the first practical private database query scheme for searching on encrypted data in cloud and provided the security proofs for the scheme, some other schemes to address privacy protection issues in cloud database queries have also been proposed [17, 18]. In order to support more complex queries, the conjunctive keyword search scheme [14] over encrypted data has been proposed. After that, a more general approach, predicate encryption [16], which supports inner-product, was also proposed.

In general, most of the above schemes [12–18, 42] are based on public key cryptography such as RSA, and its security is based on mathematical NP-hard problems. Therefore, these schemes are difficult to crack in polynomial time for classic computers. All of the above protocols are based on public key cryptography such as RSA. On a quantum computer, to factor an integer N, Shor’s algorithm [19] can run in polynomial time (the time taken is polynomial in \( \log N \)), which is the size of the input. Specifically, it takes quantum gates of order \( O((\log N)^2(\log \log N)(\log \log \log N)) \) using fast multiplication [43], thus demonstrating that the integer-factorization problem (the large factorization problem is the security foundation of RSA) can be efficiently solved on a quantum computer and is consequently in the complexity class BQP. This is almost exponentially faster than the most efficient known classical factoring algorithm, so we can say that these schemes [12–18, 42] are not resistant to quantum attacks. Different from classic schemes based on mathematical complexity, the security of quantum-based schemes is guaranteed by some properties of quantum mechanics, such as noncloning theorem and uncertainty principle. They are considered to have potential unconditional security and of course also include resistance to quantum attacks.

Recently, some researchers have tried to utilize quantum mechanics to design private query schemes. In 2008, Giovannetti et al. [44] proposed the first quantum private query (QPQ) protocol. The client sends the query \( |j⟩_Q \) and a decoy state \( |j⟩_Q |0⟩_Q/\sqrt{2} \) to the server in random order, then Bob uses each of them to interrogate his database using a qRAM (which records the reply to her queries in a register \( R \)) and returns \( |j⟩_Q |A_j⟩_R \) or \( |j⟩_Q |A_j⟩_R + |0⟩_Q |0⟩_R/\sqrt{2} \). The returned decoy state is used to check the eavesdropping of the server or the outside party. In 2011, Olejnik [45] presented a new QPQ protocol in a similar form with Giovannetti et al’s protocol. By subtly selecting the oracle operation and the encoding scheme, one query state can achieve two aims simultaneously, i.e., obtaining the expected information and checking Bob’s potential attack, so the communication complexity is reduced. Unfortunately, it is very vulnerable to the realities of significant transmission losses.

Therefore, Jakobi et al. [39] proposed a novel QPQ protocol (J11) based on the QKD protocol, where QKD is essentially a quantum analog of SE. In this protocol, an asymmetric key can be distributed between Alice and Bob by utilizing SARG04 QKD protocol, and Bob encrypts the whole database with the QKD key. Alice only knows few bits of the key, which ensures the database privacy. Compared with the previous QPQ protocols, J11 protocol is loss-tolerant and more secure. What is more, the J11 protocol can be easily generalized to the large database. Later, Gao et al. [40] proposed a flexible generalized protocol (G12) based on the J11 protocol, which introduced a variable \( \theta \) to adjust the balance between database security and client privacy. Considering a database with size \( N \), the J11 and G12 protocols have a communication complexity of \( O(N\log N) \). In order to reduce the complexity, Rao et al. [41] gave two more efficient protocols (R13), which reduced the number of exchanged qubits to \( O(N) \).

Different from classical encryption schemes based on some mathematical difficult problems, these findings have shown the potential in either the improvements of efficiency or the enhancements of security in cloud computing field with large computing resources and also brought new quantum technologies to solve private database query problems. However, to the best of our knowledge, there are few studies focusing on the quantum-based privacy-preserving database query problem in cloud environment. Therefore, we combine quantum mechanics with cloud database queries and proposed a QBDQ scheme which aims to realize the privacy preservation for the clients and cloud server.

6. Conclusion and Future Work

As far as we know, the existing QPQ schemes either belong to the qRAM-based schemes, such as Giovannetti et al.’s [44] and Olejnik’s [45] schemes, or belong to the QKD-based schemes, such as Jakobi et al.’s [39], Gao et al.’s [40], and Rao et al.’s [41] schemes. These QKD-based schemes solve the problem of the server’s privacy; their communication complexity needs to be further reduced. In this study, we propose an efficient quantum private query scheme based on oracle operation, modified Grover iteration, oblivious transfer strategy, and the special offset encryption mechanism rather than QKD or qRAM. Compared with those schemes, our QBDQ scheme shows higher efficiency in terms of the communication complexity, the consumption of exchanged message, and the quantum measurement.

In our QBDQ scheme, we adopt the oblivious transfer strategy to solve the problem of the client’s privacy; i.e., the client will ask the server to transmit all these encrypted data items to him/her. But in a real-world cloud environment, this is not a good approach. Although it guarantees that there is no information about the query index to be leaked, but it needs to transmit too many data items from the cloud database. Even if quantum resources have an exponential high-capacity advantage, it is also a waste of resources. Maybe the “query window” strategy is a better choice. To be specific, the client can firstly choose an index window that contains the desirable query item and ask the server to transmit these encrypted data items in this window scope other than the all data items, to him/her in a quantum way. Although there is certain information leakage from the perspective of information theory, it can save quantum resources. In this strategy, the selection of the size of a query window is a key point. In order to achieve a balance of efficiency and security, perhaps some
game theory (such as, Nash Equilibrium [46, 47]) and penalty functions [48–50] can provide relevant optimized solutions. It is worth noting that although the proposed solution involves two clients, for the sake of brevity (and for comparison with other quantum schemes), Alice and Bob do not interact. This is the most common pattern in cloud database queries. For the multiparty joint inquiry method, we will discuss it in future work. In addition, we just consider the ideal framework of the privacy-preserving database query in cloud environment; i.e., all the clients and cloud server are semihonest. But in a real cloud environment, clients and servers may be untrustworthy. How to generalize our QBDO into such multiuser and the untrusted scenario is an interesting work.

Data Availability

The database items and the corresponding encryption keys used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by Nature Science Foundation of China (Grants nos. 71461005, 61502101, 61501247, and 61672290), Natural Science Foundation of Jiangsu Province (Grant no. BK20171458), Natural Science Foundation for Colleges and Universities of Jiangsu Province (Grant no. 16KJB520030), the Six Talent Peaks Project of Jiangsu Province (Grant no. 2015-XXRJ-013), and the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD).

References


