

Quantum Privacy-Preserving Data Analytics

Shenggang Ying¹, Mingsheng Ying^{1,2,3}, Yuan Feng¹

¹ University of Technology Sydney, Australia

² Institute of Software, Chinese Academy of Sciences, China

³ Tsinghua University, China

Abstract. Data analytics (such as association rule mining and decision tree mining) can discover useful statistical knowledge from a big data set. But protecting the privacy of the data provider and the data user in the process of analytics is a serious issue. Usually, the privacy of both parties cannot be fully protected simultaneously by a classical algorithm. In this paper, we present a quantum protocol for data mining that can much better protect privacy than the known classical algorithms: (1) if both the data provider and the data user are honest, the data user can know nothing about the database except the statistical results, and the data provider can get nearly no information about the results mined by the data user; (2) if the data user is dishonest and tries to disclose private information of the other, she/he will be detected with a high probability; (3) if the data provider tries to disclose the privacy of the data user, she/he cannot get any useful information since the data user hides his privacy among noises.

1 Introduction

Privacy-preserving data analytics: Data analytics has become an indispensable technology in the big data era. Mining statistical knowledge from a big data set is one of the most important tasks of data analytics. A typical example is association rule mining, which was introduced to find useful links from a large set of transactions in a supermarket [2]. An association rule is a probabilistic implication $A \Rightarrow B$, which means event A implies event B with a high probability. Another example is to mine decision trees [17], which are a core model of classification problems.

Data analytics has numerous applications in the areas like market basket problem, scientific data analysis, web mining, just name a few [2,13]. In practical applications, one major issue arises: how to protect the privacy of each individual in a database while mining the statistical knowledge? For instance, the privacy of each patient should not be leaked during mining an association rule or a decision tree for medical diagnosis from a database of patients. To address this issue, various algorithms for privacy-preserving data mining has been developed in the last twenty years [6,7,12,18]. In these algorithms, however, the privacy of the data provider and the data user cannot be protected simultaneously.

Quantum computing and cryptography: Since 1990's, various quantum algorithms have been discovered and proved to be much faster than the

known classical algorithms for the same tasks. For example, Grover’s quantum search algorithm [10] can find the target element in a database in $O(\sqrt{N})$ oracle calls. Quantum counting algorithm [5] has a quadratic speed-up over classical algorithms as well. More recently, several quantum machine learning algorithms [14,15] have been presented based on quantum random access memory [8], and they can achieve an exponential speed-up over classical algorithms.

Several quantum protocols that can better protect privacy have also been found; for example, the famous quantum key distribution protocol BB84 [3], quantum private queries [9], and revocable quantum timed-release encryption [21].

Contribution of this paper: In this paper, we present a quantum protocol for mining statistical knowledge in a database, such as association rules and decision trees. This protocol can protect the privacy of both the data provider and data user provided they are honest. Furthermore, the privacy of both data provider and data user is protected: no useful private information will be disclosed.

The basic idea of our protocol can be described as follows. The basic idea for the data provider is to employ tests to detect attacks. Without any influence on the computational results, the data provider randomly detects attacks from the data user. Meanwhile, the basic idea for the data user is to hide his privacy among noises. The data user introduces noises into her/his private query functions, and these noises in different steps cancel each other if the data provider follows the protocol strictly. The novelty is that the privacy of both parties is preserved by techniques in quantum computing and cryptography, but can hardly be achieved by classical methods.

Structure of the paper: For convenience of the reader, preliminaries and notations are introduced in Section 2. We present our quantum protocol in three steps: we first explain the design idea in Section 3, an outline of the protocol is then shown in Section 4, and we examine some details in the execution of the protocol in Section 5. The correctness of the protocol is proven in Section 6. The privacy analysis is given in Section 7 for the data provider and in Section 8 for the data user. The complexity analysis is given in Section 9. Some further discussions are presented in Section 10. All the proofs of lemmas and theorems are given in the Appendix.

2 Preliminaries

2.1 Association Rule Mining

As pointed out above, we are going to develop a quantum algorithm for association rule mining. (The application for decision tree learning is presented in Section 10.2.) For convenience of the reader, in this subsection, we briefly review association rule mining; for more details, see [2]. Let $S = \{1, 2, \dots, k\}$ be a set of **items**, where each index $i \in S$ stands for an item; for instance, 1 may stand for “Apple”, 2 for “Orange”. A **transaction** or **itemset** tr is a set of items, i.e.,

$tr \subseteq S$. Moreover, an m -**itemset** is an itemset which has exactly m items. For example, a transaction can be the items a customer buys in one purchase. In order to store a transaction into a computer or a database, a transaction tr is represented by a string $\pi = \pi_1\pi_2 \cdots \pi_k \in \{0, 1\}^k$:

$$\pi_\iota = \begin{cases} 1, & \iota \in tr, \\ 0, & \iota \notin tr. \end{cases} \quad (1)$$

In this paper, we always use strings in $\{0, 1\}^k$ to represent transactions or itemsets based on Eq. (1). Then we can talk about the **inclusion relation** $\pi \subseteq \tau$ for two strings $\pi, \tau \in \{0, 1\}^k$ since they refer to two sets (transactions or itemsets): $\pi \subseteq \tau \Leftrightarrow \pi_\iota \leq \tau_\iota$ for every $\iota \in S$. Moreover, we can define other set-theoretic operations and relations of π and τ .

A **database** D of transactions is a set $D = \langle d_0, d_1, \dots, d_{N-1} \rangle$, where $d_j \in \{0, 1\}^k$ is a transaction and N is the size of D , i.e., the number of transactions in D . The **support** $\text{supp}(d)$ of an itemset d is defined to be its frequency in database D :

$$\text{supp}(d) = f^{(d)}(D) = \frac{1}{N} \sum_{j=0}^{N-1} f^{(d)}(d_j), \quad (2)$$

where

$$f^{(d)}(d_j) = \begin{cases} 1, & d \subseteq d_j, \\ 0, & d \not\subseteq d_j. \end{cases} \quad (3)$$

The superscript (d) of $f^{(d)}(\cdot)$ may be omitted if the itemset d is clear from the context or not explicitly specified.

A **rule** is a probabilistic implication between two disjoint itemsets in D . The support and confidence of a rule $\pi \Rightarrow \tau$ are defined by

$$\text{supp}(\pi \Rightarrow \tau) = \text{supp}(\pi \cup \tau),$$

$$\text{conf}(\pi \Rightarrow \tau) = \frac{\text{supp}(\pi \cup \tau)}{\text{supp}(\pi)},$$

respectively. Roughly speaking, the support of a rule indicates its importance (frequency) in a database. The confidence of a rule means its correctness probability; more precisely, $\text{conf}(\pi \Rightarrow \tau)$ is the probability that if π appears in d ($\pi \subseteq d$), then τ will as well appear in d ($\tau \subseteq d$).

The task of association rule mining is to find all rules with high support and confidence, namely **association rule**.

Definition 1 (Association Rule). *An association rule $\pi \Rightarrow \tau$ is a relation between two itemsets $\pi, \tau \subseteq S$, which satisfies the following conditions:*

- $\pi \cap \tau = \emptyset$,
- $\text{supp}(\pi \Rightarrow \tau) > s_{\min}$,
- $\text{conf}(\pi \Rightarrow \tau) > c_{\min}$,

where s_{\min} (resp. c_{\min}) is the preset (constant) threshold for supports (resp. confidences).

The algorithms for association rule mining in the literature [2] are usually divided into the following two steps:

1. Find all **frequent itemsets** ξ , which are itemsets with high support/frequency, i.e., $\text{supp}(\xi) > s_{\min}$.
2. For each frequent itemset ξ , find all association rules $\pi \Rightarrow \tau$ with $\pi \cup \tau = \xi$.

Moreover, only the first step is crucial because once it is done, the second becomes very easy by the definition of confidence. Note $\xi \subseteq d$ implies $\tau \subseteq d$ for any $\tau \subseteq \xi$. So, the supports of itemsets are non-increasing: $\tau \subseteq \xi$ implies $\text{supp}(\tau) \geq \text{supp}(\xi)$. Thus, each frequent m -itemset is a superset of some frequent $(m - 1)$ -itemset, which leads to the level-wise algorithm [2]:

- Initialization. Let $F_1 = \{\{i\} : i = 1, 2, \dots, k\}$ be the set of all 1-itemsets. Set $F_l = \emptyset$ for all $l > 1$, and $G_j = \emptyset$ for all $j \geq 1$.
- Induction on l starting from $l = 1$. If $F_l = \emptyset$, output all itemsets in G_j for all j , and terminate the algorithm. Otherwise, do the following steps for every $\tau \in F_l$:
 1. Compute $\text{supp}(\tau)$.
 2. If $\text{supp}(\tau) > s_{\min}$, add τ into G_l and all supersets of τ with $l + 1$ items into F_{l+1} .

One can see that in the above algorithm, the key step is to compute the support of a given itemset. In particular, only this step may cause disclosure of private data. So, in this paper, we will focus on it. Note that computing the support of a given itemset can be done by quantum counting algorithm [5]. Our work is to develop a privacy-preserving extension of quantum counting for this task on a centralized database.

2.2 Quantum Database

To employ quantum algorithms for mining classical database, we first recall from [8] how a (classical) database can be stored in a quantum computer.

Definition 2 (Quantum database). Let $D = \langle d_0, d_1, \dots, d_{N-1} \rangle$ be a database where $d_j \in \{0, 1\}^k$ for all j . For convenience, we always assume that $N = 2^n$. Then the quantum database corresponding to D is a unitary transformation O_D on $n + k$ qubits defined as follows:

$$O_D|x\rangle|\tau\rangle = |x\rangle|\tau \oplus d_x\rangle$$

for every $x \in \{0, 1\}^n$ and $\tau \in \{0, 1\}^k$. Here we identify x with the integer it represents (by binary representation).

In the above definition, x is used to denote the address of a data cell, and d_x is the content stored in data cell x . The quantum database O_D can be seen as a quantum oracle; for instance, if a data user queries it with a basis state $|i\rangle|0\rangle$, the oracle will return $|i\rangle|d_i\rangle$. This is equivalent to querying the classical database D with address i . More interestingly, a data user can also query O_D with a superposition $\sum_i \alpha_i |i\rangle|0\rangle$ of addresses, and it will return

$$O_D \left(\sum_i \alpha_i |i\rangle|0\rangle \right) = \sum_i \alpha_i |i\rangle|d_i\rangle, \quad (4)$$

a (superposed) state which in principle contains *all* transactions of the database. Note also that, however, an attempt to read out a particular transaction (by performing a quantum measurement) will cause collapse of the state into one where all information of other transactions is completely destroyed.

It is worth mentioning that in our protocol the quantum database O_D will be permuted to $U_D(y)$ (see Eq. (9)) to improve the data provider's privacy.

2.3 Privacy-preserving Data Analytics

Now let us consider the following problem:

Problem 1 (Privacy-preserving counting). Suppose Alice holds a database $D = \langle d_0, d_1, \dots, d_{N-1} \rangle$ where $d_j \in \{0, 1\}^k$ for all j . For a function $f : \{0, 1\}^k \rightarrow \{0, 1\}$, Bob wants to compute

$$f(D) = \frac{1}{N} \sum_{j=0}^{N-1} f(d_j), \quad (5)$$

and after the computation,

1. *Privacy preserving for Alice:* for each j , Bob will not know d_j (even approximately);
2. *Privacy preserving for Bob:* Alice will not know the function f .

Obviously, whenever f is taken to be $f^{(d)}$ defined in Eq. (3), then $f(D)$ is the support of item set d .

The majority of classical algorithms in the literature aim at protecting Alice's privacy. The idea is to publish a distorted database D' so that Bob can compute f over it. Thus, the problem becomes how to modify D to D' with a high accuracy of statistical properties. The suggested solutions include: (1) modify each transaction independently; for instance, the occurrence of each item in a transaction is flipped randomly [7]; (2) replace some items by others without changing the number of items in a transaction [18]; (3) modify transactions within the entire database; for instance, swap elements between different transactions [6].

It is easy to see that the function in Eq.(2) can be efficiently computed by quantum counting algorithm [5] with the corresponding quantum database O_D . However, a simple application of quantum counting is unable to achieve the goal of privacy protection. It has to be extended to fit the new task.

3 Basic Ideas of the Protocol

The overall aim of this paper is to develop a quantum protocol solving Problem 1. In this section, we introduce the basic ideas employed in the design of our protocol, which is essentially the quantum counting algorithm [5] with new strategies for privacy preserving. Quantum counting is a combination of controlled Grover iterations modified from Grover search algorithm [10] and quantum Fourier transform [16]. As quantum Fourier transform is not applied to the original data set, privacy preserving in Grover search is the core of our protocol.

To explain the ideas more clearly, we elaborate in the following a quantum algorithm for *privacy-preserving search*, a problem which can be regarded as a special case of Problem 1 where $f(D)$ returns an index (if there is any) j such that $f(d_j) = 1$.

3.1 Two-Party Grover Search

For privacy preserving, we adapt Grover search algorithm [10] to the two-party scenario. To simplify the presentation, we omit the detail of communication between Alice and Bob, and assume implicitly that when Alice (resp. Bob) performs a quantum operation, the corresponding quantum system has been sent to her (resp. him) by Bob (resp. Alice) or prepared by herself (resp. himself). The algorithm goes as follows:

- Bob prepares the initial state $|+\rangle_{q_a}^{\otimes n}|0\rangle_{q_d}^{\otimes k} = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle_{q_a} |\vec{0}\rangle_{q_d}$ where q_a denotes the (n -qubit) address system while q_d the (k -qubit) data system, $N = 2^n$, and $\vec{0}$ is the k -length binary representation of 0.
- Repeat the following steps for $T = \lceil \frac{\pi}{4} \sqrt{N} \rceil$ times:
 1. Alice applies the database O_D on systems q_a and q_d . Let $|\phi_0\rangle = \sum_j \alpha_j |j\rangle |\vec{0}\rangle$ be the initial state of the current iteration. Then now it becomes

$$|\phi_1\rangle = O_D |\phi_0\rangle = \sum_j \alpha_j |j\rangle |d_j\rangle.$$

2. Bob applies U_f , obtaining

$$|\phi_2\rangle = U_f |\phi_1\rangle = \sum_j (-1)^{f(d_j)} \alpha_j |j\rangle |d_j\rangle,$$

where U_f is the oracle defined by:

$$U_f : |j\rangle |\tau\rangle \mapsto (-1)^{f(\tau)} |j\rangle |\tau\rangle. \quad (6)$$

3. Alice applies O_D again to disentangle the systems q_a and q_d , reaching

$$|\phi_3\rangle = O_D |\phi_2\rangle = \sum_j (-1)^{f(d_j)} \alpha_j |j\rangle |\vec{0}\rangle.$$

4. Bob performs G on system q_a only to update the amplitude, obtaining

$$|\phi'_0\rangle = G \otimes I_{q_d} |\phi_3\rangle = \sum_j \alpha'_j |j\rangle |\vec{0}\rangle,$$

where $G = I - 2|+\rangle^{\otimes n} \langle +|^{\otimes n}$. The state $|\phi'_0\rangle$ will be the initial state of the next iteration.

- Another iteration of the above loop is executed with U_f in Eq.(6) replaced by U'_f , and it is applied on q_a , q_d and an auxiliary qubit system q_g which has been set to $|0\rangle$, where

$$U'_f : |j\rangle_{q_a} |\tau\rangle_{q_d} |x\rangle_{q_g} \mapsto |j\rangle_{q_a} |\tau\rangle_{q_d} |x \oplus f(\tau)\rangle_{q_g}. \quad (7)$$

- Bob measures q_a and q_g , and reports the measurement outcome.

By a similar argument as that given in [10], we can show that the above algorithm returns an index j with $f(d_j) = 1$ with a high probability, provided that both Alice and Bob follow the protocol honestly.

3.2 Possible Attacks

Bob's attack: An obvious Bob's attack for the above algorithm is to send state $|j\rangle |\vec{0}\rangle$ for a chosen j to Alice before Step 1 in the loop. Then an honest Alice will send back to him $|j\rangle |d_j\rangle$, from which he is able to successfully disclose d_j . Note that in one run of the algorithm, Bob may cheat $2T$ times. Thus if it is called M times as a procedure in, say, association-rule mining protocol, Bob will obtain complete information of $2TM$ transactions of the database.

Alice's attack: Similarly, Alice can cheat by sending some chosen states to Bob to retrieve information about the query function f . To see this, note that in both association rule and decision tree mining, $f(\vec{1}) = 1$ for all legal f , where $\vec{1}$ is the k -length binary representation of $2^k - 1$. Now suppose Alice would like to know the value of $f(\tau)$ for some $\tau \in \{0, 1\}^k$. Then she chooses to send Bob the state $\frac{1}{\sqrt{2}} |0\rangle^{\otimes(n-1)} (|0\rangle |\tau\rangle + |1\rangle |\vec{1}\rangle)$ before Step 2 of the loop. Note that

$$\frac{1}{\sqrt{2}} |0\rangle^{\otimes(n-1)} (|0\rangle |\tau\rangle + |1\rangle |\vec{1}\rangle) \xrightarrow{U_f} \frac{1}{\sqrt{2}} |0\rangle^{\otimes(n-1)} [(-1)^{f(\tau)} |0\rangle |\tau\rangle - |1\rangle |\vec{1}\rangle].$$

Now Alice can obtain $f(\tau)$ by performing a quantum measurement on systems q_a and q_d , since the states $|0\rangle |\tau\rangle - |1\rangle |\vec{1}\rangle$ and $|0\rangle |\tau\rangle + |1\rangle |\vec{1}\rangle$ are orthogonal.

3.3 Privacy Preserving in Quantum Search

This subsection is devoted to an intuitive explanation of the techniques we are going to employ in the protocol presented in Section 4 to protect the privacy of both Alice and Bob.

Alice's strategy: The idea for protecting Alice's privacy is to employ tests to detect Bob's attacks. Originally it is hard to distinguish Bob's attacks from honest actions, since Alice does not know Bob's function f . Fortunately, if Bob is honest, two same states will still be the same after Bob's action U_f . Suppose Alice randomly generates two different strings $\mu, \nu \in \{0, 1\}^k$, and $f(\mu) = f(\nu)$ (resp. $f(\mu) \neq f(\nu)$). Alice sends Bob two same states $\frac{1}{\sqrt{2}}|0\rangle^{\otimes n-1}(|0\rangle|\mu\rangle + |1\rangle|\nu\rangle)$ to Bob. Then she will receive two same states $\frac{1}{\sqrt{2}}|0\rangle^{\otimes n-1}(|0\rangle|\mu\rangle + |1\rangle|\nu\rangle)$ (resp. $\frac{1}{\sqrt{2}}|0\rangle^{\otimes n-1}(|0\rangle|\mu\rangle - |1\rangle|\nu\rangle)$) from Bob. After disentangling the data qubits, Alice gets two copies of $|0\rangle^{\otimes n-1}|+\rangle|\vec{0}\rangle$ (resp. $|0\rangle^{\otimes n-1}|-\rangle|\vec{0}\rangle$). Finally Alice performs measurements on the last address qubits with basis $\{|+\rangle, |-\rangle\}$, and gets outcomes $+, +$ (resp. $-, -$).

But if Bob is dishonest and performs measurements on data qubits to read information, each state that Alice receives will be $|0\rangle^{\otimes n-1}|0\rangle|\mu\rangle$ or $|0\rangle^{\otimes n-1}|1\rangle|\nu\rangle$ independently. Finally the measurement outcomes on the last address qubits will be $+, -$ or $-, +$ with probability 0.5. These outcomes can be distinguished from those of honest actions.

Bob's strategy: The idea for protecting Bob's privacy is to add noises which cancel each other when Alice follows the protocol honestly. Recall that the net effect of a single iteration of the loop in the algorithm presented in Section 3.1 is $\bar{G}O_D U_f O_D$ where $\bar{G} = G \otimes I_d$. Then in four consecutive iterations, for instance, if the four calls of oracle U_f at Step 2 are replaced by $U, I_{a,d}, U, I_{a,d}$, respectively, where U is any unitary operator with $U = U^\dagger$ and $I_{a,d}$ is the identity operator on q_a and q_d , then the effect of the four modified iterations becomes

$$\bar{G}O_D I_{a,d} O_D \bar{G}O_D U O_D \bar{G}O_D I_{a,d} O_D \bar{G}O_D U O_D = I_{a,d}. \quad (8)$$

More generally, if Bob needs to use U_f for T times, he can insert T operators $I_{a,d}$ and $U_{f'}$ with different $f' \neq f$ between the T occurrences of U_f . By Eq.(8), we see that half of the information Alice gets is noise and not related to f , and thus she cannot recover f .

4 Protocol

4.1 Main Protocol

We are now ready to present our main protocol in Algorithm 1, which computes $f(D)$ for a given function f by applying procedure GroverIteration. In the protocol,

- At Step 2, $U_D(y)$ is defined as follows:

$$U_D(y) = (X^y \otimes I_d) O_D (X^y \otimes I_d). \quad (9)$$

where $X^y = X^{y_1} \otimes X^{y_2} \otimes \dots \otimes X^{y_n}$, $X^0 = I$, and $X^1 = X$. Note that

$$U_D(y)|x\rangle|\tau\rangle = |x\rangle|\tau \oplus d_{x \oplus y}\rangle.$$

Algorithm 1: Main protocol for privacy-preserving quantum counting on a centralized database.

Parameters: Number of address qubits n and number of data qubits k determined by the database D , and number of control qubits t determined by Bob's strategy in Section 5.3.

Output : two numbers $s_1, s_2 \in [0, 1]$, which are approximately $f(D)$.

```

1 begin
2   Alice generates  $y \in \{0, 1\}^n$  uniformly at random, and constructs a modified
   database  $U_D(y)$  from  $O_D$ ; see Eq. (9);
3   Bob prepares two identical states  $|+\rangle_{q_{c1}}^{\otimes t} |+\rangle_{q_{a1}}^{\otimes n} |\vec{0}\rangle_{q_{d1}}$  and  $|+\rangle_{q_{c2}}^{\otimes t} |+\rangle_{q_{a2}}^{\otimes n} |\vec{0}\rangle_{q_{d2}}$ .
   Here  $q_{ci}$ ,  $q_{ai}$ , and  $q_{di}$  denote the control, address, and data qubits,
   respectively;
4   For  $i = 0, \dots, T - 1$ , where  $T = 2^t$ , do GroverIteration( $i$ );
5   Alice generates  $r \in (0, 1)$  uniformly at random;
6   If  $r \leq p$ , Alice employs procedure TestBob2 to test whether Bob is honest.
   If dishonesty is detected, she terminates the entire protocol; otherwise, she
   sends a message "Repeat" to Bob;
7   Alice applies  $U_D(y)$  on  $q_{c1}$ ,  $q_{a1}$ ,  $q_{d1}$ ;
8   Bob performs  $U'_f$  in Eq. (7) on  $q_{a1}$ ,  $q_{d1}$ ,  $q_{g1}$  where  $q_{g1}$  is an auxiliary qubit
   which has been set to  $|0\rangle$ ;
9   Alice and Bob repeat Step 7 to Step 8 for  $q_{c2}$ ,  $q_{a2}$ ,  $q_{d2}$ . The new blank
   ancilla qubit is denoted  $q_{g2}$ ;
10  If  $p < r \leq 2p$ , Alice first sends a message "Repeat" to Bob, and then
   employs procedure TestBob2 to test whether Bob is honest. If dishonesty
   is detected, Alice terminates the entire protocol;
11  Alice applies  $U_D(y)$  on  $q_{a1}$ ,  $q_{d1}$ , and  $q_{a2}$ ,  $q_{d2}$  respectively;
12  Bob performs measurements on  $q_{g1}$  and  $q_{g2}$  to get outcome  $g_1, g_2 \in \{0, 1\}$ ;
13  Bob performs quantum Fourier transform, followed by measurements on  $q_{c1}$ 
   to get outcome  $\theta \in \{0, 1, \dots, T - 1\}$ ;
14  Bob computes  $s_i = \sin^2(\theta\pi/T)$  if  $g_i = 1$ , or  $\cos^2(\theta\pi/T)$  if  $g_i = 0$ , for  $i = 1, 2$ .
15 end

```

Procedure GroverIteration(i)

```

1 begin
2   Alice generates  $r \in (0, 1)$  uniformly at random;
3   If  $r \leq p$ , Alice employs procedure TestBob1( $i$ ) to test whether Bob is honest.
     If dishonesty is detected, Alice terminates the entire protocol; otherwise,
     she sends a message “Repeat” to Bob;
4   Alice applies  $U_D(y)$  and then Bob applies controlled  $U_{f_i}$  on  $q_{c1}, q_{a1}, q_{d1}$ 
     with  $q_{c1}$  being control qubits;
5   Alice and Bob repeat Step 4 for  $q_{c2}, q_{a2}, q_{d2}$ ;
6   If  $p < r \leq 2p$ , Alice first sends a message “Repeat” to Bob, and then
     employs procedure TestBob1( $i$ ) to test whether Bob is honest. If
     dishonesty is detected, Alice terminates the entire protocol;
7   Alice applies  $U_D(y)$  and then Bob applies controlled  $G$  on  $q_{c1}, q_{a1}, q_{d1}$  with
      $q_{c1}$  being control qubits, where  $G$  is defined in Sec 3.1;
8   Alice and Bob repeat Step 7 for  $q_{c2}, q_{a2}, q_{d2}$ ;
9 end

```

This modification of O_D permutes the transactions in the database to protect Alice’s privacy (Compare it with O_D in Definition 2).

- In the main protocol, Alice employs the test TestBob2 for Bob’s dishonesty with probability $2p$. Furthermore, the test is conducted either before or after Steps 7 to 9, with equal probability. Consequently, both Step 6 and Step 10 are executed with probability p . In this paper, we set $p = 0.05$.
- The message “Repeat” means that a test was or will be used, and Bob should prepare to repeat what he did for the last two copies of states.

4.2 Grover Iteration

In this subsection, we present the procedure GroverIteration called at Step 4 in Algorithm 1, which is essentially a controlled Grover iteration. In this procedure,

- the functions f_0, f_1, \dots, f_{T-1} are generated by Bob using the strategy presented in Section 5.3.
- for each i , U_{f_i} is a unitary operator similarly defined as that in Eq.(6).

In the following, we discuss briefly some implementation issues for procedure GroverIteration.

Controlled Operators. As said before, procedure GroverIteration is a controlled Grover iteration. Two controlled unitary operators, controlled U_{f_i} in Step 4 and controlled G in Step 7, need to be implemented. Fortunately, both controlled U_{f_i} and controlled G can be implemented locally by Bob with $O(n+k)$ CNOT gates and Toffoli gates.

Control qubit	Loop i
None	0
First qubit of q_c	$1, \dots, 2^{t-1}$
Second qubit of q_c	$2^{t-1} + 1, \dots, 2^{t-1} + 2^{t-2}$
\vdots	\vdots

Table 1. Control qubit for each loop i .

Control Qubits q_c . Note that $t = \log T$ qubits q_c are used as the control bits for U_{f_i} and G . Observe that for any unitary operator U ,

$$\frac{1}{\sqrt{T}} \sum_{c=0}^{T-1} |c\rangle U^c |\Psi_0\rangle = \frac{1}{\sqrt{T}} \sum_{c=0}^{T-1} |c\rangle \otimes (U^{c_0 2^{t-1}} U^{c_1 2^{t-2}} \dots U^{c_{t-1}} |\Psi_0\rangle). \quad (10)$$

We can use the first qubit of q_c (corresponding to c_0) as the control for 2^{t-1} times (for loop $i = 1, \dots, 2^{t-1}$), and the second one for 2^{t-2} times (for loop $i = 2^{t-1} + 1, \dots, 2^{t-1} + 2^{t-2}$), and so on; see Table 1. Note that one control qubit is enough to implement the controlled operators for each i . Therefore, controlled U_{f_i} or G is activated if and only if the state of the corresponding control qubit is $|1\rangle$. For instance, if $0 < i \leq 2^{t-1}$, we have

$$|c\rangle \sum_j \alpha_j |j\rangle |u\rangle \xrightarrow{\text{Controlled } U_{f_i}} |c\rangle U_{f_i}^{c_0} \left(\sum_j \alpha_j |j\rangle |u\rangle \right).$$

State Evolution. We now examine the state evolution in GroverIteration. Suppose the initial state of q_{c1} , q_{a1} and q_{d1} is

$$|\varphi\rangle = \frac{1}{\sqrt{T}} \sum_c \sum_j \alpha_{c,j} |j\rangle |\vec{0}\rangle.$$

Then its evolution can be summarised in Table 2, in which we only illustrate the part on q_{a1} and q_{d1} . It is worth noting that Step 3 and Step 6 will never change the state of q_{c1} , q_{a1} , q_{d1} and q_{c2} , q_{a2} , q_{d2} . This is because during the tests, all these qubits are preserved and only new constructed test states are sent to Bob. Therefore, the controlled Grover iteration is actually realized in procedure GroverIteration. Moreover, if Bob uses a trivial strategy in which all $f_i = f$, Eq.(10) is implemented. For nontrivial strategies, see Section 5.3.

4.3 Alice's Tests

Finally, we present the two test procedures called in Algorithm 1 and procedure GroverIteration to complete the picture of our protocol. Since they are similar, we only show procedure TestBob1 in this subsection. The differences between it and TestBob2 are briefly shown in Figure 1. The detailed descriptions of TestBob2 are given Appendix A. Some details of procedure TestBob1 are described as follows:

Step	State	
	Operators activated	Operators not activated
Step 1	$ c\rangle \sum_j \alpha_j j\rangle \vec{0}\rangle$	$ c\rangle \sum_j \alpha_j j\rangle \vec{0}\rangle$
Step 4 Alice $U_D(y)$	$ c\rangle \sum_j \alpha_j j\rangle d_{j\oplus y}\rangle$	$ c\rangle \sum_j \alpha_j j\rangle d_{j\oplus y}\rangle$
Step 4 Bob U_f	$ c\rangle \sum_j (-1)^{f(d_{j\oplus y})} \alpha_j j\rangle d_{j\oplus y}\rangle$	$ c\rangle \sum_j \alpha_j j\rangle d_{j\oplus y}\rangle$
Step 7 Alice $U_D(y)$	$ c\rangle \sum_j (-1)^{f(d_{j\oplus y})} \alpha_j j\rangle \vec{0}\rangle$	$ c\rangle \sum_j \alpha_j j\rangle \vec{0}\rangle$
Step 7 Bob G	$ c\rangle \sum_j (-1)^{f(d_{j\oplus y})} \alpha_j (G j\rangle) \vec{0}\rangle$	$ c\rangle \sum_j \alpha_j j\rangle \vec{0}\rangle$

Table 2. State evolution for $|c\rangle \sum_j \alpha_j |j\rangle |\vec{0}\rangle$ in procedure GroverIteration. Here “Operators activated” means $|c\rangle$ and i activate controlled operators.

Procedure TestBob1(i)

Output: “Dishonesty detected”, if Bob’s dishonesty is detected.

1 **begin**

2 Alice generates $\mu < \nu \in \{0, 1\}^k$, $c \in \{0, 1\}^t$, $m \in \{0, 1, \dots, n-1\}$,
 $x \in \{0, 1\}^n$, and $b \in \{0, 1\}$ uniformly at random;

3 Alice prepares $|\Phi\rangle = |c\rangle_{q_c} \otimes U_t(m, x, b) |0\rangle_{q_a, q_d}^{\otimes(n+k)}$ on new control qubits q_c ,
address qubits q_a , and data qubits q_d ;

4 Bob applies U_{f_i} on q_a and q_d ;

5 Alice applies $U_t(m, x, b)^\dagger$ on q_a and q_d , obtaining the state

$$|\Phi_1\rangle = |c\rangle_{q_c} \otimes U_t(m, x, b)^\dagger U_{f_i} U_t(m, x, b) |0\rangle_{q_a, q_d}^{\otimes(n+k)};$$

6 Alice and Bob repeat Step 3 to Step 5 to get $|\Phi_2\rangle$;

7 Alice measures all address and data qubits of $|\Phi_1\rangle$, and $|\Phi_2\rangle$, according to
the basis $\{|0\rangle, |1\rangle\}$. Let the outcomes be v and w , respectively, both in
 $\{0, 1\}^{n+k}$;

8 If $v_0 \neq w_0$, or $v_j = 1$, or $w_j = 1$ for any $j > 0$, **return** “Dishonesty
detected”;

9 **end**

- $\mu < \nu$ means the binary number represented by μ is smaller than that represented by ν .
- In this test, the state $|c\rangle$ on control qubits is not checked. It is introduced here, only because originally the states on control qubits are involved during the computation.
- $U_t(m, x, b) = U_{SWAP(0,m)} Z(x) X_0^b V(\mu, \nu) (W \otimes I_d)$, where $W = H^{\otimes n}$ and H is the Hadamard gate.
- $V(\mu, \nu)$ writes μ and ν into $|+\rangle_{q_a}^{\otimes n} |0\rangle_{q_d}^{\otimes k}$. It consists of at most k CNOT gates, where the control qubits are the first address qubit, and the target qubits range over all data qubits, where the first address qubit serves as the control, and all data qubits are the target. To be specific,

$$V(\mu, \nu) |0\rangle |\xi\rangle |\tau\rangle = |0\rangle |\xi\rangle |\tau \oplus \mu\rangle,$$

$$V(\mu, \nu) |1\rangle |\xi\rangle |\tau\rangle = |1\rangle |\xi\rangle |\tau \oplus \nu\rangle,$$

- Ancilla qubits q_{g1} and q_{g2} are involved.
- A controlled swap test is employed to test whether $|\Phi_1\rangle$ and $|\Phi_2\rangle$ are same.
- Step 8: The condition is a bit different.

Fig. 1. The difference of TestBob2 to TestBob1. See Appendix A for details.

	Honest Actions	Measurements on q_d	Measurements on q_a and q_d
Alice \rightarrow Bob	$ \psi_{0,0,0}(\mu, \nu)\rangle$	$ \psi_{0,0,0}(\mu, \nu)\rangle$	$ \psi_{0,0,0}(\mu, \nu)\rangle$
Bob \rightarrow Alice	$ \psi_{0,0,0}(\mu, \nu)\rangle$	$ 0\rangle +\rangle^{\otimes n-1} \mu\rangle$	$ 0\rangle \gamma\rangle \mu\rangle$
$V(\mu, \nu)$	$ +\rangle^{\otimes n} 0\rangle^{\otimes k}$	$ 0\rangle +\rangle^{\otimes n+k-1}$	$ 0\rangle \gamma\rangle 0\rangle^{\otimes k}$
$W \otimes I_d$	$ 0\rangle^{\otimes n+k}$	$ +\rangle 0\rangle^{\otimes n+k-1}$	$ +\rangle \omega\rangle 0\rangle^{\otimes k}$

Table 3. One possible situation of state evolution in Procedure TestBob1, where $\gamma \in \{0, 1\}^{n-1}$, and $\omega \in \{+, -\}^{n-1}$. Moreover it is assumed that $f(\mu) = f(\nu)$ and the test state is $|\psi_{0,0,0}(\mu, \nu)\rangle$. The control qubits are omitted. Unitary operators $U_{SWAP(0,0)}$, X_0^0 , $Z(0)$ are omitted as well, as they are all identity operators here.

for any $\xi \in \{0, 1\}^{n-1}$ and $\tau \in \{0, 1\}^k$. For simplicity, $V(\mu, \nu)$ will be abbreviated to V at some places.

- $U_{SWAP(0,m)}$ swaps the states of address qubits number 0 and number m .
- $Z(x)$ consists of a sequence of Pauli Z gates which act on address qubit j if and only if $x_j = 1$.
- X_0 denotes Pauli X gate acting on the first address qubit.
- Since all the component operators in $U_t(m, x, b)$ are self-adjoint, so is $U_t(m, x, b)$; that is, $U_t(m, x, b)^\dagger = U_t(m, x, b)$.

5 Execution of the Protocol

5.1 Test Rounds

To better understand our protocol, let us show in this section how it is executed. We first see how dishonest Bob cannot pass tests with a high probability.

- Definition 3.**
1. One execution of procedure TestBob1 or TestBob2 is called a *test round*.
 2. Correspondingly, one execution from Step 4 to Step 5 in procedure GroverIteration or one execution from Step 7 to Step 9 in Algorithm 1 is called a *computational round*.

One possible state evolution in procedure TestBob1 is given in Table 3, where the post-measurement state is assumed to be $|0\rangle|+\rangle^{\otimes n-1}|\mu\rangle$ or $|0\rangle|\gamma\rangle|\mu\rangle$ for some $\gamma \in \{0, 1\}^{n-1}$. We can see that if Bob is honest, he can always pass TestBob1. On the other hand, we present two examples to illustrate how Bob's attack can be detected (A detailed analysis is postponed to Section 7.6). First, we assume that Bob performs measurements only on the data qubits.

Example 1. Suppose in a test round of procedure TestBob1, Alice first sends a test state $|\psi_{0,0,0}(\mu, \nu)\rangle$ to Bob, where $f(\mu) = f(\nu)$. Bob performs measurements on the data qubits, gets post-measurement state $|0\rangle|+\rangle^{\otimes n-1}|\mu\rangle$, and then sends it back to Alice. Secondly, Alice sends the same test state $|\psi_{0,0,0}(\mu, \nu)\rangle$ to Bob. Then, as illustrated in Table 4,

1. if Bob does not perform measurements on the second test state, it will be detected by the condition $v_0 \neq w_0$ at Step 8 with probability 0.5.
2. if Bob performs measurements on the data qubits, then with probability 0.5, the post-measurement state is $|0\rangle|+\rangle^{\otimes n-1}|\mu\rangle$, and with the same probability, it is $|1\rangle|+\rangle^{\otimes n-1}|\nu\rangle$. For each case, it will be detected by the condition $v_0 \neq w_0$ at Step 8 with probability 0.5.

States after Bob's actions		Probability at Step 8
State #1	State #2	
	$ \psi_{0,0,0}(\mu, \nu)\rangle$	0.5
$ 0\rangle +\rangle^{\otimes n-1} \mu\rangle$	$ 0\rangle +\rangle^{\otimes n-1} \mu\rangle$	0.5
	$ 1\rangle +\rangle^{\otimes n-1} \nu\rangle$	0.5

Table 4. Probabilities to detect Bob's attacks in Example 1. "State #1" (resp. "State #2") stands for the first (resp. second) test state.

One situation not mentioned in the above example is that Bob first performs honestly, and then attacks on the second test state. But it is essential the same as the above example.

Another attack that Bob may take is to perform measurements on both the address and data qubits.

Example 2. Similarly to Example 1, Bob measures the address and data qubits for the first test state, gets post-measurement state $|0\rangle|\gamma\rangle|\mu\rangle$, and then sends it back to Alice. Then for the second test state, no matter what Bob does, it can be detected by one or both of the two conditions at Step 8 with probability ≈ 1 .

In the above two examples, we assumed that the test state is $|\psi_{0,0,0}(\mu, \nu)\rangle$ for simplicity. Other test states are similar. Furthermore, it was assumed that Bob directly sends the post-measurement state to Alice. Indeed, he can construct a new state and send it to Alice. This case can be detected as well; see Section 7.3.

5.2 Testing or Computing

The design idea of tests is to guarantee that Bob cannot know whether he is dealing with a test state or a computational state. In Algorithm 1 and procedure GroverIteration, the order of test and computational rounds are decided by the random number r . So it is clear that Bob does not know what states he is

dealing with. Every time he receives a quantum state, it may be a test state (with probability at least p). Figure 2 shows a flowchart that illustrates Bob's view for the T calls of controlled Grover iterations in Algorithm 1.

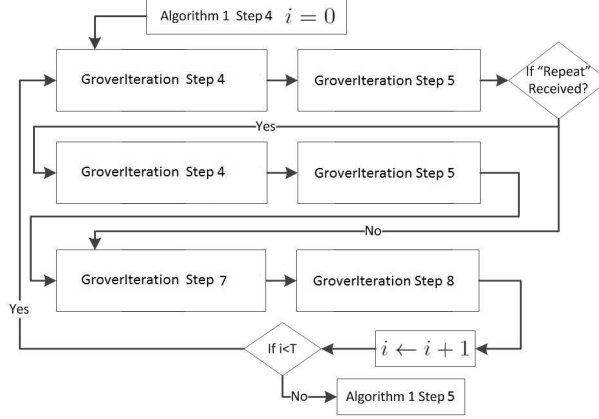


Fig. 2. Bob's view for the T calls of controlled Grover iterations in Algorithm 1. Indeed, in Alice's view, the first (resp. second) appearance of Steps 4 and 5 may be a test at Step 3 (resp. Step 6) when Alice employs a test in GroverIteration according to $r \leq p$ (resp. $p < r \leq 2p$).

5.3 Bob's Strategy

As said in Subsection 3.3, Bob's strategy is to add noises to f (thus applying f_i instead) in procedure GroverIteration, which cancel each other if Alice follows the protocol honestly. A detailed analysis will be given in Section 8. Here we observe:

$$\bar{G}U_D U_f U_D \bar{G}U_D I_{a,d} U_D \bar{G}U_D U_f U_D = \bar{G}, \quad (11)$$

where U_D is short for $U_D(y)$. This equation indeed represents the unitary operators after three iterations with $f_i = f$, $f_{i+1} = h$, and $f_{i+2} = f$, where h is the function corresponding to $I_{a,d}$ and $h(\mu) = 0$ for all $\mu \in \{0, 1\}^k$. So, a sequence of f, h, f, h or h, f, h, f leads to the identity operator, meaning that Bob does nothing. One step further from Eq. (11), we have:

$$\prod_{i=1}^j (\bar{G}U_D U_{f_i} U_D) \bar{G}U_D I_{a,d} U_D \prod_{i=1}^j (\bar{G}U_D U_{f_{j+1-i}} U_D) = \bar{G}, \quad (12)$$

for all j and all functions f_1, \dots, f_j on D . Another useful observation is

$$\bar{G}U_D I_{a,d} U_D \bar{G}U_D I_{a,d} U_D = I_{a,d}. \quad (13)$$

This means two repetitions of h do nothing.

We can construct strategies for privacy preserving based on Eqs. (11), (12) and (13). Let us first see a simple example.

Example 3. Suppose Bob wants to run Algorithm 1 with $T_0 = 8$ loops. He adds one control qubit to make $T = 16$. Then there are four control qubits, denoted by C_0, C_1, C_2, C_3 . Bob chooses C_1 as a confusing qubit, and add noise to the functions corresponding to C_0 . In detail,

- C_0 : h, h, f, f, h, h, f, f ,
- C_1 : f', h, f', h ,
- C_2 : f, f ,
- C_3 : f ,

where f' are functions different from f . At last the Fourier transformation is performed only on C_0, C_2, C_3 .

We now formally define the notion of Bob's strategy.

Definition 4. Suppose in Algorithm 1 there are $t = \log T$ control qubits C_0, \dots, C_{t-1} . We say a sequence of function f_0, \dots, f_{T-1} is a strategy \mathcal{S} for computing $f(D)$, if

- it is trivial, i.e. all $f_i = f$,
- or the following conditions are satisfied:
 - One control qubit C_u with $u < t - 1$ is chosen to be the confusing qubit.
 - Based on Eq. (11), Eq. (12) and Eq. (13), noises are added between the functions corresponding to C_0, \dots, C_u .
 - For C_w with $w < u$, the effect of its corresponding functions is equivalent to that of 2^{t-w-1} repetitions of f .
 - For C_u , the effect of its corresponding functions is the identity.

In conclusion, a strategy realizes Eq. (10) or

$$\begin{aligned} \frac{1}{\sqrt{T}} \sum_c |c\rangle G^{c'} |\Psi_0\rangle = \\ \frac{1}{\sqrt{T}} \sum_c |c\rangle \otimes (G^{c_0 2^{t-2} + c_1 2^{t-3} + \dots + c_{u-1} 2^{t-u-1} + c_u 2^{t-u-2} + \dots + c_{t-1}} |\Psi_0\rangle), \end{aligned} \quad (14)$$

where $c = \sum c_j 2^{t-j-1}$, and $c' = c_0 2^{t-2} + c_1 2^{t-3} + \dots + c_{u-1} 2^{t-u-1} + c_u 2^{t-u-2} + \dots + c_{t-1}$. If a confusing qubit is added, the final measurement is performed on the control qubits except C_u to get θ .

6 Correctness for Honest Parties

Now we start to prove the correctness of Algorithm 1. In this section, we consider the simplest case where Alice and Bob are both honest.

The discussion in Sections 4.2 and 5.3 showed that in Algorithm 1, the T calls of procedure GroverIteration realize controlled Grover iterations Eq.(10) or Eq.(14), depending on which strategy (see Definition 4) Bob employs. So Algorithm 1 executes the quantum counting algorithm [5] twice, independently on $q_{c1}, q_{a1}, q_{d1}, q_{g1}$, and $q_{c2}, q_{a2}, q_{d2}, q_{g2}$. Then for Problem 1, we directly have the following result.

Theorem 1. (*[5, Theorem 5, Theorem 6]*) *In Algorithm 1, if Alice and Bob are both honest and Bob employs a trivial strategy, then for $i \in \{1, 2\}$,*

$$|s_i - s| < \frac{2\pi}{T}\sqrt{s} + \frac{\pi^2}{T^2}, \forall i \in \{1, 2\}, \quad (15)$$

holds with probability at least $\frac{8}{\pi^2} > 0.8$, where $s = f(D) = \frac{1}{N} \sum_j f(d_j)$ is the correct answer.

Therefore, by setting $T > 100/\sqrt{s_{\min}}$ for a trivial strategy or $T > 200/\sqrt{s_{\min}}$ for a nontrivial strategy, we immediately obtain:

Corollary 1. *In Algorithm 1, if Alice and Bob are both honest, then for $i \in \{1, 2\}$,*

$$\begin{cases} | \frac{s_i}{s} - 1 | < \frac{2\pi}{100} \sqrt{\frac{s_{\min}}{s}} + \frac{\pi^2}{10^4} \frac{s_{\min}}{s} < 0.07, & s \geq s_{\min}, \\ \frac{|s_i - s|}{s_{\min}} < \frac{2\pi}{100} \sqrt{\frac{s}{s_{\min}}} + \frac{\pi^2}{10^4} < 0.07, & s < s_{\min}, \end{cases}$$

holds with probability at least $\frac{8}{\pi^2} > 0.8$, where $s = f(D) = \frac{1}{N} \sum_j f(d_j)$ is the correct answer, and s_{\min} is the preset threshold of supports.

This corollary gives the relative error and success probability for Bob. Since usually s_{\min} is set to be a constant, say 0.2, 0.1 or 0.01, the number T of iterations does not depend on the size of the database.

7 Protecting Alice's Privacy

In this section, we continue to prove correctness of the protocol and show how it can protect Alice's privacy. Only procedure TestBob1 is considered, and the results for procedure TestBob2 are similar and thus omitted.

Dishonest Bob may employ attacks to read information from $q_{c1}, q_{a1}, q_{d1}, q_{g1}$, and/or $q_{c2}, q_{a2}, q_{d2}, q_{g2}$. His attacks can be classified according to the number of rounds/iterations that these attacks cost.

7.1 One-round Attacks

Definition 5 (One-round attack). *A one-round attack consists of one or more successive steps of the following:*

1. *Bob sends some qubits to Alice,*
2. *Alice applies U_D , and sends these qubits to Bob,*

3. Bob's actions,
4. Bob sends some qubits to Alice.

For instance, a one-round attack may consist of Steps 1-2, Steps 2-4, or Steps 1-4. In this subsection, we list some one-round attacks which leak information.

The following are several typical one-round attacks:

Example 4 (Attack1). Bob sets q_a to be a single address $|i\rangle$ and q_d to be blank $|\vec{0}\rangle$. Then he sends q_c, q_a, q_d to Alice. After Alice applies U_D , Bob receives $|i\rangle|d_i\rangle$. Finally, he can measure q_d to get d_i .

Example 5 (Attack2). After Bob receives $\frac{1}{\sqrt{T}} \sum_c \sum_j \alpha_{c,j} |j \oplus y\rangle |d_{j \oplus y}\rangle$, he performs measurements (1) on q_d to get some $d \in D$, or (2) on q_a and q_d to get $d_{j \oplus y}$.

Besides directly reading data from q_a and q_d by measurements, Bob may use some unitary gates (e.g. CNOT) to copy data on additional blank qubits, say q_e . Then he can read information from q_e later.

Example 6 (Attack3). After Bob receives $\frac{1}{\sqrt{T}} \sum_c \sum_j \alpha_{c,j} |j \oplus y\rangle |d_{j \oplus y}\rangle$, he add ancilla qubits and performs unitary operators to store data, i.e.

$$\frac{1}{\sqrt{T}} \sum_c \sum_j \alpha_{c,j} |j \oplus y\rangle |d_{j \oplus y}\rangle |e_{j \oplus y}\rangle.$$

7.2 Detection of One-round Attacks

We first show that TestBob1 can detect Bob's one-round attacks. The main assumption here is:

- Whenever Bob tries to attack, he believes that he cannot distinguish the following two situations from each other:
 1. He is dealing with a test state.
 2. He is dealing with a computational state.

This assumption is reasonable because no one will cheat if he knows that he is dealing with a test state, which carries no useful information about database D .

Example Attacks Now let us see what happens if Bob cheats in a test. As the starting point, we focus on the attacks in Examples 4, 5 and 6, since they are simplest and typical ones.

Lemma 1 (Attack1). *Suppose, in a test, it is Bob's turn to send back computational qubits to Alice. Bob prepares $|\varphi\rangle|a\rangle|d\rangle$ in Procedure TestBob1, where $|\varphi\rangle \in \mathcal{H}_c$, $a \in \{0, 1\}^n$ and $d \in \{0, 1\}^k$, and sends this state to Alice. Then it can be detected with probability at least $1 - \frac{1}{N}$.*

Lemma 2 (Attack1). *Suppose Bob successfully sends $|\varphi\rangle|a\rangle|d\rangle$ to Alice. If this communication is followed by a test (Procedure TestBob1) and he performs measurements on q_a and q_d (resp. only a measurement on q_d) [in order to get private information], then it will be detected with probability at least $1 - \frac{1}{N}$ (resp. $\frac{1}{2}$).*

Lemma 3 (Attack2). *Suppose Bob performs measurements on q_a and q_d (resp. only a measurement on q_d) in Procedure TestBob1. Then it will be detected with probability at least $1 - \frac{1}{N}$ (resp. $\frac{1}{2}$).*

Lemma 3 is essentially the same as Lemma 2, since in both of them the same measurements are performed on a test state. But the analysis of **Attack3** is much more complicated.

Lemma 4 (Attack3). *Suppose in Procedure TestBob1, Bob adds q_g to q_a and q_d and uses a unitary operator E to entangle q_g to q_a and q_d :*

$$E|i\rangle|d\rangle|0\rangle = |i\rangle|d\rangle|\lambda_{i,d}\rangle, \quad (16)$$

where $|\lambda_{i,d}\rangle$ is a pure state of q_g . In order to read information, $|\lambda_{i,d}\rangle$ should vary for i, d . Then it will be detected with a positive probability P_{DET} depending on E . In particular,

1. if $E|i\rangle|d\rangle|0\rangle = |i\rangle|d\rangle|i\rangle|d\rangle$, then $P_{DET} \geq 1 - \frac{1}{N}$.
2. if $E|i\rangle|d\rangle|0\rangle = |i\rangle|d\rangle|d\rangle$, then $P_{DET} = 0.5$.

General Attacks Now let us consider general attacks. The following theorem identifies all of Bob's actions that enable him to pass Alice's tests.

Theorem 2. *Suppose Bob applies a super-operator $\mathcal{E} = \sum_j E_j \circ E_j^\dagger$ on q_a , q_d and blank q_g in a round of TestBob1. If it always passes the test, \mathcal{E} can be written as*

$$\mathcal{E} = U \circ U^\dagger \otimes \mathcal{E}_g,$$

where U is a unitary operator on q_a and q_d , and \mathcal{E}_g is a super-operator on q_g .

Its implication to privacy is the following:

Corollary 2. *If Bob wants to always pass the tests, he cannot read any information from q_a and q_d by one-round attacks.*

Note that in procedure GroverIteration, we only add tests around Step 4. One question directly arises: what happens if Bob attacks at Step 7? The following lemma answers this question.

Lemma 5. *At Step 7, if Bob performs measurements to read information or sends a special state for future attacks at Step 4, then it can be detected by procedure TestBob1.*

7.3 Impossibility of Recovery

In this subsection, we further show that Bob cannot distinguish the test states. Therefore, he cannot recover his measurement even if he finds that he is dealing with a test state.

The impossibility of distinguishability is based on the following observation:

Lemma 6. *The test set $\{|\psi_{m,x,b}(\mu, \nu)\rangle\}$ can be decomposed into the union of $n(2^k - 1)$ disjoint bases:*

$$\{|\psi_{m,x,b}(\mu, \nu)\rangle\} = B_1 \cup \dots \cup B_{n(2^k-1)},$$

where $B_i \cap B_j = \emptyset$, and B_i is a orthogonal basis of the Hilbert space of q_a and q_d , for all $i \neq j$.

The above lemma then implies that Bob cannot distinguish all of the test states.

Lemma 7. *Suppose Bob tries to use measurement $\{M_v\}$ on q_a and q_d to find which specific test state Alice sends. Then the correct probability is*

$$\Pr(m, x, b, \mu, \nu | M_v) \leq \frac{1}{n(2^k - 1)}. \quad (17)$$

In other words, if the measurement outcome is v , then the probability that the state is $|\psi_{m,x,b}(\mu, \nu)\rangle$ is at most $\frac{1}{n(2^k-1)}$. More generally,

$$\Pr(B | M_v) = \sum_{|\psi_{m,x,b}(\mu, \nu)\rangle \in B} \Pr(m, x, b, \mu, \nu | M_v) \leq \frac{1}{n(2^k - 1)}, \quad (18)$$

where B is an orthogonal basis as in Lemma 6.

Now we can present the main theorem in this subsection.

Theorem 3. *Suppose Bob uses a measurement $\{M_v\}$ to read information in a test round, and sends a new state $|\psi_{m',x',b'}(\mu', \nu')\rangle$ (based on the measurement results) back to Alice instead. Then, the expected success probability that he passes the test is at most $\frac{1}{4} + \frac{3}{4n(2^k-1)}$.*

The above theorem ensures that Bob cannot recover the test states after attacks. Recall from Theorem 2 that if Bob directly sends states back to Alice after his attacks, it will be detected. So, these two theorems together warrant that once Bob wants to read private information from Alice through one-round attacks, it will be detected.

7.4 Multi-round Attacks

We have discussed one-round attacks in the last subsection. In this subsection, we further consider multi-round attacks. A multi-round attack will finish in more than one calls of procedure `GroverIteration`. More precisely, we have:

Definition 6. *A multi-round attack consists of the following steps:*

1. *Bob sends some qubits to Alice,*
2. *Several calls of Procedure `GroverIteration` are executed,*
3. *Bob performs measurements to read information after receiving qubits from Alice.*

We will see in Sections 7.4 and 7.6 that multi-round attacks can actually be ignored, since (1) they can hardly leak information, and (2) they are very hard to be detected. But here let us see two typical multi-round attacks:

Example 7. Bob employs function $f(x) = \delta(x, d)$ as the target function, where $\delta(x, d) = 1$ if and only if $x = d$. Then Bob runs the protocol honestly to find whether $d \in D$.

This function discloses the information whether $d \in D$ and can be treated as an attack, since we only allow target functions to be maps indicating the inclusion relation \subseteq . For this kind of attacks, Alice can construct tests to detect it with a certain probability, although this probability is extremely low (see Appendix D.1).

Fortunately, we can ignore this attack because (1) if $\text{supp}(d)$ is high, then the information $d \in D$ is no longer private information when mining association rules or decision trees, and (2) if $\text{supp}(d)$ is low, the result can be hardly derived from Algorithm 1 (see Section 7.6 for more details).

Another attack focuses on more specific information.

Example 8. Bob employs Oracle

$$U_f|j\rangle|d_j\rangle = (-1)^{\delta(j,i)g(d_j)}|j\rangle|d_j\rangle,$$

as the target function in Algorithm 1, where $g(x) = 1$ if and only if $x \subseteq d$. One alternative attack is $g(x) = \delta(x, d)$.

As shown in the next lemma, this kind of attacks is very hard to detect.

Lemma 8. *Suppose Bob acts as in Example 8, and Alice only employs tests based on state comparison in a single round (the tests are not restricted to those in this paper). It can be detected in a single round with probability at most $O(\frac{1}{N}) = O(\frac{1}{2^n})$. Furthermore, Bob can pass all tests in one execution of Algorithm 1 with probability approximately 1.*

Fortunately, since the database O_D is modified to be $U_D(y)$, Example 8 is reduced to Example 7 finally. Indeed, Bob wants finally to get the exact form of d_j by employing attacks in Example 8. But since d_j is changed to be $d_{j \oplus y}$ and Bob does not know y , Bob only gets information $d \in D$ for some d . This is exactly the case of Example 7.

7.5 Attacks on q_c and q_g

In the previous subsections, we only consider attacks on q_a or on q_d . In this subsection, we analyse attacks on the two parts jointly.

First, by the following observations, we can see that q_c will not introduce further information leakage:

- There is no information about D on q_c .
- Bob cannot verify whether the current round is a test round by measurements on q_c . This is because no matter Bob performs measurements on q_c in a test round or an original round, the outcome distributions are the same, i.e.,

$$\Pr(c = i | \text{test round}) = \frac{1}{T} = \Pr(c = i | \text{original round}). \quad (19)$$

Second, for q_g , since q_g is entangled to q_d , attacks on q_g are the same as the attacks on q_d , which we have already analysed.

7.6 Privacy Analysis

Now, we are able to analyse the privacy level of the entire protocol. Let us first examine information disclosed by one-round attacks, and then give the privacy analysis for multi-round attacks.

The Entire Database In this subsection, we analyse the privacy of the entire database; that is, how much of D will be disclosed if Bob is dishonest? Consider the following:

Example 9. Suppose Alice is a data provider, who sells data, and Bob is a customer, who wants to buy some access to the data from Alice. Alice wants to keep her data private, as she wants to sell it to other costumers. Bob wants to keep his research private, as his research outcome may bring outcomes. So he will not send the function f to Alice.

In this example, Alice tries to preserve the entire database. Then how many transactions will be disclosed in our protocol:

Case 1. Bob is honest: He exactly follows the protocol. Before measurements in Algorithm 1, due to the quantum counting algorithm [5], he holds the state

$$\sum_c \sum_j \alpha_{c,j} |c\rangle |j\rangle |\vec{0}\rangle |g_j\rangle = \frac{1}{\sqrt{T}} \sum_c |c\rangle (\beta_{c,0} |\varphi_0\rangle |\vec{0}\rangle |0\rangle + \beta_{c,1} |\varphi_1\rangle |\vec{0}\rangle |1\rangle),$$

where $g_j = f(d_{j \oplus y})$, and $\alpha_{c,j}$, $\beta_{c,0}$, $\beta_{c,1}$ are amplitudes. Since honest Bob only performs measurements on the control qubits q_c and ancilla qubit q_g of this state, he only gets the information of $f(D)$. As he knows nothing else, no transactions in D is disclosed.

Case 2. Bob is semi-honest: He may do further computation on the state $|\theta\rangle |\varphi_j\rangle |\vec{0}\rangle |j\rangle$ with $j = 0$ or $j = 1$, which he holds after the final computation.

From this state, the information, which Bob can further get by measurements on the address qubits q_a , is whether $g_j = f(d_{j \oplus y})$ is 1 or 0 for some $j \in \{0, 1\}^n$. Totally he can get this information g_{j_1} and g_{j_2} for two address j_1 and j_2 randomly generated from measurements in one run of Algorithm 1, as there are two copies of states in one run. But unfortunately Bob does not know y , and Alice changes y in every run of Algorithm 1. This means the information he gets is useless. In detail, note that $g_j = f(d_{j \oplus y})$ is a random variable dependent on y . Since y is chosen uniformly at random, we have:

$$\Pr(g_j = 1) = f(D), \forall j.$$

So what Bob can get from g_j is $f(D)$, which he already known from the honest computation. Therefore, Bob disclose no detailed transaction in D .

Case 3. Bob is dishonest: He may perform measurements on the state received from Alice at any time. In previous subsections, we already observed that once Bob tries to get information in a test round through measurements, he may have a probability at least 0.5 to be detected. As a consequence, Alice will stop the whole computation. Then the expected number E_c of rounds that Bob can cheat before being detected, may be computed as follows. If Bob's attack happens in the first (resp. second) round of a loop i , it will be a test round with probability p (resp. 0.5). So each time Bob tries to get information through one-round attacks, it will be detected with probability at least $0.5p$. Thus, the expected numbers of one-round attacks before being detected is

$$E_c \leq \sum_{i \geq 1} i * 0.5p * (1 - 0.5p)^i = \frac{2}{p} - 1 = O(1/p).$$

Therefore, dishonest Bob can get at most a constant number of transactions from D .

To conclude this section, let us see the advantage of our quantum protocol over a classical method. Usually, a classical data provider will provide a modified database D' , generated from D by adding noise into it, to Bob. So, if the quantum protocol is run on D , it is not appropriate to compare it with a classical protocol. But the quantum protocol can also run on D' , by combining it with a classical one together (see Section 10.1). A comparison of the quantum protocol (combined with a classical one) with a classical protocol is shown in Table 5. In this table, $O(TM)$ is the number of transactions disclosed without protection in the protocol.

Multi-round Attack In Section 7.4, we already mentioned that multi-round attacks can be ignored in our quantum protocols. Now we are ready to give a detailed explanation.

Suppose that Bob employs function $f(x) = \delta(x, d)$ in order to learn whether $d \in D$. He uses this function to run Algorithm 1 several times and get an approximate result $s \approx |\{j : d = d_j\}|/N$. Then there are the following three situations:

	Honest Bob	Semi-honest Bob	Dishonest Bob
Quantum Protocol	0	≈ 0	$O(\frac{1}{p})$
Quantum Protocol without tests	0	≈ 0	$O(TM)$
Classical Method	N	N	N

Table 5. Number of transactions disclosed in D or D' . $p \in (0,1)$ is a constant, N is the size of database, T is the number of iterations in one run of Algorithm 1, and M is the total number of runs of Algorithm 1.

- $s > s_{\min}$, where constant s_{\min} is the threshold of support. Then this result is not treated to be private, as it cannot be distinguished from that of a *frequent itemset* and thus can be mined by Bob legally. For instance, since $\text{supp}(d) = |\{j : d \subseteq d_j\}|/N \geq |\{j : d = d_j\}|/N \approx s$, Bob can first get $\text{supp}(d)$ legally. Then he computes $\text{supp}(d')$ for possible supersets $d' \supseteq d$ to approximate s .
- $s < s_{\min}$, but s is not far from s_{\min} . In this case, since parameter T is determined by s_{\min} , the results may be not far to s_{\min} . For instance, if T is set to be $T > 100/\sqrt{s_{\min}}$, then by Corollary 1 we see that Bob may get result $0.07s_{\min}$ with probability greater than 0.8. So this still cannot be treated to be private, because this result may be probably mined by Bob legally on a *candidate itemset*.
- $s \ll s_{\min}$. In this case, Bob has to enlarge T to get s without intolerable errors, for instance, $T > 100/\sqrt{s}$. Since Bob does not know s before computation, he has to adjust T again and again [5] or directly sets a very large T . The comparison of costs for this case is given in Table 6.

s	N_R	C-cost	Q-cost
$s \ll s_{\min}$	1	$O(Nk)$	$O((C_D + k)/\sqrt{s})$
	L	$O(Nk)$	$O(L(C_D + k)/\sqrt{s})$

Table 6. Comparison of cost to check whether $d \in D$. In this table, s is the frequency of transactions d_j , satisfying $d_j = d$. N_R is the number of different rules $d \in D$, which Bob wants to check. “C-cost” is the cost on classical database D or D' , and “Q-cost” is the cost of multi-round attacks on quantum database U_D or $U_{D'}$. C_D is the cost to call $U_D/U_{D'}$ once. See Section 10.1 for $U_{D'}$.

In Table 6, we notice that usually it is cheaper to cheat in a quantum database U_D if L is small, since it is a search problem to check whether $d \in D$. So one method to overcome this weakness is to combine a classical protocol and a quantum one together: roughly speaking, Alice first modifies D to another D' , and then runs the protocol on $U_{D'}$ (see Section 10.1 for more discussions about this point). After combining the classical and quantum protocols together, it is still faster for Bob to cheat on quantum database $U_{D'}$. But the information he

gets on $U_{D'}$ is the same as that on D' . Then our quantum protocol is at least as good as a classical one for this function.

Before concluding this section, let us briefly consider Alice's strategy for multi-round attacks. In order to read small s , Bob requires large T . So Alice can set an upper bound for T . Then for a rule $d \in D$ with a low frequency, it can hardly be mined correctly with small T .

8 Protecting Bob's Privacy

In Section 7.6, we showed from the Alice's side how our quantum protocol can protect privacy. In this section, we analyse Bob's privacy in terms of his functions f . For this purpose, it is certainly appropriate to assume that Bob itself is honest. Otherwise, if Bob is dishonest, he can protect his privacy by never sending f .

We first consider semi-honest Alice, and the analysis for honest Alice is similar. Semi-honest Alice follows the protocol, but she will do further computation based on measurement outcomes on the test states. In each test round, Alice may get the information about whether $f_i(\mu) = f_i(\nu)$ for some randomly generated μ, ν . Now we see how many pairs (μ, ν) are required for this task. For association rule mining, there are totally at most 2^k functions (itemsets). For each pair, Alice compares $f_i(\mu)$ and $f_i(\nu)$, and gets one-bit information of $f_i(\mu) = f_i(\nu)$. So, she has to build a k -level binary decision tree to include all possible 2^k leaves. Consequently, in general the number of test rounds is at least $k/2$ to recover one f as there are two copies in each round. Since (1) there is at most only one test round in each loop i , and (2) the test round appears randomly, Alice can hardly get enough information to recover f . Moreover, as Bob adds noises into f (see Section 5.3), the information Alice gets may be wrong and thus useless. It is worth noting that some privacy leakage might happen in the last loop $i = T - 1$. In Definition 4, no noise is added for $i = T - 1$, which means $f_{T-1} = f$. So, if a test round appears, then Alice may know $f(\mu) = f(\nu)$ for some randomly generated (μ, ν) . This leakage is not serious, since there are 2^{k-1} functions (itemsets) satisfying this one-bit property.

For dishonest Alice, the situation is different. Dishonest Alice may set a test at each loop and construct a special policy to choose test states to read information about f . The simple strategy in Definition 4 is not sufficient to protect Bob's privacy. Fortunately Bob can protect his privacy from Alice's attacks by simply adding a second confusing qubit in Definition 4. Together with other methods, Bob can further improve his privacy level; see Appendix C for details.

Remark 1. The privacy analysis for the case that Bob does not add noise and tests is postponed to Appendix D.2.

9 Complexity Analysis

The aim of this section is to analyse the complexity of our protocol. Actually, the cost of Algorithm 1 is easy to settle. Let us only consider association rule mining

as an example. Suppose that the threshold of support is s_{\min} , and Bob totally run M times of Algorithm 1 (since he wants to compute the supports of different itemsets or achieve a high accuracy by repetitions). Then the *computational complexity* is simply

$$O(MT(C_D + k + n + t)) = O(M(C_D + k + n + t)/\sqrt{s_{\min}}),$$

where C_D is the cost of one call of Alice's database. So, if a *quantum database* is available (e.g. as a quantum random access memory [8]), then $C_D = O(nk)$, and the total computational is $O(M(nk + t)/\sqrt{s_{\min}})$. Since $t = \log T$, and $T \leq \frac{\pi}{4}\sqrt{N}$ (meaning that the accuracy level is $\frac{1}{N}$), we have $t = O(n)$. So, the total computational complexity is $O(Mnk/\sqrt{s_{\min}})$. On the other hand, if the data is stored in a *classical database*, then Alice has to use certain quantum gates to construct O_D , which costs $O(N(n + k))$, and the total computational complexity is $O(MN(n + k)/\sqrt{s_{\min}})$. The *communication complexity* can be analysed similarly, and is $O(MT(t + n + k)) = O(M(n + k)/\sqrt{s_{\min}})$. The results are illustrated in Table 7. Note that in many applications the communication cost may not be important and necessary. For a centralized database, Alice and Bob are at the same location, and we can imagine Alice as a preset database with an access to Bob. In this case, during communicating the problem of privacy including channel noise is not serious or even does not happen at all.

	T-cost	C-cost
Quantum database	$O(Mnk/\sqrt{s_{\min}})$	$O(M(n + k)/\sqrt{s_{\min}})$
Classical database	$O(MN(n + k)/\sqrt{s_{\min}})$	$O(M(n + k)/\sqrt{s_{\min}})$

Table 7. Cost of the entire quantum protocol, with data stored in a quantum database or a classical database. “T-cost” means computational complexity, and “C-cost” means communication complexity.

Now let us compare the complexity of our quantum protocol with that of a classical algorithm. Many different classical algorithms for the same task have been developed in the literature, and each of them has a different cost and accuracy level. For those classical algorithms that require to input the whole database D or D' to achieve a better result, the computational and communication costs are both $O(Nk)$. Note that usually in practice $M \ll N$; for instance, $N = 10^6$, and Bob might only care the most important hundreds of association rules with $M < 10^3$. Then the costs of quantum protocol except the lower left entry of Table 7 are better than those of classical algorithms, as $Nk > M(n + k)/\sqrt{s_{\min}}$.

10 Discussions

In this section, we point out several possibilities for further improvements of the protocol.

10.1 Combining Classical and Quantum Protocols

As mentioned before, combining our quantum protocol with a classical one is a way to further improve the privacy for Alice. In this strategy, there are totally two steps. The first step is to apply a classical approach on D to get D' . Most of the classical approaches in the literature are suitable for this step; for example, randomly flipping elements in each transaction [18], replacing elements partly [7], swapping elements among different transactions [6]. The second step is to store D' into a quantum database $O_{D'}$. Then our quantum protocol can be executed on $O_{D'}$.

The benefit of this method is obvious. Suppose that a classical approach changes D to D' . Then in the classical case, Bob knows the entire D' . In the quantum case, however, Bob only knows a small part of D' , even if he is dishonest (see Section 7.6). So, this combination protects Alice's privacy much better than solely using a classical approach.

The disadvantage is that additional error may be introduced. A combination of our quantum protocol and a classical one has two places to generate errors: one is from randomization in the classical protocol, the other is from the quantum counting. Thus, the total error may be larger than that of the classical algorithm.

10.2 Decision Tree Learning

Our protocol was presented mainly for association rule mining, but Algorithm 1 can be directly used to mine decision trees. Consider the basic algorithm for decision tree mining proposed in [17]. Here, we show how it can be combined with Algorithm 1 so that privacy can be protected.

Example 10. Suppose that Alice holds a database

$$D = \langle (d_0, g_0), (d_1, g_1), \dots, (d_{N-1}, g_{N-1}) \rangle,$$

where $d_j \in \{0, 1\}^k$, $g_j = f(d_j) \in \{0, 1\}$ for a function f . Suppose that K is the set of all first k attributes. Bob wants to build a decision tree, with one attribute in K at each node, to decide $f(d)$ for any input d , based on the database D . The algorithm is shown below:

1. Set $L = 0$, and the root r is set to be an empty node.
2. For each empty node on level L , computes its corresponding attribute:
 - Suppose F is the set of attributes corresponding to the ancestors of this node.
 - Denote $A = \{y : y \in F\}$. Bob computes the support s_0 of $(A, 0)$ and s_1 of $(A, 1)$ by Algorithm 1. If $H(A) = -\sum_i s_i \log s_i$ is smaller than a preset threshold H_{\min} , the node is set to be value 0 (if $s_0 > s_1$) or 1 (if $s_0 < s_1$) for f . No child is generated. Return.
 - For each attribute $x \in K \setminus F$, denote $A_x = \{x\} \cup \{y : y \in F\}$. Alice computes the support $s_0(x)$ of $(A_x, 0)$ and $s_1(x)$ of $(A_x, 1)$ by Algorithm 1. Then she computes the entropy $H(x) = -\sum_i s_i(x) \log s_i(x)$.

- Bob chooses the attribute y which maximizes $H(y) = \max H(x)$. The corresponding attribute of this node is set to be y , and two children are generated. Each is for value 0 or 1 of y .
- 3. If no child is generated in this level L , terminates. Otherwise, $L := L + 1$ and goes to Step 2.

The privacy and complexity analyses for the above example are similar to what we did for association rule mining in the previous sections.

10.3 Dishonesties of Both Alice and Bob

In this paper, we presented a method for Alice to deal with dishonest Bob, and also a method for Bob to deal with dishonest Alice. In particular, we showed:

- If Alice and Bob are both honest, our protocol computes the final results and preserves privacy for both parties.
- If Alice is honest and Bob is dishonest, our protocol can (1) compute the final results, (2) detect Bob's attack to protect Alice's privacy, and (3) preserve Bob's privacy.
- If Alice is dishonest and Bob is honest, our protocol can (1) compute the final results, and (2) preserve privacy for both Alice and Bob (by adding a second confusing qubit).

Then a question naturally arises: what happens when both Alice and Bob are dishonest? In this case, there is no definite conclusion. It depends on what actions are taken. For example, suppose:

- Alice acts honestly if i is odd. If i is even, she stores the computational state aside for the next loop, and tries to read $f(\mu)$ by sending Bob a state like $\frac{1}{\sqrt{2}}|c\rangle|0\rangle^{\otimes n-1}(|0\rangle|\mu\rangle + |1\rangle|\bar{1}\rangle)$.
- Bob acts honestly if i is even. If i is odd, he performs measurements to read d_j , and sends to the post-measurement state back to Alice.

Then in each loop i , either Alice or Bob cheats, and the computation cannot be accomplished. But if Bob's actions are switched, then both Alice and Bob act honestly when i is odd. Furthermore, if Alice stores the computational states properly when i is even, then the computation can be accomplished (but with a larger error).

10.4 Compatibility with Other Quantum Algorithms

Note that in the protocol, Alice's part is compatible with other quantum algorithms in the sense that if Bob wants to run a quantum algorithm on Alice's database other than quantum counting, he only needs to modify his part of protocol. For example, suppose Bob wants to find whether a given transaction d is in the database by running a quantum walk on a hyper cube [20], where each node corresponds to an address j and a transaction d_j (or $d_{j\oplus y}$). In a quantum walk-based search, the operator G is replaced by some other operators. What we need to do are the following modifications on Bob's part:

- Change the initial state of the control qubits. In Algorithm 1, Alice does not check the initial state on control qubits. So for the searching problem, Bob can simply set all control qubits to be $|1\rangle$.
- Remove Step 14 in Algorithm 1 and change his actions at Step 7 in procedure GroverIteration.

It is easy to see that privacy of both parties is preserved in the same way as our original protocol.

10.5 Parameter p in Algorithm 1

The parameter p in Algorithm 1 indicates how frequently tests are employed. Obviously, for different models, the best choice of p varies. Note that p only matters in (1) detecting Bob's one-round attacks (dishonest actions), and (2) disclosing Bob's privacy f by comparing $f(\mu)$ and $f(\nu)$. So, $p = 0$ or $p \rightarrow 0$ is preferred for honest or semi-honest Bob. If Bob is dishonest, the situation becomes quite different:

- Honest Alice: A big p is preferred, as it protects Alice's privacy better than small p .
- Semi-honest Alice: Either a big or small p is not the best choice, since one party's privacy is likely to be disclosed in both cases. So, a medium p is the most suitable choice.
- Dishonest Alice: No best choice exists, because the protocol may not work if Alice always cheats.

The preferred choices of p are summarised in Table 8. However, Alice and/or

		Bob		
		Honest	Semi-honest	Dishonest
Alice	Honest	$p \rightarrow 0$	$p \rightarrow 0$	Big p
	Semi-honest	$p \rightarrow 0$	$p \rightarrow 0$	Medium p
	Dishonest	$p \rightarrow 0$	$p \rightarrow 0$	–

Table 8. Preferred choice of p in Algorithm 1 for different models.

Bob cannot know which situation they are facing. So, Table 8 is helpless in practice. Generally speaking, Alice prefers a big p . But if p is too big, Bob's privacy will be disclosed when Alice is not honest. In Section 7.6, it was shown that if N is big enough, the ratio of information (transactions) disclosed is nearly 0 for any $p \in (0, 1)$. So, in practice, $p = 0.05$ may work well. Indeed, the most important implication of parameter $p \in (0, 1)$ is not to detect Bob's privacy but to tell Bob that once he cheats, he may be caught. This fact may force Bob to be honest.

References

1. Agrawal, R., Evfimievski, A., Srikant, R.: Information sharing across private databases. In Proceedings of the 2003 ACM SIGMOD international conference on Management of data, pp. 86-97. ACM, New York (2003)
2. Agrawal, R., Imielinski, T., Swami, A.: Mining Association Rules between Sets of Items in Large Databases. In: Proceedings of the 1993 ACM SIGMOD international conference on Management of data, pp. 207-216. ACM, New York (1993)
3. Bennett, C. H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science* 560, 7-11 (2014)
4. Boyer, M., Brassard, G., Høyer, P., Tapp, A.: Tight bounds on quantum searching. *Fortsch. Phys.* 46 , 493-506 (1998)
5. Brassard, G., Høyer, P., Tapp, A.: Quantum counting. In: ICALP 1998, LNCS, vol. 1443, pp. 820-831. Springer, Heidelberg (1998)
6. Estivill-Castro, V., Brankovic, L.: Data Swapping: Balancing Privacy against Precision in Mining for Logic Rules. In: DaWaK 1999. LNCS, vol. 1676, pp 389-398. Springer, Heidelberg (1999)
7. Evfimievski, A., Srikant, R., Agrawal, R., Gehrke, J.: Privacy preserving mining of association rules. *Information Systems*, 29(4), 343-364 (2004)
8. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum Random Access Memory. *Phys. Rev. Lett.* 100, 160501 (2008).
9. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum Private Queries. *Phys. Rev. Lett.* 100, 230502 (2008).
10. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: STOC 1996, pp. 212-219, ACM, New York (1996)
11. Kobayashi, H., Matsumoto, K., Yamakami, T.: Quantum certificate verification: Single versus multiple quantum certificates. arXiv:quant-ph/0110006, (2001)
12. Kargupta, H., Datta, S., Wang, Q., Sivakumar, K.: On the privacy preserving properties of random data perturbation techniques. In: Third IEEE International Conference on Data Mining, pp. 99-106. IEEE (2003)
13. Kotsiantis, S., Kanellopoulos, D.: Association Rules Mining: A Recent Overview. *International Transactions on Computer Science and Engineering*, 32 (1), 71-82 (2006)
14. Lloyd, S., Mohseni, M., Rebentrost, P.: Quantum algorithms for supervised and unsupervised machine learning. arXiv:1307.0411.
15. Lloyd, S., Mohseni, M., Rebentrost, P.: Quantum principal component analysis. *Nature Physics* 10, 631 (2014).
16. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press (2000)
17. Quinlan, J.R.: Induction of Decision Trees. *Machine learning*, 1(1), 81-106 (1998)
18. Rizvi, S.J., Haritsa, J.R.: Maintaining data privacy in association rule mining. In: Proceedings of the 28th International Conference on Very Large Data Bases, pp. 682-693, VLDB Endowment (2002)
19. Shannon, C.E.: A Mathematical Theory of Communication. *Bell System Technical Journal*, 27(3), 379-423 (1948)
20. Shenvi, N., Kempe, J., Whaley, K.B.: Quantum random-walk search algorithm. *Physical Review A*, 67(5), 052307 (2003)
21. Unruh, D.: Revocable quantum timed-release encryption. *Journal of the ACM*, 62(6), article no. 49 (2015)

A Procedure TestBob2

In this Appendix, we present the detailed description of procedure TestBob2 that was only very briefly discussed in Section 4.

Procedure TestBob2

output: “Dishonesty detected”, if Bob’s dishonesty is detected.

1 begin

2 Alice generates $\mu < \nu \in \{0, 1\}^k$, $c \in \{0, 1\}^t$, $m \in \{0, 1, \dots, n-1\}$,
 $x \in \{0, 1\}^n$, and $b \in \{0, 1\}$ uniformly at random;

3 Alice prepares $|\Phi\rangle = |c\rangle_{q_c} \otimes U_t(m, x, b)|0\rangle_{q_a, q_d}^{\otimes(n+k)}$ on new control qubits q_c ,
address qubits q_a , and data qubits q_d ;

4 Bob adds a qubit q_g initialized to be $|0\rangle$ to the end of these qubits, and Bob
applies U'_f on q_a , q_d , and q_g ;

5 Alice applies $U_t(m, x, b)^\dagger$ on q_a and q_d , obtaining the state

$$|\Phi_1\rangle = |c\rangle_{q_c} \otimes U_t(m, x, b)^\dagger \otimes I_g(U'_f(U_t(m, x, b)|0\rangle^{\otimes(n+k)} \otimes |0\rangle));$$

6 Alice and Bob repeat Step 3 to Step 5 to get $|\Phi_2\rangle$;

7 Alice employs a quantum controlled swap test to test whether $|\Phi_1\rangle$ and $|\Phi_2\rangle$
are the same. If not, Alice terminates the entire protocol;

8 Alice measures all address and data qubits except the first address qubit of
 $|\Phi_1\rangle$, and $|\Phi_2\rangle$, according to the basis $\{|0\rangle, |1\rangle\}$. Let the outcomes be v and
 w , respectively, both in $\{0, 1\}^{n+k-1}$;

9 If $v_j = 1$, or $w_j = 1$ for any j , **return** “Dishonesty detected”;

10 end

A.1 Controlled Swap Test

Controlled swap tests are employed at Step 7 in procedure TestBob2 to check whether Bob performs measurements on q_g or q_d . In this subsection, we briefly describe these tests. For details, we refer to [11].

A quantum swap gate consists of three CNOT gates, and swaps the states of two qubits:

$$SWAP : \sum_{i,j \in \{0,1\}} \alpha_{i,j} |i\rangle |j\rangle \rightarrow \sum_{i,j} \alpha_{i,j} |i\rangle |j \oplus i\rangle \rightarrow \sum_{i,j} \alpha_{i,j} |j\rangle |j \oplus i\rangle \rightarrow \sum_{i,j} \alpha_{i,j} |j\rangle |i\rangle.$$

Then a controlled swap test on two n -qubit states $|\psi\rangle$ and $|\phi\rangle$ works as follows:

1. Add an ancilla qubit in state $|+\rangle$ before $|\psi\rangle$ and $|\phi\rangle$, and get

$$|\Psi_1\rangle = |+\rangle |\psi\rangle |\phi\rangle.$$

2. Apply a controlled swap operator U_{CS} on $|\Psi_1\rangle$, where the first qubit is the control qubit, and the other qubits are the target:

$$|\Psi_2\rangle = U_{CS}|\Psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi\rangle|\phi\rangle + |1\rangle|\phi\rangle|\psi\rangle),$$

where $|\psi\rangle$ and $|\phi\rangle$ are swapped if the control qubit is in state $|1\rangle$.

3. Apply a Hadamard gate on the control qubit, and get

$$\begin{aligned} |\Psi_3\rangle &= \frac{1}{\sqrt{2}}(|+\rangle|\psi\rangle|\phi\rangle + |-\rangle|\phi\rangle|\psi\rangle) \\ &= \frac{1}{2}(|0\rangle(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) + |1\rangle(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle)). \end{aligned}$$

If $|\psi\rangle = |\phi\rangle$, we have $|\Psi_3\rangle = |0\rangle|\psi\rangle|\phi\rangle$.

4. Measure the control qubit in basis $\{|0\rangle, |1\rangle\}$. If outcome is 1, $|\psi\rangle \neq |\phi\rangle$ is detected.

At Step 4, the probability to get outcome 1 is

$$\Pr(1) = \frac{1}{4} \| |\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle \|^2 = \frac{1}{4} (2 - 2\langle\phi|\psi\rangle\langle\psi|\phi\rangle) = \frac{1 - |\langle\phi|\psi\rangle|^2}{2}.$$

Omitting the control qubit, the post-measurement states are

$$\begin{cases} |\varphi_0\rangle = \frac{1}{2}(|\psi\rangle|\phi\rangle + |\phi\rangle|\psi\rangle) & \text{if outcome is 0} \\ |\varphi_1\rangle = \frac{1}{2}(|\psi\rangle|\phi\rangle - |\phi\rangle|\psi\rangle) & \text{if outcome is 1.} \end{cases}$$

In conclusion, if $|\psi\rangle = |\phi\rangle$, the outcome is always 0, and the state $|\psi\rangle|\phi\rangle$ remains unchanged. Otherwise, there is a probability $\frac{1 - |\langle\phi|\psi\rangle|^2}{2}$ to have outcome 1.

B Proofs of Lemmas and Theorems

In this Appendix, we provide the proofs of the lemmas and theorems presented in the main text.

B.1 Proof of Lemma 1

We first specify the situation:

1. Alice sends $|c\rangle|\psi_{m,x,b}(\mu, \nu)\rangle$ to Bob.
2. After Bob's actions, he sends a state to Alice; see Table 9.
3. Alice checks the test state.

Now we prove that it can be detected by the final measurement (Step 8).

Case 1 $d = \mu$: Let $|\psi'\rangle$ denote the state that Bob sends back to Alice. Then $|\psi'\rangle = |\varphi\rangle|a\rangle|\mu\rangle$. Alice will transfer it to

$$|\phi'\rangle = V(\mu, \nu)X_0^b Z(x)U_{SWAP(0,m)}|\psi'\rangle,$$

Test	State if honest	State in this attack
TestBob1	$ c\rangle \psi_{m,x',b}(\mu,\nu)\rangle$	$ \varphi\rangle i\rangle d\rangle$

Table 9. The state Bob sends to Alice. In this table x' depends on whether $f(\mu) = f(\nu)$.

and then

$$|\Phi_1\rangle = I_c \otimes W \otimes I_d |\phi'\rangle.$$

Now we see what $|\Phi_1\rangle$ is. The initial state is $|\psi'\rangle = |\varphi\rangle|a\rangle|\mu\rangle$. Then

1. $U_{SWAP(0,m)}$ maps a to $a' \in \{0, 1\}^n$;
2. $Z(x)$ only possibly adds a global phase -1 ;
3. X_0^b maps a' to a'' ;
4. $V(\mu, \nu)$ only works on the data qubits, and then $|\phi'\rangle$ can be $|a''\rangle|\vec{0}\rangle$ or $|a''\rangle|\mu \oplus \nu\rangle$, after omitting the global phase.

Consequently, $|\phi_1\rangle$ may be $|w\rangle|*\rangle$, where $w \in \{+, -\}^n$. On each address qubit, the measurement outcome will be 0 with probability $\frac{1}{2}$. Therefore, this attack passes the final measurement (Step 8) with probability at most $\frac{1}{2^{n-1}} = \frac{2}{N}$.

Since the test consists of two copies, the attack can be further detected. Suppose that Bob sends $|\varphi\rangle|a\rangle|\mu\rangle$ in the first round. By the above discussion, this means that v_0 has a fifty-fifty chance to be 0 or 1. For the other round, we assume that w_0 comes out as 0 with probability p , and 1 with probability $1 - p$. Then Bob has probability $\frac{1}{2}(1 - p) + \frac{1}{2}p = \frac{1}{2}$ to fail. Thus, the total probability to pass the test is at most $\frac{1}{N}$.

Case 2. $d = \nu$: Similar.

Case 3. $d \neq \mu$ and $d \neq \nu$: The probability to pass the final measurement may be lower. This is because there must be at least one $|1\rangle$ occurring in the data qubits of $|\Phi_1\rangle$ at last. So, it will be detected with probability 1.

B.2 Proof of Lemma 2

In the scenario of this lemma, Bob thinks that he receives $|\varphi\rangle|a\rangle|d_{a \oplus y}\rangle$ from Alice. But indeed, he receives $|c\rangle|\psi_{m,x,b}(\mu,\nu)\rangle$. Then the measurements are taken on $|c\rangle|\psi_{m,x,b}(\mu,\nu)\rangle$.

If the measurements are performed jointly on q_a and q_d , then the post-measurement state is $|c\rangle|j\rangle|\mu\rangle$ or $|c\rangle|j\rangle|\nu\rangle$, and it can be reduced to Lemma 1 as Bob will send this state back to Alice. So, it remains to analyse the case when measurements are on only q_d .

Since measurements are only performed on q_d , all the measurement operators are local operators on q_d and have the form $M = I^{\otimes n} \otimes |w\rangle\langle w|$, where $w \in \{0, 1\}^k$. Thus, each M commutes with X_0 , $Z(x)$ and $U_{SWAP(0,m)}$, as the latter three operators are local operators on q_a . Therefore, the post-measurement state of $|c\rangle|\psi_{m,x,b}\rangle$ can be written as

$$|\psi'\rangle = \begin{cases} |c\rangle U_{SWAP(0,m)} Z(x) X_0^b |0\rangle |+\rangle^{\otimes n-1} |\mu\rangle, & \text{the outcome is } \mu \\ |c\rangle U_{SWAP(0,m)} Z(x) X_0^b |1\rangle |+\rangle^{\otimes n-1} |\nu\rangle, & \text{the outcomes is } \nu \end{cases}.$$

Bob sends it back to Alice, and then Alice has

$$|\phi'\rangle = \begin{cases} |c\rangle V(\mu, \nu)|0\rangle|+\rangle^{\otimes n-1}|\mu\rangle = |0\rangle|+\rangle^{\otimes n-1}|\vec{0}\rangle, & \text{the case } \mu \\ |c\rangle V(\mu, \nu)|1\rangle|+\rangle^{\otimes n-1}|\nu\rangle = |1\rangle|+\rangle^{\otimes n-1}|\vec{0}\rangle, & \text{the case } \nu \end{cases}$$

Furthermore, it holds that

$$|\Phi_1\rangle = \begin{cases} |c\rangle|+\rangle|0\rangle^{\otimes n+k-1}, & \text{the case } \mu \\ |c\rangle|-\rangle|0\rangle^{\otimes n+k-1}, & \text{the case } \nu \end{cases}$$

In both cases, the first element v_0 of the final outcome result v has a fifty-fifty probability to become 0 or 1. This means that this attack can be detected by TestBob1 with probability $\frac{1}{2}$ by the condition $v_0 \neq w_0$.

B.3 Proof of Lemma 4

In this proof, we omit $|c\rangle$, since it indeed does not change through the test. Moreover, we use $|\Psi'\rangle$, $|\Phi'\rangle$ and $|\Phi'_1\rangle$ on q_a, q_d, q_g to replace $|\psi'\rangle$, $|\phi'\rangle$ and $|\Phi_1\rangle$, respectively.

(1) The general case. By the assumption of this lemma, there exist some $i, i' \in \{0, 1\}^n$, and $d, d' \in \{0, 1\}^k$ such that $|\lambda_{i,d}\rangle \neq |\lambda_{i',d'}\rangle$. We can further assume $i \neq i'$ and $d \neq d'$. (Otherwise, if $i = i'$ or $d = d'$, we choose $i'' \notin \{i, i'\}$ and $d'' \notin \{d, d'\}$, and then $|\lambda_{i'',d''}\rangle$ must be different to one of the original two.)

Suppose $d < d'$. By the construction of test states, we find $\mu = d$, and $\nu = d'$ with probability $\frac{2}{2^k(2^k-1)}$. As $i \neq i'$, there exists m such that $i_m \neq i'_m$. Then for $b = i_m$ and any x , we can find both item $|i\rangle|d\rangle$ and $|i'\rangle|d'\rangle$ in $|\psi_{m,x,i_m}(\mu, \nu)\rangle$. The total probability to generate this state is

$$\frac{2}{2^k(2^k-1)} \frac{1}{n} \frac{1}{2} = \frac{1}{n2^k(2^k-1)}.$$

Now $|\psi_{m,x,i_m}(\mu, \nu)\rangle$ is entangled to be $|\Psi_{m,x,i_m}(\mu, \nu)\rangle$. Alice transforms it to

$$|\Phi'_1(\mu, \nu)\rangle = (V(\mu, \nu)X_0^{i_m}Z(x)U_{SWAP(0,m)}) \otimes I_g |\Psi'_{m,x,i_m}(\mu, \nu)\rangle.$$

Since these operators are unitary and only on the address and data qubits, the address and data qubits are still entangled to q_g . Then no matter whether measurement operator $M_v = |v\rangle\langle v|$ or $M_{v'} = |v'\rangle\langle v'|$ is used with $|v\rangle = |0\rangle|0\rangle^{\otimes n+k-1}$ and $|v'\rangle = |1\rangle|0\rangle^{\otimes n+k-1}$, it holds

$$\begin{cases} p_0 = \|M_v \otimes I_g |\Phi'_1(\mu, \nu)\rangle\|^2 < 1, \\ p_1 = \|M_{v'} \otimes I_g |\Phi'_1(\mu, \nu)\rangle\|^2 < 1. \end{cases}$$

Thus, if $p_0 + p_1 < 1$, it will be detected by $v_j = 1$ with $j > 0$. Otherwise it will be still detected by the condition $v_0 \neq w_0$ with a positive probability as $p_0 < 1$ and $p_1 < 1$.

(2) The case $E|i\rangle|d\rangle|0\rangle = |i\rangle|d\rangle|i\rangle|d\rangle$. We have:

$$\begin{aligned} |\Phi'(\mu, \nu)\rangle &= (V(\mu, \nu)X_0^{i_m}Z(x)U_{SWAP(0,m)}) \otimes I_q \frac{1}{\sqrt{N}} \sum_i \beta_i |i\rangle|\tau_i\rangle|i\rangle|\tau_i\rangle \\ &= \frac{1}{\sqrt{N}} \sum_i \beta_i (V(\mu, \nu)X_0^{i_m}Z(x)U_{SWAP(0,m)}|i\rangle|\tau_i\rangle)|i\rangle|\tau_i\rangle \\ &= \frac{1}{\sqrt{N}} \sum_i \beta_i |i'\rangle|\tau'_i\rangle|i\rangle|\tau_i\rangle, \end{aligned}$$

where $\beta_i \in \{1, -1\}$, $\tau_i \in \{\mu, \nu\}$, $V(\mu, \nu)X_0^{i_m}Z(x)U_{SWAP(0,m)}$ is a bijection mapping i to i' , and $\tau'_i \in \{0, \mu \oplus \nu\}$. Then

$$|\Phi'_1(\mu, \nu)\rangle = \frac{1}{\sqrt{N}} \sum_i \beta_i (W|i'\rangle)|\tau'_i\rangle|i\rangle|\tau_i\rangle.$$

Since each item has a $|i\rangle$ which belongs to q_g and is orthogonal to each other, probabilities p_0 and p_1 can be calculated:

$$\begin{aligned} p_0 &= \|M_v \otimes I_g |\Phi'_1(\mu, \nu)\rangle\|^2 \\ &= \left\| \frac{1}{\sqrt{N}} \sum_i \beta_i (\langle 00 \dots 000 | W | i' \rangle) \langle 00 \dots 00 | \tau'_i \rangle |i\rangle |\tau_i\rangle \right\|^2 \\ &= \frac{1}{N} \sum_i \| (\langle 00 \dots 000 | W | i' \rangle) \langle 00 \dots 00 | \tau'_i \rangle \|^2 \\ &= \frac{1}{N^2} \sum_i \| \langle 00 \dots 00 | \tau'_i \rangle \|^2 \leq \frac{1}{N}, \end{aligned}$$

Similarly, we obtain:

$$\begin{aligned} p_1 &= \frac{1}{N} \sum_i \| (\langle 10 \dots 000 | W | i' \rangle) \langle 00 \dots 00 | \tau'_i \rangle \|^2 \\ &= \frac{1}{N^2} \sum_i \| \langle 00 \dots 00 | \tau'_i \rangle \|^2 \leq \frac{1}{N}. \end{aligned}$$

Therefore the probability to fail is

$$\Pr(\text{detected}) = 1 - p_0 - p_1 + (p_0 + p_1) \Pr(v_0 \neq w_0) \geq 1 - \frac{1}{N}.$$

(3) For the case $E|i\rangle|d\rangle|0\rangle = |i\rangle|d\rangle|d\rangle$, as in the proof of Lemma 2, we have

$$|\Phi'_1(\mu, \nu)\rangle = \frac{1}{\sqrt{2}} (|0\rangle|0\rangle^{\otimes n+k-1} |\mu\rangle + |1\rangle|0\rangle^{\otimes n+k-1} |\nu\rangle).$$

Then we have $p_0 = p_1 = \frac{1}{2}$. It will be detected by $v_0 \neq w_0$ with probability $\frac{1}{2}$.

B.4 Proof of Theorem 2

We check what will happen, if the state is entangled to q_g . Assume the test states are $|\psi_{m,x,b}(\mu, \nu)\rangle$. For simplicity, we denote it by $|\psi\rangle$. Suppose Bob employ \mathcal{E}_1 and \mathcal{E}_2 on the two test states with new ancilla qubits (initialed to be $|\theta_1\rangle$ and $|\theta_2\rangle$ respectively). Then we have

$$\begin{cases} \mathcal{E}_1(\psi \otimes \theta_1) = \rho = \sum_u \lambda_u |\varphi_u\rangle \langle \varphi_u|, \\ \mathcal{E}_2(\psi \otimes \theta_2) = \sigma = \sum_v \chi_v |\omega_v\rangle \langle \omega_v|, \end{cases}$$

where $\lambda_u, \chi_v \in [0, 1]$, and $\{|\varphi_u\rangle\}, \{|\omega_v\rangle\}$ are orthonormal bases. Since density operators can be seen as probabilistic distributions over pure states, the following two facts are equivalent:

- ρ and σ pass the test with probability 1.
- For any u, v , $|\varphi_u\rangle$ and $|\omega_v\rangle$ pass the test with probability 1.

Suppose $|\varphi\rangle$ stands for any $|\varphi_u\rangle$ and $|\omega\rangle$ stands for any $|\omega_v\rangle$, and

$$\begin{cases} |\varphi\rangle = \sum_j \alpha_j |\xi_j\rangle |j\rangle, \\ |\omega\rangle = \sum_j \beta_j |\gamma_j\rangle |j\rangle, \end{cases}$$

where $\{|j\rangle\}$ is an orthonormal basis of the Hilbert space \mathcal{H}_g on q_g , and $|\xi_j\rangle, |\gamma_j\rangle$ are normalized states ($\sum_j |\alpha_j|^2 = \sum_j |\beta_j|^2 = 1$). Suppose the same recovery operator for these two states in the test is R . Then after recovery, the states become

$$\begin{cases} |\bar{\varphi}\rangle = \sum_j \alpha_j (R|\xi_j\rangle) |j\rangle, \\ |\bar{\omega}\rangle = \sum_j \beta_j (R|\gamma_j\rangle) |j\rangle. \end{cases}$$

Note that Bob holds the second part of $|\varphi'\rangle$ and $|\omega'\rangle$, Alice performs measurements only on the first part. Then in order to pass Step 8, the measurement outcomes are always fixed, and the above states must be

$$\begin{cases} |\bar{\varphi}\rangle = |\tau\rangle |0\rangle^{\otimes n+k-1} |\varphi'\rangle, \\ |\bar{\omega}\rangle = |\tau\rangle |0\rangle^{\otimes n+k-1} |\omega'\rangle, \end{cases}$$

where $\tau \in \{0, 1\}$, and $|\varphi'\rangle, |\omega'\rangle$ are states of q_g . Since R is a unitary operator, we have

$$\begin{cases} |\varphi\rangle = R^\dagger \otimes I_g |\bar{\varphi}\rangle = |\xi\rangle \otimes |\varphi'\rangle, \\ |\omega\rangle = R^\dagger \otimes I_g |\bar{\omega}\rangle = |\xi\rangle \otimes |\omega'\rangle. \end{cases}$$

Moreover, since $|\varphi\rangle$ stands for any $|\varphi_u\rangle$ and $|\omega\rangle$ stands for any $|\omega_v\rangle$, $|\xi\rangle$ is independent of u, v . Then we have

$$\begin{cases} \mathcal{E}_1(\psi \otimes \theta_1) = \rho = |\xi\rangle \langle \xi| \otimes \rho', \\ \mathcal{E}_2(\psi \otimes \theta_2) = \sigma = |\xi\rangle \langle \xi| \otimes \sigma'. \end{cases}$$

Since all possible test states $|\psi\rangle$ can be used to construct several orthonormal bases (see Lemma 6), \mathcal{E}_1 can be written as

$$\mathcal{E}_1 = U \circ U^\dagger \otimes \mathcal{E}_g,$$

where U is a unitary operator on q_a and q_d , and $|\xi\rangle = U|\psi\rangle$. The conclusion about \mathcal{E}_2 can be proved similarly.

Now we prove that ρ' (σ') is independent on ξ . By the above explicit form of \mathcal{E}_1 , it seems obvious intuitively. But here we give a strict proof. Suppose $|\psi_1\rangle$ and $|\psi_2\rangle$ are two test states for short. Suppose $\mathcal{E}(\psi_i \otimes \theta) = U|\psi_i\rangle\langle\psi_i|U^\dagger \otimes \rho'_i$. Since the fidelity $F(\psi_i \otimes \theta, \psi_i \otimes \theta)$ will increase after super-operator \mathcal{E} , we have

$$\begin{aligned} F(\psi_1 \otimes \theta, \psi_2 \otimes \theta) &\leq F(\mathcal{E}(\psi_1 \otimes \theta), \mathcal{E}(\psi_2 \otimes \theta)) \\ &= F(U|\psi_1\rangle\langle\psi_1|U^\dagger \otimes \rho'_1, U|\psi_2\rangle\langle\psi_2|U^\dagger \otimes \rho'_2) \\ &= F(U|\psi_1\rangle\langle\psi_1|U^\dagger, U|\psi_2\rangle\langle\psi_2|U^\dagger)F(\rho'_1, \rho'_2) \\ &\leq F(U|\psi_1\rangle\langle\psi_1|U^\dagger, U|\psi_2\rangle\langle\psi_2|U^\dagger) \\ &= F(|\psi_1\rangle\langle\psi_1|, |\psi_2\rangle\langle\psi_2|). \end{aligned}$$

On the other hand,

$$F(\psi_1 \otimes \theta, \psi_2 \otimes \theta) = F(\psi_1, \psi_2)F(\theta, \theta) = F(\psi_1, \psi_2).$$

Therefore, $F(\rho'_1, \rho'_2) = 1$, i.e., $\rho'_1 = \rho'_2$. This means ρ' is independent on $|\psi\rangle$.

B.5 Proof of Corollary 2

Suppose Bob employs certain operators and measurements in one test round. Then all of Bob's actions are equal to the measurement with measurement operators E_j . Note these measurement operators form the super-operator $\mathcal{E} = \sum E_j \circ E_j^\dagger$ (performing a measurement without reading the outcomes is equivalent to performing a super-operator). By Theorem 2, each measurement operator E_j has the form $E_j = U \otimes M_j$. So, on q_a and q_d , no measurements are performed, which means that Bob cannot read any information from q_a and q_d .

B.6 Proof of Lemma 5

In order to read information about specific d from D , Bob needs to perform measurements on a state like $\sum_{c,j} \alpha_{c,j} |c\rangle|j\rangle|d_{j\oplus y}\rangle$, instead of a state like $\sum_{c,j} \alpha_{c,j} |c\rangle|j\rangle|\vec{0}\rangle$. But if Bob is honest or he does not construct a new state to send to Alice at some step, the state he gets at Step 7 is always the latter. So Bob has to first send a state to Alice at some step, and then perform measurements.

There are three different ways to attacks at Step 7 of Algorithm 1 here. The first two ways correspond to direct attacks (reading information) at Step 7. Bob can first send a cheating state (for instance, $|c\rangle|j\rangle|\vec{0}\rangle$) back to Alice at Step 4 or Step 7, and then perform measurements on the received state (for instance,

$|c\rangle|j\rangle|d_{j\oplus y}\rangle$) at Step 7. The last way is to do some preparation at Step 7 for a future attack. In this way, Bob sends a cheating state back to Alice at Step 7, and then performs measurements on the received state at Step 4 (Note that sending a cheating state and performing measurements both at Step 4 is not related to the attacks at Step 7.) Obviously, each of the above attacks can be divided into two parts: (1) sending state; and (2) performing measurements. All of the possible cases are listed in Table 10. We analyse these cases one by one.

	Sending a cheating state	Performing measurements
1	Step 4	Step 7
2	Step 7	Step 7
3	Step 7	Step 4

Table 10. Three different ways related to one-round attacks at Step 7.

Case 1. Bob's measurements at Step 7 will not be detected. But the part of sending a cheating state at Step 4 will be detected. For instance, if Bob sends state $|c\rangle|j\rangle|\vec{0}\rangle$ at Step 4, it will be detected by procedure TestBob1 with probability at least 0.5 (See Lemma 1). If Bob sends any other state, it can be also detected by the results in Section 7.6.

Case 2. This case cannot be detected, if there is no test corresponding to Step 7. But Bob cannot read any information about some specific $d \in D$ from this kind of attacks. Indeed, from procedure GroverIteration, one sees that there are an even number of calls of database $U_D(y)$ on the cheating state from sending it to receiving it. So, if the cheating state is $\sum \beta_{c,j}|c\rangle|j\rangle|\vec{0}\rangle$, it becomes $\sum \beta'_{c,j}|c\rangle|j\rangle|\vec{0}\rangle$ when Bob receives it again. There is still no information about specific $d \in D$ on the data qubits. Therefore, this attack does not work.

Case 3. Similar to Case 1, this attack will be detected at Step 4 after measurements.

B.7 Proof of Lemma 6

We first prove the following technical lemma.

Lemma 9. *Suppose $B_m(\mu, \nu) = \{|\psi_{m,x,b}(\mu, \nu)\rangle : \forall x, b\}$. Then B_m is an orthogonal basis of Hilbert space spanned by $\{|i\rangle|\mu\rangle, |i\rangle|\nu\rangle : i \in \{0, 1\}^n\}$.*

Proof. It is sufficient to prove that $B_{n-1}(\mu, \nu)$ is an orthogonal basis. Observe that any $|\psi_{n-1,x,b}(\mu, \nu)\rangle$ can be rewritten as

$$|\psi_{n-1,x,b}(\mu, \nu)\rangle = |\phi_{x_1, \dots, x_{n-1}}\rangle \otimes |\beta_{x_0, b}\rangle,$$

where $|\phi_{x_1, \dots, x_{n-1}}\rangle = Z^{x_{n-1}} \otimes Z^{x_1} \otimes Z^{x_2} \otimes \dots \otimes Z^{x_{n-2}} |+\dots+\rangle$, and

$$|\beta_{x_0, b}\rangle = Z^{x_0} X^b \frac{1}{\sqrt{2}}(|0\rangle|\mu\rangle + |1\rangle|\nu\rangle).$$

Since $Z|+\rangle = |-\rangle$, all $|\phi_{x_1, \dots, x_{n-1}}\rangle$ form an orthogonal basis of the first $n-1$ qubits. Meanwhile, four different states of $|\beta_{x_0, b}\rangle$ form an orthogonal basis of the other part. Thus, $B_{n-1}(\mu, \nu)$ is an orthogonal basis of Hilbert space spanned by $\{|i\rangle|\mu\rangle, |i\rangle|\nu\rangle : i \in \{0, 1\}^n\}$.

Now we can prove Lemma 6. Put

$$\Psi(m, k) = \{|\psi_{m, x, b}(\mu, \nu)\rangle : \forall \mu < \nu \in \{0, 1\}^k, \forall x \in \{0, 1\}^n, \forall b \in \{0, 1\}\}.$$

Obviously, for $m \neq m'$, the two sets $\Psi(m, k)$ and $\Psi(m', k)$ are disjoint to each other, i.e., $\Psi(m, k) \cap \Psi(m', k) = \emptyset$. So it is sufficient to prove that $\Psi(0, k)$ can be decomposed into the union of disjoint orthogonal bases:

$$\Psi(0, k) = C_1(0, k) \cup \dots \cup C_{2^{k-1}}(0, k). \quad (20)$$

Before continuing the proof, we define two concepts:

- a set $P = \{\lambda = \{\mu, \nu\} : \mu < \nu \in \{0, 1\}^k\}$ is called a *partition* of the set $\Lambda(k) = \{0, 1\}^k$ if for any $\lambda, \lambda' \in P$, $\lambda \cap \lambda' = \emptyset$ and $\bigcup_{\lambda \in P} \lambda = \Lambda(k)$.
- the set generated by a couple $\lambda = \{\mu, \nu\} \in P$ is

$$B(\lambda) = B_0(\mu, \nu) = \{|\psi_{0, x, b}(\mu, \nu)\rangle : \forall x \in \{0, 1\}^n, \forall b \in \{0, 1\}\}.$$

Since $\Lambda(k)$ has 2^k elements, there are always such partitions.

We first prove that each partition corresponds to an orthogonal basis. By Lemma 9, $C(\mu, \nu)$ is a orthogonal basis of the subspace spanned by $\{|\alpha\rangle|\mu\rangle, |\alpha\rangle|\nu\rangle : \forall |\alpha\rangle \in \mathcal{H}_a\}$. This implies that the set

$$B(P) = \bigcup_{\lambda \in P} B(\lambda)$$

is an orthogonal basis for any partition P .

Observe that $\Psi(0, k) = \bigcup_{\lambda \in Q(k)} B(\lambda)$, where $Q(k) = \{\{\mu, \nu\} : \forall \mu < \nu \in \{0, 1\}^k\}$. Therefore, Eq. (20) can be derived by

$$Q(k) = P_1 \cup \dots \cup P_{2^{k-1}}, \quad (21)$$

where $P_i \cap P_j = \emptyset$ for any $i \neq j$. Thus, we prove Eq. (21) by induction on k .

(1) For $k = 1$, it is obvious, as $Q(1) = \{\{0, 1\}\}$, i.e., it only contains one couple/set $\{0, 1\}$.

(2) Suppose Eq. (21) holds for $k = l$, i.e., $Q(l) = P_1 \cup \dots \cup P_{2^{l-1}}$. Then for $k = l + 1$, we construct P'_i in the following three cases:

1. P'_1, \dots, P'_u , where $u = 2^l$. In this case, P'_i can be constructed as follows:

$$P'_i = \{\{\mu \cdot 0, \nu \cdot 0\}, \{\mu \cdot 1, \nu \cdot 1\} : \forall \{\mu, \nu\} \in P_i\}, \quad (22)$$

where “.” is the concatenation operator. For instance, if $\mu = 01001 \in \{0, 1\}^5$, then $\mu \cdot 0 = 010010 \in \{0, 1\}^6$.

2. P'_{u+1}, \dots, P'_{2u} can be constructed as follows:

$$P'_i = \{\{\mu \cdot 0, \nu \cdot 1\}, \{\mu \cdot 1, \nu \cdot 0\} : \forall \{\mu, \nu\} \in P_i\}. \quad (23)$$

3. P'_v with $v = 2^{l+1}$ is

$$P'_v = \{\{\mu \cdot 0, \mu \cdot 1\} : \forall \mu \in \{0, 1\}^l\}. \quad (24)$$

After constructing such P'_i 's, it remains to prove that they satisfies Eq. (21). First, we show that each P'_i is a partition.

- Case 1. $i \leq u$: Suppose $\lambda_1 = \{\mu'_1 = \mu_1 \cdot a_1, \nu'_1 = \nu_1 \cdot a_1\} \neq \lambda_2 = \{\mu'_2 = \mu_2 \cdot a_2, \nu'_2 = \nu_2 \cdot a_2\} \in P'_i$, where $\mu_1, \nu_1, \mu_2, \nu_2 \in \{0, 1\}^l$, $a_1, a_2 \in \{0, 1\}$, and $\lambda_1 \cap \lambda_2 \neq \emptyset$. Since the join of λ_1 and λ_2 is nonempty, we have $a_1 = a_2$. As a consequence, it holds that $\{\mu_1, \nu_1\} \cap \{\mu_2, \nu_2\} \neq \emptyset$. But this is not true because P_i is a partition. A contradiction! So for any $\lambda_1 \neq \lambda_2 \in P'_i$, $\lambda_1 \cap \lambda_2 = \emptyset$. Furthermore, as $|P'_i| = 2|P_i|$ and P_i is a partition of $\Lambda(l)$, we see that P'_i is a partition of $\Lambda(l+1)$.
- Case 2. $u < i \leq 2u$: Similar to Case 1.
- Case 3. $i = v$: Obvious, as P'_v can be written as $\{\{0, 1\}, \{2, 3\}, \dots, \{2^{l+1} - 2, 2^{l+1} - 1\}\}$.

Secondly, we prove that each couple $\{\mu' = \mu \cdot a, \nu' = \nu \cdot b\}$ belongs to one and only one P'_i , where $\mu' < \nu'$, $\mu, \nu \in \{0, 1\}^l$ and $a, b \in \{0, 1\}$. In fact, the existence of index $i = \text{Index}(\mu', \nu')$ for such set P'_i can be verified as follows:

1. If $a = b$, then $\mu < \nu$, and $\text{Index}(\mu', \nu') \leq u$. By Eq. (22), we have $\text{Index}(\mu', \nu') = \text{Index}(\mu, \nu)$.
2. If $a \neq b$ and $\mu \neq \nu$, then $\mu < \nu$, and $u < \text{Index}(\mu', \nu') \leq 2u$. By Eq. (23), we have $\text{Index}(\mu', \nu') = \text{Index}(\mu, \nu) + u$.
3. If $a \neq b$ and $\mu = \nu$, then $a = 0, b = 1$ and $\text{Index}(\mu', \nu') = 2u + 1 = v$.

The above two facts indicates that Eq. (21) holds for $k = l + 1$. Consequently, by induction we complete the proof.

B.8 Proof of Lemma 7

By Bayes' theorem, we obtain:

$$\begin{aligned} \Pr(m, x, b, \mu, \nu | M_v) &= \frac{\Pr(M_v | m, x, b, \mu, \nu) \Pr(m, x, b, \mu, \nu)}{\Pr(M_v)} \\ &= \frac{q \Pr(M_v | m, x, b, \mu, \nu)}{\Pr(M_v)}, \end{aligned}$$

where we denote:

$$q = \Pr(m, x, b, \mu, \nu) = \frac{1}{n2^{n+1}2^k(2^k - 1)}.$$

Now we only need to compute $\Pr(M_v)$ and $\Pr(M_v|m, x, b)$. By Lemma 6, we have

$$\begin{aligned}\Pr(M_v) &= \sum_{l, y, a, \mu, \nu} \Pr(M_v|l, y, a, \mu, \nu) \Pr(l, y, a, \mu, \nu) = \sum q \Pr(M_v|l, y, a, \mu, \nu) \\ &= \sum q \|\mathcal{M}_v |\psi_{l, y, a}(\mu, \nu)\rangle\|^2 = \sum q \text{tr}(M_v^\dagger M_v |\psi_{l, y, a}(\mu, \nu)\rangle \langle \psi_{l, y, a}(\mu, \nu)|) \\ &= \sum_B q \text{tr}(M_v^\dagger M_v) = n(2^k - 1) q \text{tr}(M_v^\dagger M_v),\end{aligned}$$

where B ranges over all possible bases in Lemma 6. Therefore,

$$\begin{aligned}\sum_{|\psi_{l, y, a}(\mu', \nu')\rangle \in B_0} \Pr(l, y, a, \mu, \nu | M_v) &= \sum \frac{q \Pr(M_v|l, y, a, \mu, \nu)}{\Pr(M_v)} \\ &= \frac{q \text{tr}(M_v^\dagger M_v)}{\Pr(M_v)} = \frac{1}{n(2^k - 1)},\end{aligned}$$

where B_0 is the basis in Lemma 6 that contains $|\psi_{m, x, b}(\mu, \nu)\rangle$. Especially,

$$\Pr(m, x, b, \mu, \nu | M_v) \leq \sum_{|\psi_{l, y, a}(\mu', \nu')\rangle \in B_0} \Pr(l, y, a, \mu, \nu | M_v) = \frac{1}{n(2^k - 1)}.$$

B.9 Proof of Theorem 3

We first decompose $|\psi_{m, x, b}(\mu, \nu)\rangle$ into some other test states.

Lemma 10. *For any $m \neq l \in \{0, \dots, n-1\}$, $x \in \{0, 1\}^n$, $b \in \{0, 1\}$, and $\mu < \nu \in \{0, 1\}^k$, we have:*

$$\begin{aligned}|\psi_{m, x, b}(\mu, \nu)\rangle &= (-1)^{bx_m} \frac{1}{2} (|\psi_{l, x', 0}(\mu, \nu)\rangle + (-1)^{x_m} |\psi_{l, x', 1}(\mu, \nu)\rangle \\ &\quad + (-1)^b |\psi_{l, x'', 0}(\mu, \nu)\rangle - (-1)^{b+x_m} |\psi_{l, x'', 1}(\mu, \nu)\rangle),\end{aligned}\quad (25)$$

where $x' = x_0 x_1 x_2 \cdots x_{m-1} x'_m x_{m+1} x_{m+2} \cdots x_{l-1} x'_l x_{l+1} x_{l+2} \cdots x_{n-1}$ with $x'_m = x_m \oplus x_l$, $x'_l = 0$, and $x'' = x_0 x_1 x_2 \cdots x_{m-1} x''_m x_{m+1} x_{m+2} \cdots x_{l-1} x''_l x_{l+1} x_{l+2} \cdots x_{n-1}$ with $x''_m = x_m \oplus x_l \oplus 1$, $x''_l = 1$.

Proof. First, we observe:

$$\begin{cases} |0\rangle|+\rangle = \frac{1}{2}(|+\rangle|0\rangle + |+\rangle|1\rangle + |-\rangle|0\rangle + |-\rangle|1\rangle) \\ |1\rangle|+\rangle = \frac{1}{2}(|+\rangle|0\rangle + |+\rangle|1\rangle - |-\rangle|0\rangle - |-\rangle|1\rangle) \end{cases} \quad (26)$$

For any x , we can rewrite $|\psi_{0, x, 0}(\mu, \nu)\rangle$ as

$$|\psi_{0, x, 0}(\mu, \nu)\rangle = \frac{1}{\sqrt{2}} Z(x) (|0\rangle|+\rangle^{\otimes n-1} |\vec{0}\rangle + |1\rangle|+\rangle^{\otimes n-1} |\vec{1}\rangle) \quad (27)$$

$$= \frac{1}{\sqrt{2}} Z_1^{x_1} (|0\rangle|+\rangle |\varphi\rangle |\vec{0}\rangle + (-1)^{x_0} |1\rangle|+\rangle |\varphi\rangle |\vec{1}\rangle), \quad (28)$$

where $|\varphi\rangle = \otimes_{j=2}^{n-1} (Z^{x_j}|+\rangle)$, and Z_j represents Pauli Z gate on j -th address qubit. By Eq. (26), it can be further decomposed into

$$\begin{aligned} |\psi_{0,x,0}(\mu, \nu)\rangle &= Z_1^{x_1} \left(\frac{1}{2\sqrt{2}} (|+\rangle|0\rangle + |+\rangle|1\rangle + |-\rangle|0\rangle + |-\rangle|1\rangle) |\varphi\rangle |\vec{0}\rangle \right. \\ &\quad \left. + (-1)^{x_0} \frac{1}{2\sqrt{2}} (|+\rangle|0\rangle + |+\rangle|1\rangle - |-\rangle|0\rangle - |-\rangle|1\rangle) |\varphi\rangle |\vec{1}\rangle \right). \end{aligned}$$

We permute it and get

$$\begin{aligned} |\psi_{0,x,0}(\mu, \nu)\rangle &= \frac{1}{2\sqrt{2}} Z_1^{x_1} (|+\rangle|0\rangle |\varphi\rangle |\vec{0}\rangle + (-1)^{x_0} |+\rangle|1\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{2\sqrt{2}} Z_1^{x_1} (|+\rangle|1\rangle |\varphi\rangle |\vec{0}\rangle + (-1)^{x_0} |+\rangle|0\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{2\sqrt{2}} Z_1^{x_1} (|-\rangle|0\rangle |\varphi\rangle |\vec{0}\rangle - (-1)^{x_0} |-\rangle|1\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{2\sqrt{2}} Z_1^{x_1} (|-\rangle|1\rangle |\varphi\rangle |\vec{0}\rangle - (-1)^{x_0} |-\rangle|0\rangle |\varphi\rangle |\vec{1}\rangle). \quad (29) \end{aligned}$$

Then apply $Z_1^{x_0}$ and get

$$\begin{aligned} |\psi_{0,x,0}(\mu, \nu)\rangle &= \frac{1}{2\sqrt{2}} (|+\rangle|0\rangle |\varphi\rangle |\vec{0}\rangle + (-1)^{x_0+x_1} |+\rangle|1\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{2\sqrt{2}} (-1)^{x_0} ((-1)^{x_0+x_1} |+\rangle|1\rangle |\varphi\rangle |\vec{0}\rangle + |+\rangle|0\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{2\sqrt{2}} (|-\rangle|0\rangle |\varphi\rangle |\vec{0}\rangle - (-1)^{x_0+x_1} |-\rangle|1\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad - \frac{1}{2\sqrt{2}} (-1)^{x_0} ((-1)^{x_0+x_1} |-\rangle|1\rangle |\varphi\rangle |\vec{0}\rangle + |-\rangle|0\rangle |\varphi\rangle |\vec{1}\rangle). \quad (30) \end{aligned}$$

Extracting $U_{SWAP(0,1)}$, we have:

$$\begin{aligned} |\psi_{0,x,0}(\mu, \nu)\rangle &= \frac{1}{2} U_{SWAP(0,1)} \left(\frac{1}{\sqrt{2}} (|0\rangle|+\rangle |\varphi\rangle |\vec{0}\rangle + (-1)^{x_0+x_1} |1\rangle|+\rangle |\varphi\rangle |\vec{1}\rangle) \right. \\ &\quad + \frac{1}{\sqrt{2}} (-1)^{x_0} ((-1)^{x_0+x_1} |1\rangle|+\rangle |\varphi\rangle |\vec{0}\rangle + |0\rangle|+\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad + \frac{1}{\sqrt{2}} (|0\rangle|-\rangle |\varphi\rangle |\vec{0}\rangle - (-1)^{x_0+x_1} |1\rangle|-\rangle |\varphi\rangle |\vec{1}\rangle) \\ &\quad \left. - \frac{1}{\sqrt{2}} (-1)^{x_0} ((-1)^{x_0+x_1} |1\rangle|-\rangle |\varphi\rangle |\vec{0}\rangle + |0\rangle|-\rangle |\varphi\rangle |\vec{1}\rangle) \right). \quad (31) \end{aligned}$$

By using

$$|\psi_{0,x,1}(\mu, \nu)\rangle = \frac{1}{\sqrt{2}} Z_1^{x_1} ((-1)^{x_0} |1\rangle|+\rangle |\varphi\rangle |\vec{0}\rangle + |0\rangle|+\rangle |\varphi\rangle |\vec{1}\rangle), \quad (32)$$

together with Eq. (28), we obtain:

$$\begin{aligned}
 |\psi_{0,x,0}(\mu, \nu)\rangle &= \frac{1}{2}U_{SWAP(0,1)}(|\psi_{0,x',0}(\mu, \nu)\rangle + (-1)^{x_0}|\psi_{0,x',1}(\mu, \nu)\rangle \\
 &\quad + |\psi_{0,x'',0}(\mu, \nu)\rangle - (-1)^{x_0}|\psi_{0,x'',1}(\mu, \nu)\rangle) \\
 &= \frac{1}{2}(|\psi_{1,x',0}(\mu, \nu)\rangle + (-1)^{x_0}|\psi_{1,x',1}(\mu, \nu)\rangle \\
 &\quad + |\psi_{1,x'',0}(\mu, \nu)\rangle - (-1)^{x_0}|\psi_{1,x'',1}(\mu, \nu)\rangle), \tag{33}
 \end{aligned}$$

where $x' = x'_0 x'_1 x_2 x_3 \cdots x_{n-1}$ with $x'_0 = x_0 \oplus x_1$, $x'_1 = 0$, and $x'' = x''_0 x''_1 x_2 x_3 \cdots x_{n-1}$ with $x''_0 = x_0 \oplus x_1 \oplus 1$, $x''_1 = 1$. Since $|\psi_{0,x,b}\rangle = (-1)^{bx_0} X_0^b |\psi_{0,x,0}\rangle$, we have:

$$\begin{aligned}
 |\psi_{0,x,b}(\mu, \nu)\rangle &= (-1)^{bx_0} X_0^b \frac{1}{2}U_{SWAP(0,1)}(|\psi_{0,x',0}(\mu, \nu)\rangle \\
 &\quad + (-1)^{x_0}|\psi_{0,x',1}(\mu, \nu)\rangle + |\psi_{0,x'',0}(\mu, \nu)\rangle - (-1)^{x_0}|\psi_{0,x'',1}(\mu, \nu)\rangle) \\
 &= (-1)^{bx_0} \frac{1}{2}U_{SWAP(0,1)} X_1^b (|\psi_{0,x',0}(\mu, \nu)\rangle + (-1)^{x_0}|\psi_{0,x',1}(\mu, \nu)\rangle \\
 &\quad + |\psi_{0,x'',0}(\mu, \nu)\rangle - (-1)^{x_0}|\psi_{0,x'',1}(\mu, \nu)\rangle) \\
 &= (-1)^{bx_0} \frac{1}{2}U_{SWAP(0,1)} ((-1)^{bx'_1} |\psi_{0,x',0}(\mu, \nu)\rangle + (-1)^{bx'_1} (-1)^{x_0} |\psi_{0,x',1}(\mu, \nu)\rangle \\
 &\quad + (-1)^{bx''_1} |\psi_{0,x'',0}(\mu, \nu)\rangle - (-1)^{bx''_1} (-1)^{x_0} |\psi_{0,x'',1}(\mu, \nu)\rangle) \\
 &= (-1)^{bx_0} \frac{1}{2}U_{SWAP(0,1)} (|\psi_{0,x',0}(\mu, \nu)\rangle + (-1)^{x_0} |\psi_{0,x',1}(\mu, \nu)\rangle \\
 &\quad + (-1)^b |\psi_{0,x'',0}(\mu, \nu)\rangle - (-1)^{b+x_0} |\psi_{0,x'',1}(\mu, \nu)\rangle) \\
 &= (-1)^{bx_0} \frac{1}{2} (|\psi_{1,x',0}(\mu, \nu)\rangle + (-1)^{x_0} |\psi_{1,x',1}(\mu, \nu)\rangle \\
 &\quad + (-1)^b |\psi_{1,x'',0}(\mu, \nu)\rangle - (-1)^{b+x_0} |\psi_{1,x'',1}(\mu, \nu)\rangle) \tag{34}
 \end{aligned}$$

Now we briefly consider the general case where $|\psi_{l,x,b}(\mu, \nu)\rangle$ are used to decompose $|\psi_{m,x,b}(\mu, \nu)\rangle$. The only thing that we need to do is to replace the 1-st (resp. 0-th) qubit by the l -th (resp. m -th) qubit in the above proof.

A different decomposition can be done when m does not change.

Lemma 11. *For any $m \in \{0, \dots, n-1\}$, $x \in \{0, 1\}^n$, $b \in \{0, 1\}$, and $\mu < \nu \in \{0, 1\}^k$, $\omega \in \{0, 1\}^k \setminus \{\mu, \nu\}$, we have:*

$$\begin{aligned}
 |\psi_{m,x,b}(\mu, \nu)\rangle &= \frac{1}{2} (|\psi_{m,x,b'}(\mu, \omega)\rangle + (-1)^b |\psi_{m,x',b'}(\mu, \omega)\rangle \\
 &\quad + |\psi_{m,x,b''}(\omega, \nu)\rangle - (-1)^b |\psi_{m,x',b''}(\omega, \nu)\rangle), \tag{35}
 \end{aligned}$$

where

- $x' = x'_0 x_1 x_2 \cdots x_{n-1}$ with $x'_0 = x_0 \oplus 1$,
- $b' = b \oplus b_1$ with $b_1 = 0$ if $\mu < \omega$, and $b_1 = 1$ if $\mu > \omega$,
- $b'' = b \oplus b_2$ with $b_2 = 0$ if $\omega < \nu$, and $b_2 = 1$ if $\omega > \nu$,

– we denote $|\psi_{m,x,b'}(\mu, \omega)\rangle = |\psi_{m,x,b'}(\omega, \mu)\rangle$ if $\mu > \omega$. The same for ν and ω .

Proof. First, we observe:

$$\begin{aligned} \frac{|0\rangle|\mu\rangle + |1\rangle|\nu\rangle}{\sqrt{2}} &= \frac{1}{2} \left(\frac{|0\rangle|\mu\rangle + |1\rangle|\omega\rangle}{\sqrt{2}} + \frac{|0\rangle|\mu\rangle - |1\rangle|\omega\rangle}{\sqrt{2}} \right. \\ &\quad \left. + \frac{|0\rangle|\omega\rangle + |1\rangle|\nu\rangle}{\sqrt{2}} - \frac{|0\rangle|\omega\rangle - |1\rangle|\nu\rangle}{\sqrt{2}} \right). \end{aligned}$$

This directly leads to

$$\begin{aligned} V(\mu, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle &= \frac{1}{2} (X_0^{b_1}V(\mu, \omega) + Z_0X_0^{b_1}V(\mu, \omega) \\ &\quad + X_0^{b_2}V(\omega, \nu) - Z_0X_0^{b_2}V(\omega, \nu))|+\rangle^{\otimes n}|\vec{0}\rangle, \end{aligned}$$

where $b_1 = 0$ if $\mu < \omega$, $b_1 = 1$ if $\mu > \omega$, and $b_2 = 0$ if $\omega < \nu$, $b_2 = 1$ if $\omega > \nu$. Therefore,

$$\begin{aligned} Z(x)X_0^bV(\mu, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle &= \frac{1}{2} (Z(x)X_0^{b\oplus b_1}V(\mu, \omega)|+\rangle^{\otimes n}|\vec{0}\rangle + Z(x)X_0^bZ_0X_0^{b_1}V(\mu, \omega)|+\rangle^{\otimes n}|\vec{0}\rangle \\ &\quad + Z(x)X_0^{b\oplus b_2}V(\omega, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle - Z(x)X_0^bZ_0X_0^{b_2}V(\omega, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle) \\ &= \frac{1}{2} (Z(x)X_0^{b\oplus b_1}V(\mu, \omega)|+\rangle^{\otimes n}|\vec{0}\rangle + (-1)^bZ(x)Z_0X_0^{b\oplus b_1}V(\mu, \omega)|+\rangle^{\otimes n}|\vec{0}\rangle \\ &\quad + Z(x)X_0^{b\oplus b_2}V(\omega, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle - (-1)^bZ(x)Z_0X_0^{b\oplus b_2}V(\omega, \nu)|+\rangle^{\otimes n}|\vec{0}\rangle) \end{aligned}$$

and we complete the proof.

Now we are ready to prove Theorem 3. The control qubits $|c\rangle$ here can be ignored, since Bob can read c by measurements without changing it. Suppose: (i) the correct test state is $|\psi_{m,x,b}(\mu, \nu)\rangle$; (ii) measurement operator M_v is observed; and (iii) Bob sends the state $|\psi_{m',x',b'}(\mu', \nu')\rangle$ to Alice. Write $\Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |M_v\rangle)$ for the probability that Bob success to pass the test in this case. First, we have:

$$\begin{aligned} &\Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |M_v\rangle) \\ &= \sum_{m,x,b,\mu,\nu} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu, M_v\rangle) \Pr(m, x, b, \mu, \nu | M_v) \\ &= \sum_{m,x,b,\mu,\nu} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu\rangle) \Pr(m, x, b, \mu, \nu | M_v), \end{aligned}$$

where the last equality is because of the following fact:

– once the original test state $|\psi_{m,x,b}(\mu, \nu)\rangle$ is fixed, Bob's success probability is independent of the measurement results and only dependent on what state he sends.

Now we compute the probability $\Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle$ passes $|m, x, b, \mu, \nu\rangle$ that the correct test state is $|\psi_{m,x,b}(\mu, \nu)\rangle$, and Bob sends the state $|\psi_{m',x',b'}(\mu', \nu')\rangle$ to Alice:

Case 1. $|\psi_{m',x',b'}(\mu', \nu')\rangle$ and $|\psi_{m,x,b}(\mu, \nu)\rangle$ are in the same basis of Lemma 6. Then $\Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle$ passes $|m, x, b, \mu, \nu\rangle \leq 1$.

Case 2. $|\psi_{m',x',b'}(\mu', \nu')\rangle$ and $|\psi_{m,x,b}(\mu, \nu)\rangle$ are in different bases of Lemma 6, and $m = m'$. There are two subcases:

Subcase 2.1. Bob sends $|\psi_{m',x',b'}(\mu', \nu')\rangle$ for both two test states. Then the best situation for Bob is $x' = x$, $b = b'$, and $\mu = \mu'$ without any loss of generality. (Another best situation is $x' = x$, $b = b'$, and $\nu = \nu'$.) Then after $U_{SWAP(0,m)}$, $Z(x)$, X_0^b , $V(\mu, \nu)$ and W , the state $|\psi_{m',x',b'}(\mu', \nu')\rangle$ becomes

$$\frac{1}{\sqrt{2}}(|+\rangle|0\rangle^{\otimes n+k-1} + |-\rangle|0\rangle^{\otimes n-1}|\nu \oplus \nu'\rangle).$$

Since $\nu \neq \nu'$ (Otherwise, it becomes Case 1), we have four different measurement outcomes:

1. $00 \cdots 0$ on address and data qubits.
2. $100 \cdots 0$ on address and data qubits.
3. $00 \cdots 0$ on address qubits, and $\nu \oplus \nu' \neq 0 \cdots 0$ on data qubits.
4. $10 \cdots 0$ on address qubits, and $\nu \oplus \nu' \neq 0 \cdots 0$ on data qubits.

Each of the four have probability 0.25. Then the situation that the two states pass the test only happens when both of the outcomes in Case 1 are observed, or both of the outcomes in Case 2 are observed. The corresponding probability is $\frac{1}{8}$.

Case 2.2. Bob sends $|\psi_{m',x',b'}(\mu', \nu')\rangle$ for only one test state. Then at Step 8, no matter what test state Bob sends for the other one, the probability is at most 0.25 by the analysis of Case 2.1.

Case 3. $|\psi_{m',x',b'}(\mu', \nu')\rangle$ and $|\psi_{m,x,b}(\mu, \nu)\rangle$ are in different bases of Lemma 6, and $m \neq m'$. Then there are also two subcases. The analysis is similar to Case 2, and the probability is at most 0.25.

Now by Lemma 6 and Lemma 7, we have:

$$\begin{aligned} & \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |M_v\rangle) \\ &= \sum_{m,x,b,\mu,\nu} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu, M_v\rangle) \Pr(m, x, b, \mu, \nu | M_v) \\ &= \sum_{m,x,b,\mu,\nu} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu\rangle) \Pr(m, x, b, \mu, \nu | M_v) \\ &= \sum_{B:|\psi'\rangle \in B} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu\rangle) \Pr(m, x, b, \mu, \nu | M_v) \\ &\quad + \sum_{B:|\psi'\rangle \notin B} \Pr(|\psi_{m',x',b'}(\mu', \nu')\rangle \text{ passes } |m, x, b, \mu, \nu\rangle) \Pr(m, x, b, \mu, \nu | M_v) \\ &\leq 1 \times \frac{1}{K} + \frac{1}{4} \times \frac{K-1}{K} = \frac{1}{4} + \frac{3}{4n(2^k-1)}, \end{aligned}$$

where $K = n(2^k - 1)$ is the number of bases in Lemma 6, $B : |\psi'\rangle \in B$ represents Case 1, and $B : |\psi'\rangle \notin B$ represents Cases 2 and 3.

B.10 Proof of Lemma 8

Suppose Alice send a test state $|\psi\rangle = \frac{1}{\sqrt{N}} \sum |i\rangle|\mu_i\rangle$ to Bob, and after Bob's action, Alice receives $|\psi'\rangle$. If $\mu_i \not\subseteq d$, then the states are the same, and Alice can not detect it. If $\mu_i \subseteq d$, then

$$|\langle\psi'|\psi\rangle|^2 = \left(1 - \frac{2}{N}\right)^2 = 1 - O\left(\frac{1}{N}\right)$$

and it can be detected with probability at most $O\left(\frac{1}{N}\right)$.

Even if in one run of the inner protocol, Alice employs such tests many times, she still cannot detect it with a considerable probability. Suppose Bob's success probability is at least $1 - \frac{a}{N}$, and Alice employs tests totally $b\sqrt{N}$ times, where a, b are constants. Since there are at most $\frac{\pi}{4}\sqrt{N}$ iterations in an entire protocol, Bob successes to cheat in a run of the whole protocol with probability $\left(1 - \frac{a}{N}\right)^{b\sqrt{N}} \approx e^{-\frac{ab}{\sqrt{N}}} \approx 1$.

C Further Methods to Protect Bob's Privacy

Due to the limit of space, protection of Bob's privacy was only very briefly discussed in Section 8. Here, we continue to consider this issue. If Alice is dishonest, one simple way for her to recover f is as follows:

1. For each loop i , Alice always employs two test rounds. Among them, one replaces the original computational round.
2. Alice always chooses $\nu = \vec{1}$. Then $f_i(\mu) = 1$ if and only if $f_i(\mu) = f_i(\nu)$.
3. For the loops corresponding to the same control qubit, Alice chooses one fixed μ , and gets $f_i(\mu)$ for all i . Then she can determine $f(\mu)$ by choosing the majority among these $f_i(\mu)$.

This simple method can recover f but with possible errors because a confusing qubit is added (see Definition 4). Alice can use some other methods to recover f without errors. For instance, she can first get $f(\mu)$ for the same μ from the loops corresponding to three different control qubits. Since there is only one confusing qubit, two of these three values of $f(\mu)$ must be correct. So, she can get the correct value $f(\mu)$ for some μ . Once she find some ξ with $f(\xi) = 0$, Alice may distinguish h from f as $h(\xi) = 1 \neq 0 = f(\xi)$, and then recover the entire f .

In remainder of this subsection, we present some further methods to preserve Bob's privacy.

C.1 Adding a Second Confusing Qubit

If Bob adds a second confusing qubit in his strategy (Definition 4), possibly only one quarter of functions f_i corresponding to some control qubit may be f . Thus, Alice cannot get correct $f(\mu)$ by choosing the majority. The following are some sequences of the 16 functions corresponding to a control qubit:

$$\begin{aligned}
 & f, f, a, h, a, h, f, f, g, g, b, h, b, g, g, h \\
 & g, g, a, h, a, g, g, h, f, f, b, h, b, h, f, f \\
 & f, h, g, a, h, a, g, f, g, b, h, b, g, h, f, f \\
 & h, h, f, f, a, a, h, a, a, h, f, f, h, b, h, b \\
 & h, h, f, f, g, g, h, g, g, h, f, f, h, f, h, f \\
 & \vdots
 \end{aligned}$$

In these sequences,

- there are no fixed locations for f , and f can be anywhere;
- f can be either the minority or the majority;
- Moreover, it is impossible for Alice to get $f(\mu)$ by counting the number of ones or zeros for the value of $f_i(\mu)$, if we set $g = 1 - f$. This is because the number of ones or zeros can be any value from 4 to 12 when $g = 1 - f$. Since the distribution is symmetric, Alice cannot recover $f(\mu)$ by voting.

Therefore, by updating his strategy and carefully choosing the noises, Bob can prevent Alice from disclosing $f(\mu)$ through voting.

C.2 Preventing Alice from Cheating in Computational Rounds

Consider the case where there is only one control qubit, and the state is $|+\rangle \sum_j \alpha_j |j\rangle |0\rangle$. Then there is only one function f to be applied.

- If $f = h$, which corresponds to the identity operator $I_{a,d}$, then after the iteration $U_D(y)$, controlled $I_{a,d}$, $U_D(y)$ and controlled \bar{G} , the state becomes

$$(|0\rangle\langle 0| \otimes I_{a,d} + |1\rangle\langle 1| \otimes \bar{G})|+\rangle \sum_j \alpha_j |j\rangle |0\rangle.$$

- If $f = \bar{h} = 1 - h$, which corresponds to the identity operator $-I_{a,d}$, then the state becomes

$$\begin{aligned}
 |+\rangle \sum_j \alpha_j |j\rangle |0\rangle & \rightarrow |+\rangle \sum_j \alpha_j |j\rangle |d_{j\oplus y}\rangle \\
 & \rightarrow \frac{1}{\sqrt{2}}(|0\rangle \otimes (I_{a,d} \sum_j \alpha_j |j\rangle |d_{j\oplus y}\rangle) + |1\rangle \otimes (-I_{a,d} \sum_j \alpha_j |j\rangle |d_{j\oplus y}\rangle)) \\
 & = |-\rangle \sum_j \alpha_j |j\rangle |d_{j\oplus y}\rangle \rightarrow |-\rangle \sum_j \alpha_j |j\rangle |0\rangle \\
 & \rightarrow (|0\rangle\langle 0| \otimes I_{a,d} + |1\rangle\langle 1| \otimes \bar{G})|-\rangle \sum_j \alpha_j |j\rangle |0\rangle.
 \end{aligned}$$

This fact means that Bob can control the final result by choosing his functions.

Example 11. Suppose Bob wants to run Algorithm 1 with $T = 8$ loops. Then there are three control qubits, denoted by C_0, C_1, C_2 . Suppose Bob chooses his function as follows:

- C_0 : f', h, f', h ,
- C_1 : \bar{h}, h ,
- C_2 : \bar{h} ,

where f' is an arbitrary function. After 8 iterations at Step 12, the state becomes

$$|+\rangle|-\rangle \otimes ((|0\rangle\langle 0| \otimes I_{a,d} + |1\rangle\langle 1| \otimes \bar{G})|-\rangle \sum_j \alpha_j |j\rangle|0\rangle |f(d_{j\oplus y})\rangle).$$

Thus, if Bob undoes the operator \bar{G} controlled by C_2 , the control qubits becomes separable from the other part and the control state is $|+\rangle|-\rangle|-\rangle$.

In the above example, if Alice cheats in any computational round, the result becomes different. For instance, if Alice cheats on the computational round corresponding to C_2 , then Bob's function \bar{h} is applied on the cheating state but not the computational state. Thus, Alice has to guess what is the correct function to recover her cheating. Consequently, even if Alice knows that Bob randomly chooses h (corresponding to result $|+\rangle$) or \bar{h} (corresponding to result $|-\rangle$) in this step, it has probability 0.5 to be detected. Therefore, Bob can use this method to detect Alice's attacks with a high success probability.

C.3 Restricting the Number of Alice's Tests

After preventing Alice from cheating in the computational rounds, Bob can further reduce the chances that Alice can cheat. Note that there is at most one test round in each loop i , and this test round appears randomly with probability $2p$. Then by Chebyshev's inequality, we have:

$$\Pr(|n_t - 2pT| \geq 6pT) \leq \frac{2p(1-2p)T}{(6pT)^2} = \frac{1-2p}{18pT},$$

where n_t is the number of test rounds. In this paper, we usually set $p = 0.05$, and T should be $400/\sqrt{s_{\min}}$ as a second confusing qubit is added. So, if $s_{\min} = 0.2$, T should be 1024. By the above inequality, the probability that there are at least $0.4T$ test rounds in one run of Algorithm 1 is no more than $\frac{0.9}{0.95 \cdot 1024} < 0.001$. Thus, Bob can count the number of test rounds in one run of Algorithm 1. If it exceeds $0.4T \approx 410$, he may terminate the current run. The false positive probability is less than 0.001. This probability is tolerable, if Algorithm 1 is executed once. If the algorithm is executed M times, this probability will be enlarged. For instance, if $M = 100$, the total false positive probability may be approximately 0.095. Fortunately, it is still easy to deal with this false positive.

- M is small, say 100. For the first time the number of test rounds exceeds $0.4T$, Bob simply terminates the current run and start a new run. He announces that Alice is cheating by setting more test rounds when this situation happens twice. Then the total false positive probability is smaller than 0.005.
- M is big, say $M > 1000$. Bob can announce Alice's dishonesty when this excess happens $0.02M$. Then the total false positive probability is smaller than 0.0025.

An Alternative Method Another way is to restrict the number of Alice's test rounds in a row. For instance, if test rounds are employed in six sequential loops, Bob terminates the algorithm. The false positive probability here is less than $1 - (1 - 0.1^6)^{1024} < 0.0011$.

C.4 Summary

Thus Bob can considerably reduce his privacy leakage

- by adding a second confusing qubit and carefully choosing noise functions (In this way, Bob can make it impossible for Alice to recover any $f(\mu)$ by voting).
- by adding tests and counting the number of Alice's test rounds (In this way, Bob can further reduce the amount of information that Alice can get).

Remark 2. It is worth noting that the above methods were not included in Algorithm 1. If Bob directly use these methods, he might be treated as a dishonest data user. So, in order to make these methods work, Algorithm 1 should be modified.

D More Discussions

D.1 Alice's Strategy to Detect Attack in Example 7

An question was left open in Example 7: how Alice can detect an attack? Since the attack there is not very serious, here we only give an example rather than a formal protocol to deal with it.

If in one test, Alice employs $|\psi_{m,x,b}(\mu, d)\rangle$ (suppose $\mu < d$) as the test state with probability $O(\frac{1}{2^k})$, then she will find $f(d) \neq f(\mu)$ after receiving the returned test state. Thus, she can flip one 0 to 1 in d and obtain d' . She further employs $|\psi_{m,x,b}(\mu, d')\rangle$ as another test state. Since $f(x) = \delta(x, d)$, the second test state leads to $f(d') = f(\mu)$, which is not a result of any function indicating an inclusion relation \subseteq . So, the attack is detected. But such a detection does not really work in practice since its probability is $O(\frac{1}{2^k})$ and extremely low, as d should be chosen randomly. This detection strategy was not included in the original protocol, since Alice changes d for the second test state.

D.2 Bob's Privacy without Noise and Tests

Bob's privacy was considered in Section 8 with the assumption that he can add noise and employs tests to protect himself. Here, we further analyse Bob's privacy in the case where he is not allowed to add noise or to use any test.

Case 1. Alice is honest: All the information she gets about Bob's function f is whether $f(\mu) = f(\nu)$ in the test rounds. Since she is honest, she will not use this information to compute the detailed form of f . So, Bob's privacy is preserved.

Case 2. Alice is semi-honest: She will employ all the legally derived information of $f(\mu) = f(\nu)$ to compute f . We have showed in Section 8 that in the best case for Alice, k couples of (μ, ν) are sufficient to recover f . On the other hand, in Algorithm 1, the expected number of test states is $4(T+1)p$. So, if the following condition is satisfied:

$$4(T+1)p < k, \quad (36)$$

then Alice cannot determine f with certainty. Note that inequality (36) is true for a big database. In fact, in a big database, since N and k may be very large, s_{\min} must not be too small. This is because small s_{\min} may result in too many rules mined by Bob, and these rules have a low support and thus are not important in practice [2]. This problem is serious for a big database. So, Eq. (36) is satisfied very likely. For example, if $k = 80$, $s_{\min} = 0.2$ and $p = 0.05$, we have that $T = 256$ ($> 100/\sqrt{s_{\min}}$) and then $4(T+1)p = 51.4 < 80 = k$.

One thing worth to mention is that the above analysis is just ideal. The pair (μ, ν) is generated randomly. So, such random k pairs may provide repetitive information, and the right side of Eq. (36) is then much larger in practice.

Case 3. Alice is dishonest: She may generate (μ, ν) by her strategy without randomness. Even further, she can make each round as a test round. Therefore, Alice can get explicitly f more likely, as k rounds are sufficient.