1-1-2015

Two quantum protocols for Oblivious Set-member Decision problem

Run-hua Shi
University of Wollongong, rshi@uow.edu.au

Yi Mu
University of Wollongong, ymu@uow.edu.au

Hong Zhong
University of Wollongong

Jie Cui
Anhui University

Shun Zhang
Anhui University

Two quantum protocols for Oblivious Set-member Decision problem

Abstract

In this paper, we defined a new secure multi-party computation problem, called Oblivious Set-member Decision problem, which allows one party to decide whether a secret of another party belongs to his private set in an oblivious manner. There are lots of important applications of Oblivious Set-member Decision problem in fields of the multi-party collaborative computation of protecting the privacy of the users, such as private set intersection and union, anonymous authentication, electronic voting and electronic auction. Furthermore, we presented two quantum protocols to solve the Oblivious Set-member Decision problem. Protocol I takes advantage of powerful quantum oracle operations so that it needs lower costs in both communication and computation complexity; while Protocol II takes photons as quantum resources and only performs simple single-particle projective measurements, thus it is more feasible with the present technology.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Shi, R., Mu, Y., Zhong, H., Cui, J. & Zhang, S. (2015). Two quantum protocols for Oblivious Set-member Decision problem. Scientific Reports, 5 1-9.

SCIENTIFIC REPORTS

OPEN

Two Quantum Protocols for Oblivious Set-member Decision Problem

Received: 16 July 2015
Accepted: 05 October 2015
Published: 30 October 2015

Run-hua Shi[1,2], Yi Mu[2], Hong Zhong[1], Jie Cui[1] & Shun Zhang[1]

In this paper, we defined a new secure multi-party computation problem, called Oblivious Set-member Decision problem, which allows one party to decide whether a secret of another party belongs to his private set in an oblivious manner. There are lots of important applications of Oblivious Set-member Decision problem in fields of the multi-party collaborative computation of protecting the privacy of the users, such as private set intersection and union, anonymous authentication, electronic voting and electronic auction. Furthermore, we presented two quantum protocols to solve the Oblivious Set-member Decision problem. Protocol I takes advantage of powerful quantum oracle operations so that it needs lower costs in both communication and computation complexity; while Protocol II takes photons as quantum resources and only performs simple single-particle projective measurements, thus it is more feasible with the present technology.

Cryptography is an important tool that enables the secure transmission of a secret message between a sender and a recipient from any potential eavesdropper. On the one hand, however, the security of most classical cryptosystems is based on the assumption of computational complexity, which is strongly challenged by the increasing capability of computations or algorithms[1,2]. Especially, it is believed that some mathematical difficulties, e.g. the integer factorization or the discrete logarithm problems, may be fragile in the future with the presence of quantum computers. On the other hand, fortunately, this difficulty can be overcome by quantum cryptography[3,4], where the security is guaranteed by physical principles. Since Bennett and Brassard presented the first quantum key distribution protocol[5], quantum cryptography has been widely studied and rapidly developed. Accordingly, a lot of results have been gained, such as quantum key distribution[6], quantum teleportation[7], quantum signature[8], and other novel quantum computations[9].

Furthermore, in many cryptographic tasks, it requires to protect not only the data privacy, but also the user privacy. Private query is an important problem of this type. Suppose that a user, Alice, wants to know an item of a database held by a database provider, Bob, but does not want him to know which item she is interested in. Bob in turn wants to limit the amount of item that she can get from the database.

In 2008, Giovannetti, *et al.*[10,11] for the first time presented a cheat sensitive quantum private query (QPQ) protocol. In their protocol, Alice and Bob only exchange two quantum messages. For example, Alice wants to find out the jth record of Bob's database. She first prepares two n-qubit query states $|j\rangle$ and $(|0\rangle + |j\rangle)/\sqrt{2}$. She then sends, in random order, these two query states to Bob, waiting for his first reply before sending the second. As a response to query, Bob performs two oracle operations on the two query states and then sends them back to Alice, respectively. Finally, Alice processes the two returned states $|j\rangle|A(j)\rangle$ and $(|0\rangle|A(0)\rangle + |j\rangle|A(j)\rangle)/\sqrt{2}$, where the $A(j)$ is the content of the jth record in the database. By measuring the first state she obtains the value of $A(j)$, and further she checks Bob's potential attack with $A(j)$, that is, she checks whether the superposition in the second state is preserved. Compared

[1]School of Computer Science and Technology, Anhui University, Hefei City, 230601, China. [2]Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia. Correspondence and requests for materials should be addressed to R.-H.S. (email: shirh@ahu.edu.cn)

to known private information retrieval protocols, this QPQ protocol achieves an exponential reduction in both communication and computation complexity. Later, Olejnik[12] presented an improved protocol for QPQ using phase-encoded queries, in which the oracle operation and the encoding method are subtly selected so that one query state $(|0\rangle + |j\rangle)/\sqrt{2}$ can achieve two aims simultaneously, i.e., obtaining the expected item and checking Bob's potential attack. So the communication complexity and the computation complexity in Olejnik's protocol are further reduced.

In addition, Jakobi *et al.*[13] proposed a novel and practical quantum private query protocol based on SARG04 quantum key distribution (QKD) protocol[14]. By using SARG04 QKD, an asymmetric key can be distributed between Alice and Bob, where Alice only knows one bit of the key, while Bob knows the whole key. For instance, Bob prepares a long sequence of photons which are randomly in one of four states $\{|\uparrow\rangle, |\downarrow\rangle, |\rightarrow\rangle, |\leftarrow\rangle\}$ and sends them to Alice. Then Alice measures each received photon in $\updownarrow$ or $\leftrightarrow$ basis at random. Obviously, Alice will measure half of the qubits she receives in the correct basis. When Bob subsequently announces the bases, we can easily see that (I) Bob knows the entire "raw key", (II) Alice knows half of the bits and (III) Bob cannot know which ones Alice has measured correctly. In order to reduce Alice's information on the key, Alice and Bob cut the raw key into multiple substrings of length N, and add these strings bitwise to obtain the final key with length N. Later, Gao *et al.* generalized Jakobi's protocol and proposed a similar 4-state QPQ protocol[15], which uses four generalized states $\{|0\rangle, |1\rangle, |0'\rangle, |1'\rangle\}$, where $|0'\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $|1'\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle\}$. Gao's protocol exhibits better database security than Jakobi's protocol, but has a higher probability with which Bob can correctly guess the address of Alice's query. Subsequently, to improve the security, yang *et al.* proposed a flexible B92-based QPQ protocol[16].

In this paper, we define a new but interesting problem, Oblivious Set-member Decision problem, which allows a server, Bob, to decide whether a secret of a user, Alice, belongs to his private set in an oblivious manner. That is, Bob wants to know whether Alice's secret is a member of his private set. But Alice does not want him to know which member it is. Oblivious Set-member Decision can be used to privately compute multi-party set intersection and union which are widely applied in some privacy-preserving and information-sharing settings[17]. In addition, there are also lots of practical applications of Oblivious Set-member Decision in fields of the identifiable or verifiable circumstances, such as anonymous authentication, electronic voting and electronic auction. Thus Oblivious Set-member Decision problem is one of the most fundamental and key problems within the multi-party collaborative computation of protecting the privacy of the users.

In next section, inspired by the QPQ protocols mentioned above, we proposed two quantum protocols for Oblivious Set-member Decision problem, which one subtly applies the powerful quantum oracle operations, while the other utilizes the asymmetric key between Alice and Bob based on the technologies of Quantum Key Distribution.

Results

Here, we first give a definition of Oblivious Set-member Decision protocol.

Definition 1 (Oblivious Set-member Decision Protocol). A user, Alice, inputs a secret k, and a server, Bob, inputs a private set $\{k_1, k_2, \ldots, k_n\}$. Finally, Alice gets nothing but Bob outputs one bit 0 or 1. This protocol should meet the following requirements:

Correctness. Bob gets 1 if $k \in \{k_1, k_{2,\ldots} k_n\}$, and 0 otherwise.

Alice's Privacy. Except knowing whether Alice's secret belongs to his private set, Bob cannot obtain any other secret information about Alice's secret k.

Alice's anonymity. Bob cannot know which member it is, if Alice's secret is a member of his private set.

Bob's Privacy. Alice cannot know any secret information about Bob's private set.

Protocol I. Protocol I follows some ideas from QPQ in refs 10,12, and refers to the oracle of Grover search algorithm[2]. Suppose Alice's secret k and Bob's all private member k_is are the elements of $\mathbb{Z}_N^*$, where $\mathbb{Z}_N^* = \{1, 2, \ldots, N-1\}$. Protocol I consists of 5 steps, which are described in detail as follows:

Step 1. Alice prepares a query state $|\psi\rangle$, where $|\psi = \frac{|0\rangle + |k\rangle}{\sqrt{2}}$ and k is her secret. Then Alice sends the query state $|\psi\rangle$ to Bob by an authenticated quantum channel.

Step 2. After receiving the query state $|\psi\rangle$ from Alice, Bob applies an oracle O_1 on it, where the oracle O_1 is a unitary operator, defined as follows:

$$f(x) = (x - k_1)(x - k_2)\cdots(x - k_n) \bmod N, \tag{1}$$

$$f^*(x) = [f(x)/N], \tag{2}$$

$$\text{i.e.}, f^*(x)\begin{cases}0 & if\ x \in \{k_1, k_2, \ldots, k_n\}\\ 1 & if\ x \notin \{k_1, k_2, \ldots, k_n\}\end{cases}, \tag{3}$$

$$|\psi\rangle \xrightarrow{O_1} |\phi\rangle, \tag{4}$$

$$\begin{aligned}|\phi\rangle &= O_1|\psi\rangle\\ &= O_1\frac{|0\rangle + |k\rangle}{\sqrt{2}}\\ &= \frac{|0\rangle + (-1)^{f^*(k)}|k\rangle}{\sqrt{2}}.\end{aligned} \tag{5}$$

Furthermore, Bob tosses a coin to decide whether applies another oracle O_2 on the state $|\phi\rangle$. That is, if the outcome is the head, he performs the oracle O_2 on the state $|\phi\rangle$. Otherwise, he does nothing. Obviously, he performs the oracle O_2 on the state $|\phi\rangle$ only with the probability of $\frac{1}{2}$, where the oracle O_2 is defined by

$$|\phi\rangle \xrightarrow{O_2} |\varphi\rangle, \tag{6}$$

$$\begin{aligned}|\varphi\rangle &= O_2|\phi\rangle\\ &= O_2\frac{|0\rangle + (-1)^{f^*(k)}|k\rangle}{\sqrt{2}}\\ &= \frac{|0\rangle - (-1)^{f^*(k)}|k\rangle}{\sqrt{2}}\\ &= \frac{|0\rangle + (-1)^{(f^*(k)+1)}|k\rangle}{\sqrt{2}}.\end{aligned} \tag{7}$$

Then Bob sends the state $|\varphi\rangle$ back to Alice by the authenticated quantum channel.

Step 3. After receiving the state $|\varphi\rangle$ from Bob, Alice performs an honest test. That is, Alice checks whether the superposition in the returned state is preserved as follows: $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$ or $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$. Since the two possible states are obviously orthogonal and further Alice knows the value of k, she is able to completely distinguish them by a von Neumann measurement. If Alice finds a cheat of Bob, she will terminate this protocol; otherwise continue to the next step.

Step 4. Alice extracts out the phase information $p(k)$ of the returned state $|\varphi\rangle$ by distinguishing it between $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$ and $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$, i.e., $p(k) = 1$ if it is in the state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$, and $p(k) = -1$ otherwise. Then she sends the classical information $p(k)$ to Bob by the authenticated classical channel.

Step 5. After receiving the classical information $p(k)$ from Alice, Bob decrypts it to further obtain $f^*(k)$, where $(-1)^{f^*(k)+1} = p(k)$ if he has applied the oracle O_2, and $(-1)^{f^*(k)} = p(k)$ otherwise. If $f^*(k) = 0$, Bob can decide that Alice's secret belongs to his private set. Otherwise, it doesn't.

Protocol II. Protocol II is inspired by the ideas from refs 13,15,16 in which an asymmetric key is distributed between Alice and Bob based on Quantum Key Distribution, where Alice only knows a few bits of the key, while Bob knows the whole key. Protocol II includes 6 steps, which is described in detail as follows:

Step 1. Bob creates an N-element database by his private set $\{k_1, k_2, \ldots, k_n\}$, where the jth element $p(j) = 1$ if $j = k_i$ ($i \in \{1, 2, \ldots, n\}$), and $p(j) = 0$ otherwise. Furthermore, Bob generates a random integer $r \in \mathbb{Z}_N^*$ and computes $s(j) = p(j) + r$ for $j = 1$ to N (encryption). Here $+$ denotes the binary XOR operation.

Step 2. By calling Gao *et al.*'s protocol[15], Alice and Bob share an N-bit key K^r, where Bob knows the whole key K^r and Alice knows only q bits of K^r, where q is a security parameter. Furthermore, among these q bits, Alice randomly chooses $q - 1$ bits to check Bob's honesty. That is, she requests Bob to announce the values of these bits. If these bits announced by Bob aren't completely same as those Alice has recorded, it will show that Bob is dishonest. If Alice finds a cheat of Bob, she will terminate this protocol; otherwise continue to the next step.

Step 3. Suppose the remaining one bit known by Alice is the jth bit $K^r(j)$ of the raw key K^r. However, she expects to get the kth bit of the shared key, where k is Alice's secret. So she declares the number $s = j - k$.

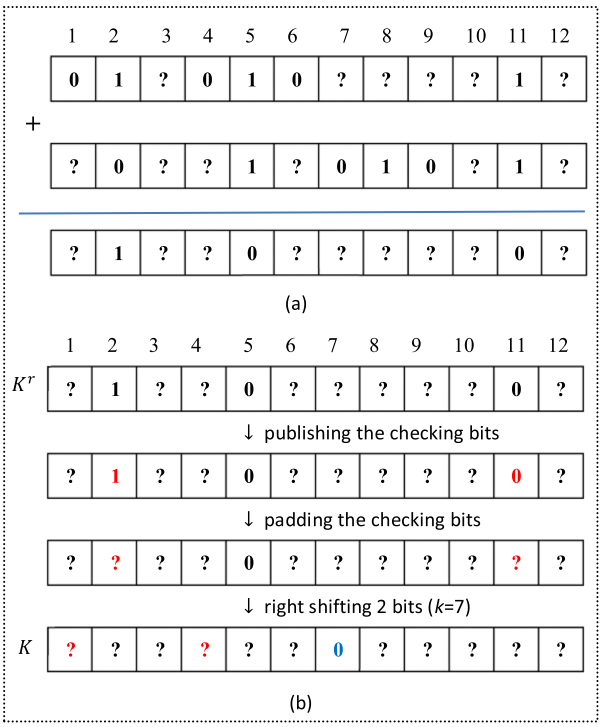

Figure 1. Illustration of creating the asymmetric key. (**a**) How to reduce Alice's information on the key. (**b**) How to process the raw key K^r to get the final key K.

Step 4. Bob replaces the announced $q - 1$ bits in the key K^r by random 0 or 1 integer. Then Bob shifts K^r by s and finally gets an asymmetric key K shared between Alice and Bob, where Bob knows the whole shared key, while Alice only knows the kth bit of the shared key. Furthermore, Bob encrypts all $s(j)$s by using the key K in one-time pad method, that is, he computes $e(j) = s(j) + K(j)$ for $j = 1$ to N, where $K(j)$ is the jth bit of the shared key K. Then Bob publishes the whole encrypted database (i.e., all $e(j)$s for $j = 1$ to N) at a public server.

Step 5. Alice gets $e(k)$ from the public encrypted database of Bob, and further decrypts it to obtain $s(k)$, since $e(k) = s(k) + K(k)$ and she (only) knows $K(k)$. Then Alice sends the classical information $s(k)$ to Bob by the authenticated classical channel.

Step 6. After receiving the classical information $s(k)$ from Alice, Bob computes $p(k) = s(k) + r$ (decryption). If $p(k) = 1$, then he can deduce that Alice's secret k belongs to his private set $\{k_1, k_2, \ldots, k_n\}$, i.e., $k \in \{k_1, k_2, \ldots, k_n\}$. Otherwise, $k \notin \{k_1, k_2, \ldots, k_n\}$.

Here we give a simple example to better illustrate Protocol II, as shown in Figs 1 and 2. In our example, Alice has a secret 7 (i.e., $k = 7$), and Bob has a private set $\{1, 4, 6, 9, 11\}$ in $\mathbb{Z}_{12}^*$. On the one hand, Alice and Bob share an asymmetric key K (see Fig. 1), where Alice only knows the seventh bit of K (i.e., $K(7)$), while Bob knows all bits of K. On the other hand, Bob creates a private database $\{p(1), p(2),\ldots, p(12)\}$ by his private set, where $p(1) = p(4) = p(6) = p(9) = p(11) = 1$ and other $p(j)$s are equal to 0 (see Fig. 2), further encrypts each item $p(j)$ twice by using two different keys, r and $K(j)$, and finally publishes all $e(j)$s. Obviously, Alice can rightly get $s(7)$ by computing $K(7) + e(7)$, but not $p(7)$ without knowing r. However, Bob can rightly get $p(7)$ by computing $s(7) + r$, but he does not know which item of his private database it is equivalent to, except knowing Alice's secret does not belong to his private set since $p(7) = 0$.

Security of the protocols

Protocol I. The oracles O_1 and O_2 are all phase transformation operations, where the former is utilized to encode $f^*(k)$, while the later to further encrypt it in the one-time pad method. On the one hand, obviously Alice doesn't know $f^*(k)$ with $p(k)$ due to the oracle O_2. However, Bob can get it rightly by whether or not the oracle O_2 has been performed and then he can easily decide whether Alice's secret lies in his private set by the value of $f^*(k)$. That is, it guarantees the **correctness** of Protocol I. On the other hand, we can easily see that $f^*(k)$ doesn't leak Alice's secret k. Even if $f^*(k) = 0$, it doesn't yet leak which member it is equal to. That is, it guarantees **Alice's anonymity**.

Bob {1, 4, 6, 9, 11}				$N = 12$ $r = 1$
$p(j)$	$s(j)$	$K(j)$	$e(j)$	j
1	0	?	?	1
0	1	?	?	2
0	1	?	?	3
1	0	?	?	4
0	1	?	?	5
1	0	?	?	6
0	**1**	**0**	**1**	**7**
0	1	?	?	8
1	0	?	?	9
0	1	?	?	10
1	0	?	?	11
0	1	?	?	12

Figure 2. Bob's encoding and encrypting methods. All $p(j)$s, $s(j)$s and $K(j)$s are private, while all $e(j)$s are public. Alice can only decrypt $e(7)$ to further get $s(7)$ with the key $K(7)$. Finally, Bob can rightly get $p(7)$ by computing $p(7) = s(7) + r$.

Furthermore, **Alice's privacy** depends on Bob's impossibility of discriminating the query state sent from Alice. Two basic laws of quantum theory enforce this: No-cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state, and Heisenberg Uncertainty Principle which implies that it is impossible to measure the state of any system without disturbing that system. In order to extract the secret information about k from the query state $|\psi\rangle = \frac{|0\rangle + k}{\sqrt{2}}$, obviously Bob must measure the state $|\psi\rangle$, but he will certainly disturb it. We will analyze two measure-based attacks by a dishonest Bob in detail.

First, if Bob directly measures the query state $\frac{|0\rangle + |k\rangle}{\sqrt{2}}$ by a simple projective measurement (intercept), the measured result can be either $|0\rangle$ or $|k\rangle$ with the probabilities $\frac{1}{2}$ and $\frac{1}{2}$, respectively. If he gets $|k\rangle$, he can successfully pass the honest test by re-preparing a new quantum system in the state $|\psi\rangle = \frac{|0\rangle + k}{\sqrt{2}}$ and returning it to Alice (resend). However, if he gets $|0\rangle$, he cannot pass the honest test. In short, this intercept-resend attack will be discovered in the honest test with the probability of $\frac{1}{2}$. That is, Protocol I is cheat sensitive[10,12].

Furthermore, we discuss a more complicated entangle-measure attack by a dishonest Bob that he is able to prepare an ancillary system and entangle the ancillary system with the query state from Alice by his local unitary operations, and afterwards he can measure the ancillary system to get the partial information about Alice's secret. Suppose that the initial state of the ancillary system is $|0\rangle_B$ and Bob's dishonest action when he receives Alice's query state can be described by a unitary operator $\widetilde{U}_{AB}$ as follows:

$$\widetilde{U}_{AB}|0\rangle_A|0\rangle_B = \sqrt{\eta_0}|0\rangle_A|\phi_0\rangle_B + \sqrt{1-\eta_0}|V_0\rangle_{AB}, \tag{8}$$

$$\widetilde{U}_{AB}|k\rangle_A|0\rangle_B = \sqrt{\eta_k}|k\rangle_A|\phi_k\rangle_B + \sqrt{1-\eta_k}|V_k\rangle_{AB}, \tag{9}$$

$$\widetilde{U}_{AB}\left(\frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)_A |0\rangle_B = \sqrt{\eta_{+k}}\left(\frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)_A \left|\phi_{+k}\right\rangle_B + \sqrt{1-\eta_{+k}}\,|V_{+k}\rangle_{AB}, \tag{10}$$

where $|V_0\rangle_{AB}$, $|V_k\rangle_{AB}$ and $|V_{+k}\rangle_{AB}$ are the vector orthogonal to $|0\rangle_A|\phi_0\rangle_B$, $|k\rangle_A|\phi_k\rangle_B$ and $|+k\rangle_A\left|\phi_{+k}\right\rangle_B$ $\left(|+k = \frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)$, respectively, i.e.,

$$_A\langle 0|_B\,\langle\phi_0|V\rangle_{0\,AB} = 0, \tag{11}$$

$$_A\langle k|_B\,\langle\phi_k|V_k\rangle_{AB} = 0, \tag{12}$$

$$_A\langle +k|_B\left\langle\phi_{+k}\middle|V_{+k}\right\rangle_{AB} = 0. \tag{13}$$

In order to completely pass the honest test, we can easily deduce that the following condition holds in Eq. (10):

$$\eta_{+k} = 1. \tag{14}$$

That is,

$$\widetilde{U}_{AB}\left(\frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)_A |0\rangle_B = \left(\frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)_A \left|\phi_{+k}\right\rangle_B. \tag{15}$$

In addition, after applying the unitary operator $\widetilde{U}_{AB}$, in order to fully pass the honest test, the returned states cannot contain other vectors except the vectors of $|0\rangle_A$ and $|k\rangle_A$. So Eqs. (8) and (9) should be changed into the following equations, accordingly:

$$\widetilde{U}_{AB}|0\rangle_A|0\rangle_B = \sqrt{\eta_0}\,|0\rangle_A|\phi_0\rangle_B + \sqrt{1-\eta_0}\,|k\rangle_A|\phi_k\rangle_B, \tag{16}$$

$$\widetilde{U}_{AB}|k\rangle_A|0\rangle_B = \sqrt{\eta_k}\,|k\rangle_A|\phi_k\rangle_B + \sqrt{1-\eta_k}\,|0\rangle_A|\phi_0\rangle_B. \tag{17}$$

By Eq. (15), when $k = 0$, we further get

$$\widetilde{U}_{AB}|0\rangle_A|0\rangle_B = |0\rangle_A|\phi_0\rangle_B. \tag{18}$$

That is,

$$\eta_0 = 1. \tag{19}$$

In addition, we can get

$$\begin{aligned}
\widetilde{U}_{AB}|k\rangle_A|0\rangle_B &= \widetilde{U}_{AB}\left[\sqrt{2}\left(\frac{|k\rangle + |0\rangle - |0\rangle}{\sqrt{2}}\right)\right]_A |0\rangle_B \\
&= \widetilde{U}_{AB}[\sqrt{2}\,|+k\rangle - |0\rangle\,]_A|0\rangle_B \\
&= \sqrt{2}\,\widetilde{U}_{AB}|+k\rangle_A|0\rangle_B - \widetilde{U}_{AB}|0\rangle_A|0\rangle_B \\
&= \sqrt{2}\,|+k\rangle_A\left|\phi_{+k}\right\rangle_B - |0\rangle_A|\phi_0\rangle_B \quad \text{(by Eqs.(15) and (18))} \\
&= \sqrt{2}\left(\frac{|0 + |k}{\sqrt{2}}\right)_A \left|\phi_{+k}\right\rangle_B - |0\rangle_A|\phi_0\rangle_B \\
&= |0\rangle_A\left|\phi_{+k}\right\rangle_B + |k\rangle_A\left|\phi_{+k}\right\rangle_B - |0\rangle_A|\phi_0\rangle_B.
\end{aligned} \tag{20}$$

If we compute the scalar product between Eqs. (17) and (20), then we will obtain the identity

$$\begin{aligned}
1 &= \sqrt{1-\eta_k}_B\left\langle\phi_0\middle|\phi_{+k}\right\rangle_B + \sqrt{\eta_k}_B\left\langle\phi_k\middle|\phi_{+k}\right\rangle_B - \sqrt{1-\eta_k}_B\langle\phi_0|\phi_0\rangle_B \\
&= \sqrt{1-\eta_k}_B\left\langle\phi_0\middle|\phi_{+k}\right\rangle_B + \sqrt{\eta_k}_B\left\langle\phi_k\middle|\phi_{+k}\right\rangle_B - \sqrt{1-\eta_k}.
\end{aligned} \tag{21}$$

Since ${}_B\langle\phi_0|\phi_{+k}\rangle_B \leq 1$ and ${}_B\langle\phi_k|\phi_{+k}\rangle_B \leq 1 \leq 1$, so we get

$$1 \leq \sqrt{1-\eta_k} + \sqrt{\eta_k} - \sqrt{1-\eta_k}. \tag{22}$$

That is,

$$1 \leq \sqrt{\eta_k}, \tag{23}$$

which implies

$$\eta_k = 1. \tag{24}$$

Thus, we can obtain the following expanded expression

$$\begin{aligned}\widetilde{U}_{AB}\left(\frac{|0\rangle + |k\rangle}{\sqrt{2}}\right)_A |0\rangle_B &= \frac{\widetilde{U}_{AB}|0\rangle_A|0\rangle_B + \widetilde{U}_{AB}|k\rangle_A|0\rangle_B}{\sqrt{2}} \\ &= \frac{|0\rangle_A|\phi_0\rangle_B + |k\rangle_A|\phi_k\rangle_B}{\sqrt{2}}.\end{aligned} \tag{25}$$

Similarly, if we compute the scalar product between Eqs. (15) and (25), then we will obtain

$$1 = \frac{1}{2}{}_B\langle\phi_0|\phi_{+k}\rangle_B + \frac{1}{2}{}_B\langle\phi_k|\phi_{+k}\rangle_B. \tag{26}$$

By Eq. (26), it gives

$${}_B\langle\phi_0|\phi_{+k}\rangle_B = 1, \tag{27}$$

$${}_B\langle\phi_k|\phi_{+k}\rangle_B = 1. \tag{28}$$

From Eqs. (27) and (28), it shows that if Bob wants to be sure that he passes the honest test, then the final states of the ancillary system B for any choice of k will coincide with $|\phi_0\rangle_B$, that is, the states of the ancillary system B are independent from the secret k. Therefore, even though Bob performs an entangle-measure attack, he will not obtain any secret information about the secret k.

In addition, **Bob's privacy** is guaranteed by the encoding and encrypting methods discussed above. If Alice honestly executes this protocol, she cannot obtain any secret information about Bob's private set. If Alice is dishonest, the simplest attack for her is to send a false query state $\frac{|j\rangle+|k\rangle}{\sqrt{2}}$ to Bob, instead of the true query state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$. Then the corresponding state returned from Bob will be in $\frac{\pm(-1)^{f^*(j)}|j\rangle \pm (-1)^{f^*(k)}|k\rangle}{\sqrt{2}}$ (i.e., $\frac{|j\rangle \pm |k\rangle}{\sqrt{2}}$). From the returned state, Alice can only infer that $f^*(j) = f^*(k)$ or $f^*(j) \neq f^*(k)$, but she cannot further deduce whether j or k belongs to Bob's private set because she does not know the values of $f^*(j)$ and $f^*(k)$. Furthermore, for more general case, Alice sends a more general sate $\frac{1}{\sqrt{N}}\sum|x\rangle$ to Bob, instead of the true query state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$. Accordingly, the returned state will be in $\frac{1}{\sqrt{N}}\Sigma \pm (-1)^{f^*(x)}|x\rangle$, where $f^*(x) \in \{0, 1\}$. Obviously, Alice cannot extract out the phase information $f^*(x)$ of single basis state $|x\rangle$ from the returned state, though she can approximatively count the number of the members in Bob's private set. However, if Alice sends a false query state, she will run a risk with the probability of $\frac{1}{2}$ that she cannot gain $p(k)$ rightly, which further affects Bob's right output. That is, Bob cannot rightly make a decision of the set-member relation without the right phase information $p(k)$. For example, in anonymous authentication applications, If Alice can prove that her secret is a member of Bob's private set (but which member is unknown) by Protocol I, then Bob will believe that Alice is an authorized user and further open the corresponding resources or provide services to Alice. But, if Alice sends a false query state, the verification will fail with the probability of $\frac{1}{2}$.

Protocol II. When Alice and Bob honestly execute this protocol, the **correctness** is guaranteed by the asymmetric key shared between Alice and Bob, whose security is based on the security of Quantum key Distribution[18–20].

In Protocol II, Alice only sends the classical messages s and $s(k)$ to Bob except checking information. Clearly, Bob cannot get any secret information about Alice's secret only from these messages except knowing whether it is a member of his private set. That is, it guarantees **Alice's privacy**. Furthermore, **Alice's anonymity** depends on the security of the asymmetric key[13,15]. When creating the asymmetric key, if Bob is dishonest, he can perform the following two attacks: one is to send other states (e.g., $|\nearrow\rangle$)

	Classical resources	Quantum resources	Oracle operation	Quantum measurement	Communication Complexity	Computation Complexity	Round
Protocol I	1 bit	$O(\log N)$ qubits	*Y*	*VNM_N*	$O(\log N)$	$O(1)$	$O(1)$
Protocol II	$O(N)$bits	$O(N)$qubits	*N*	*SPM_2*	$O(N)$	$O(N)$	$O(1)$

Table 1. Comparison of two proposed protocols. Note: *Y*, *N*, *VNM_N* and *SPM_2* denote Yes, No, von Neumann Measurement in *N*-dimensional Hilbert space and simple Projective Measurement in 2-dimensional Hilbert space, respectively.

than he announces (e.g., $\{|\uparrow\rangle, |\rightarrow\rangle\}$), and the other is to perform an entangle-measure attack, that is, he prepares a state of two qubits $\frac{1}{\sqrt{2}}(|\uparrow\rangle_A|R_0\rangle_B + |\rightarrow\rangle_A|R_1\rangle_B)$, where the first qubit is sent to Alice and the second is kept in Bob's register, and afterwards he will measure the state in his register to gain some information on the conclusiveness of Alice's measurement. However, as analyzed in refs 13,15 these attacks will introduce bit errors. That is, if Bob gains information on the conclusiveness of Alice's bits, he will lose information on the bit values she has recorded. In fact, it is impossible for Bob to have both the correct bit value and conclusiveness information of Alice's measurement (i.e., the address of the correct basis). Therefore, Bob cannot simultaneously obtain the bit $K(j)$, which is the correctly measured result of Alice, and the corresponding address *j*. In our proposed Protocol II, in order to check Bob's honesty, Alice will compare $q-1$ measurement results with these corresponding bits that Bob's announces. Thus, for a dishonest Bob, the success probability to completely pass the honest test in Step 2 of Protocol II is not more than $\frac{1}{2^{(q-1)}}$.

We further analyze **Bob's privacy**. On the one hand, if Alice is dishonest and she wants to obtain more items (i.e., $s(j)$s) in Bob's private database, she has to try to obtain more bits of the shared key. As analyzed in refs 13,15 it is possible for a dishonest Alice to store the qubits received from Bob and then take more effective measurements (e.g., the optimal unambiguous state discrimination (USD) measurement) on them after getting Bob's public information. Even so, the advantage Alice obtains by USD measurement is negligible compared with the honest measurement[13,15]. On the other hand, though a dishonest Alice can theoretically get more than one $s(j)$, she doesn't yet know any $p(j)$ rightly since $p(j) = s(j) + r$ and *r* is unknown. By these $s(j)$s, she can only decide that these indexes can be roughly classified into at most two categories: one belongs to Bob' private set and the other doesn't belong to it. But she cannot decide which category belongs to Bob's private set.

We have analyzed the security of proposed protocols. However, please note that we mainly consider the honest-but-curious parties[21] in our protocols, which is similar to the semi-honesty model in the classical settings. In classical settings, any secure protocol in semi-honesty model can be correspondingly translated into a secure protocol in malicious model. However, it still needs to further study how to translate a protocol from semi-honesty model to malicious model in quantum settings. It is also our future work (especially, the definition of malicious model in quantum settings).

Performance Comparisons. Here, we give a simple comparison of our proposed protocols with the related QPQ protocols. In Protocol I, we follow some ideas from QPQ in refs 10,12 to introduce two quantum oracles. However, compared to these related QPQ protocols, the oracles proposed in Protocol I are more specific and more elaborated, where one is for encoding, and the other is for encrypting. In Protocol II, we are inspired by the asymmetric key of QPQ in refs 13,15,16. However, compared to these related QPQ protocols, there are at least two good advantages of Protocol II: (1) When creating the asymmetric key, Alice knows some bits of the raw key, not just one. On the one hand, it is easier to control and create the raw key with the present technology. On the other hand, Alice can check the honesty of Bob by using the remaining bits among these known bits except one bit as the final key. (2) Bob cleverly creates a 0/1 database and further encrypts it twice by using different keys, thus it is more secure. Even if Alice knows more than one bit of the final asymmetric key, she also only knows the corresponding encrypted items.

Furthermore, we evaluate the performance of the proposed protocols, as listed in Table 1. In Protocol I, we introduce two powerful quantum oracle operations. In fact, the main operations of Protocol I are just the two oracle operations. In addition, Protocol I is a 3-round protocol obviously, which consumes $\log N$ qubits quantum resource and 1 bit classical resource, and further performs a von Neumann measurement in *N*-dimensional Hilbert space. Thus, Protocol I needs only $O(1)$ computation costs and $O(\log N)$ communication costs. For Protocol II, though its round is more than 3, it is also constant, irrespective of *k*, *n* and *N*. In Protocol 2, obviously it consumes $O(N)$ qubits to create the asymmetric key between Alice and Bob, and $O(N)$ bits to store the classical database for Bob. In addition, Alice performs $O(N)$ projective measurements in 2-dimensional Hilbert space and Bob computes $O(N)$ encryptions of one-time pad. So, Protocol II needs $O(N)$ costs in both communication and computation complexity.

Discussion

In this paper, we first defined Oblivious Set-member Decision problem and further proposed two constant round quantum protocols to solve the Oblivious Set-member Decision problem, where Protocol I has better advantages in term of communication and computation complexity due to powerful quantum oracle operations, while Protocol II takes photons as quantum resources and performs single-photon projective measurements, and thus it is more feasible with the present technology, that is, it is easier to implement it.

References

1. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. *35th Annual Symposium on the Foundations of Computer Science*, Santa Fe, NM, 124–134 (IEEE, New York, doi: 10.1109/SFCS.1994.365700, 1994).
2. Grover, L. K. A fast quantum mechanical algorithm for database search. In Proc. *28th Annual ACM Symposium on Theory of Computing (STOC'96)*, Philadelphia PA, 212–219 (ACM, New York, doi: 10.1145/237814.237866, 1996).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum Cryptography. *Rev. Mod. Phys.* **74,** 145 (2002).
4. Nadeem, M. Unconditionally secure commitment in position-based cryptography. *Sci. Rep.* **4,** 6774 (2014).
5. Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proc. *IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, (IEEE, New York), 175–179 (1984).
6. Dixon, A. R. & Sato, H. High speed and adaptable error correction for megabit/s rate quantum key distribution. *Sci. Rep.* **4,** 7275 (2014).
7. Sun, Y., Song, X., Qin, H., Zhang, X., Yang, Z. & Zhang, X. Non-local classical optical correlation and implementing analogy of quantum teleportation. *Sci. Rep.* **5,** 9175 (2015).
8. Wang, T. Y., Cai, X. Q., Ren, Y. L. & Zhang, R. L. Security of quantum digital signatures for classical messages. *Sci. Rep.* **5,** 9231 (2015).
9. Sheng, Y. B. & Zhou, L. Deterministic entanglement distillation for secure double-server blind quantum computation. *Sci. Rep.* **5,** 7815 (2015).
10. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **100,** 230502 (2008).
11. Giovannetti, V., Lloyd, S. & Maccone, L. Quantum Private Queries: security analysis. *IEEE T. Inform. Theory* **56,** 3465–3477 (2010).
12. Olejnik, L. Secure quantum private information retrieval using phase-encoded queries. *Phys. Rev. A* **84,** 022313 (2011).
13. Jakobi, M. *et al.* Practical private database queries based on a quantum key distribution protocol. *Phys. Rev. A* **83,** 022301 (2011).
14. Scarani, V., Acín, A., Ribordy, G. & Gisin, N. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys Rev Lett* **92,** 057901 (2004).
15. Gao, F., Liu, B. & Wen, Q. Y. Flexible quantum private queries based on quantum key distribution. *Opt Exp* **20,** 17411 (2012).
16. Yang, Y. G., Sun, S. J., Xu, P. & Tian, J. Flexible protocol for quantum private query based on B92 protocol. *Quantum Inf Process* **13,** 805–813 (2014).
17. Wu, M. E., Chang, S. Y., Lu, C. J & Sun, H. M. A communication-efficient private matching scheme in Client-Server model. *Inform. Sci.* **275** (2014) 348–359.
18. Biham, E., Boyer, M., Boykin, P. O., Mor, T. & Roychowdhury, V. A proof of the security of quantum key distribution. *J. Cryptology* **19,** 381–439 (2006).
19. Leverrier, A. & Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution. *Phys. Rev. Lett.* **102,** 180504 (2009).
20. Lu, H., Fung, C. H. F., Ma, X. F. & Cai, Q. Y. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A* **84,** 042344 (2011).
21. Baumeler, Ä. & Broadbent, A. Quantum Private Information Retrieval has linear communication complexity. *arXiv*, 1304.5490v2 (2014).

Acknowledgements

This work was supported by National Natural Science Foundation of China (Nos 61173187, 61173188 and 11301002), the Ministry of Education institution of higher learning doctor discipline and scientific research fund aids a project financially (No. 20133401110004), Natural Science Foundation of Anhui Province (No. 1408085QF107), and the 211 Project of Anhui University (Nos 33190187 and 17110099).

Author Contributions

Study conception, design, and writing of the manuscript: S.R.H. and M.Y. Analysis and discussion: Z.H., C.J. and Z.S. All authors reviewed the manuscript.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Shi, R.-h. *et al.* Two Quantum Protocols for Oblivious Set-member Decision Problem. *Sci. Rep.* **5**, 15914; doi: 10.1038/srep15914 (2015).