International Journal of Theoretical Physics (2019) 58:4249–4257
https://doi.org/10.1007/s10773-019-04296-0

Strong Privacy-preserving Two-party Scalar Product Quantum Protocol

Run-hua Shi [1,2] · Mingwu Zhang [1]

Received: 19 April 2019 / Accepted: 21 September 2019/ Published online: 8 November 2019

Abstract
Under the assumption that the parties do not change their private inputs during the whole protocol execution, we present a probabilistic quantum protocol for secure two-party scalar product without the help of any third party, which can ensure the security of the strong privacy of two parties. Especially, the communication complexity of this protocol achieves $O(1)$, and thus it is more suitable for applications with big data.

Keywords Quantum Cryptography · Privacy-Preserving · Multi-party Secure Computation · Scalar Product

1 Introduction

With the advent of fast quantum algorithms [1, 2], quantum computations and quantum communications have received extensive attention and gained lots of promising achievements, such as quantum cryptography [3], quantum teleportation [4] and quantum secret sharing [5]. However, in 1997, Lo [6] pointed unconditional secure one-sided two-party computation is impossible. Later in 2007, Colbeck [7] further showed that unconditional secure two-sided two-party computation is impossible yet. Recently, Buhrman *et al*. [8] systematically proved that unconditional secure classical two-party computation is impossible.

Furthermore, the research results show that quantum protocols still can provide a higher security than the corresponding classical protocols, e.g., quantum protocols for Oblivious Set-

✉ Mingwu Zhang
mzhang@hbut.edu.cn

Run-hua Shi
rhshi@ncepu.edu.cn

[1] School of Computer Science, Hubei University of Technology, Wuhan City 430068, China

[2] School of Control and Computer Engineering, North China Electric Power University, Beijing City 102206, China

member Decision [9] and Private Set Intersection Cardinality [10]. Therefore, how to construct and implement quantum protocols for special two-party classical computations has always been the research focus in recent years.

Secure scalar product is an important primitive of secure multi-party computation, which can usually be used as a building block for many complicated cryptographic protocols, such as private comparison, secret sharing, secure function evaluation, privacy-preserving computational geometry, etc. Let Alice has a vector $\boldsymbol{X} = (x_1, x_2, \ldots, x_m)$ and Bob has a vector $\boldsymbol{Y} = (y_1, y_2, \ldots, y_m)$, where all components belong to the set Z_N. The scalar product protocol is to securely compute the scalar (dot) product of $\boldsymbol{X}$ and $\boldsymbol{Y}$, given by $\boldsymbol{X} \cdot \boldsymbol{Y} = \sum_{i=1}^{m} x_i y_i mod\ N$.

He *et al*. [11] proposed the first quantum protocol for the secure scalar product via quantum entanglements and quantum measurements. Their protocol needs a non-colluding third party. Recently, Wang *et al*. [12] presented a new quantum approach to compute secure scalar product between two parties with continuous-variable clusters. Wang's protocol does not need any third party. However, both He's protocol and Wang's protocol need to cost too many redundant qubits and perform lots of measurements to ensure the security. In this paper, we present a novel quantum protocol for secure two-party scalar product without the help of any third party. Compared with the previously proposed quantum protocols, our protocol obtains the lower communication complexity and the lower measurement complexity.

In addition, since unconditionally secure (or perfect) two-party quantum computations are impossible in theory, some researchers further consider the honest-but-curious model in two-party quantum computations [13–15], which is similar to the semi-honesty model in the classical settings. That is, the parties honestly execute the protocol, but they try to find out as much as possible about the other inputs despite following the protocol. In this paper, we consider a stronger model than the honest-but-curious model, that is, we only assume that the parties do not change their private inputs during the whole protocol execution, but they can perform any other malicious actions, including dishonestly executing the protocol, in order to steal the other's private information.

2 Quantum scalar product protocol

Under the assumption that two parties do not change their respective private inputs during the whole protocol execution, we give a definition of a one-sided two-party scalar product protocol with strong (not perfect) privacy protections, later called strong privacy-preserving two-party scalar product protocol.

Definition 1 Strong privacy-preserving two-party scalar product (SP2P-SP) protocol - There are two parties, usually called Alice and Bob. Alice inputs a private vector $\boldsymbol{X} = (x_1, x_2, \ldots, x_m)$ and Bob inputs a private vector $\boldsymbol{Y} = (y_1, y_2, \ldots, y_m)$. After running a SP2P-SP protocol, Bob outputs the scalar product of $\boldsymbol{X}$ and $\boldsymbol{Y}$, i.e., $\sum_{i=1}^{m} x_i y_i mod\ N$, but Alice gets nothing. In addition, SP2P-SP protocol should meet the following strong privacy requirements:

> ***Alice's Privacy.*** The information about Alice's private vector $\boldsymbol{X}$ obtained by a dishonest Bob is less than or equal to the possible information inferred from his private vector $\boldsymbol{Y}$ and the final scalar product, $\sum_{i=1}^{m} x_i y_i mod\ N$ (strong privacy).

Bob's Privacy. Alice cannot get any secret information about Bob's private vector $\boldsymbol{Y}$ (perfect privacy).

In the following protocol, suppose that two parties' private vectors are $\boldsymbol{X}=(x_0, x_1, \ldots, x_{N-1})$ and $=(y_0, y_1, \ldots, y_{N-1})$, respectively, and all components belong to the set Z_N, where $N=2^n$. This assumption is reasonable, because we can let $x_m = x_{m+1} \ldots = x_{N-1} = 0$ and $y_m = y_{m+1} \ldots = y_{N-1} = 0$, if $m < N$. In addition, we further assume that two private vectors cannot be altered during the whole protocol execution.

2.1 Quantum SP2P-SP protocol

Step 1. Alice first hides her private vector $\boldsymbol{X}=(x_0, x_1, \ldots, x_{N-1})$ by secret splitting ideas as follows: Alice generates two auxiliary vectors $\boldsymbol{X_1}=(x_{1,0}, x_{j,i}, \ldots, x_{1,N-1})$ and $\boldsymbol{X_2}=(x_{2,0}, x_{2,1}, \ldots, x_{2,N-1})$ over Z_N randomly, such that $\boldsymbol{X}=(\boldsymbol{X_1}+\boldsymbol{X_2})modN$, i.e., $x_i=(x_{j,i}+x_{2,i})modN$ for any i. Then Alice prepares two quantum states, which are initially in $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle$. Furthermore, Alice applies two oracle operators U_{X_1} and U_{X_2} to two initial states, respectively, where the oracle operator U_{X_j} $(j=1, 2)$ is defined by

$$U_{X_j}: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\otimes|0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|0\otimes x_{j,i}\rangle \tag{1}$$

Let $|\psi_{A_j}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{j,i}\rangle$ for $j=1, 2$. Finally Alice sends $|\psi_{A_1}\rangle$ and $|\psi_{A_2}\rangle$ to Bob though the quantum channel.

Step 2. After receiving two quantum states sent by Alice, Bob first applies a similar oracle operator U_Y to each quantum state $|\psi_{A_j}\rangle$ $(j=1, 2)$, where U_Y is defined by,

$$U_Y: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{j,i}\rangle\otimes|0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|0\otimes y_i\rangle. \tag{2}$$

Let $|\psi_{B_j}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle$ for $j=1, 2$. Then Bob performs another oracle operator U_f to each quantum state $|\psi_{B_j}\rangle$ $(j=1, 2)$, where U_f is defined by,

$$U_f: \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle\otimes|0\rangle \rightarrow \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|0\otimes f\left(x_{j,i}, y_i\right)\rangle, \tag{3}$$

with $f(x_{j,i}, y_i) = x_{j,i}\cdot y_i$. That is,

$$U_f|\psi_{B_j}\rangle\otimes|0\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}.y_i\rangle. \tag{4}$$

Let $|\phi_{B_j}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}\,.\,y_i\rangle$ for $j=1, 2$.

Step 3. For each $|\phi_{B_j}\rangle$, Bob further prepares two auxiliary quantum states, which are initially in $\frac{1}{\sqrt{N'}}\sum_{k=0}^{N'-1}|k\rangle$ and $|0\rangle$. Here, we assume that $N' > N^2$, $n' = \log N'$ and $n = \log N$.

Furthermore, Bob performs an oracle quantum operator U_{f^*} on each quantum system $|\phi_{B_j}\rangle \otimes \frac{1}{\sqrt{N'}}\sum_{k=0}^{N'-1}|k\rangle \otimes |0\rangle$ $(j = 1, 2)$, where U_{f^*} is defined by,

$$\begin{aligned} U_{f^*}\left|\phi_{B_j}\right\rangle \otimes \frac{1}{\sqrt{N'}}\sum_{k=0}^{N'-1}|k\rangle \otimes |0\rangle &= U_{f^*}\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}\cdot y_i\rangle \otimes \frac{1}{\sqrt{N'}}\sum_{k=0}^{N'-1}|k\rangle \otimes |0\rangle \\ &= \frac{1}{\sqrt{NN'}}\sum_{i=0}^{N-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}\cdot y_i\rangle\sum_{k=0}^{N'-1}|k\rangle|0 \otimes f^*\left(i, x_{j,i}\cdot y_i, k\right)\rangle \\ &= \frac{1}{\sqrt{NN'}}\sum_{i=0}^{N-1}\sum_{k=0}^{N'-1}\left\{|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}\cdot y_i\rangle|k\rangle|f^*\left(i, x_{j,i}\cdot y_i, k\right)\rangle\right\}, \end{aligned} \tag{5}$$

with

$$f^*\left(i, x_{j,i}\cdot y_i, k\right) = \begin{cases} 1 & if\ \ x_{j,i}\cdot y_i > k \\ 0 & otherwise \end{cases}. \tag{6}$$

Step 4. For $j = 1, 2$, by using quantum counting algorithm [16–18], Bob counts the number t_j of the components satisfying $f^*(i, x_{j,\,i}\cdot y_i, k) = 1$ of the quantum state in Eq. 5, respectively. That is, Bob executing the following procedures:

For $j = 1$ to 2

{ Prepare two registers in the initial state $|R_0\rangle = \frac{1}{\sqrt{M}}\sum_{t=0}^{M-1}|t\rangle \otimes |\varphi_j\rangle$, where the state $|\varphi_j\rangle$ is in,

$$|\varphi_j\rangle = \frac{1}{\sqrt{NN'}}\sum_{i=0}^{N-1}\sum_{k=0}^{N'-1}|i\rangle\left|x_{j,i}\right\rangle|y_i\rangle|x_{j,i}\cdot y_i\rangle|k\rangle|f^*\left(i, x_{j,i}\cdot y_i, k\right)\rangle. \tag{7}$$

Apply C_F on $|R_0\rangle$, which implements $|t\rangle \otimes |\varphi_j\rangle \rightarrow |t\rangle \otimes G^t|\varphi_j\rangle$, where G is the Grover iteration [18] defined by (Fig. 1)

$$G = U_{\varphi_j}U_{f_\omega}, \tag{8}$$

$$|\omega\rangle = |i\rangle|x_{j,i}\rangle|y_i\rangle|x_{j,i}.y_i\rangle|k\rangle\left|f^*\left(i, x_{j,i}\cdot y_i, k\right)\right\rangle \tag{9}$$

$$U_{f_\omega}|\omega\rangle = \begin{cases} -|\omega\rangle & if\ \ f^*\left(i, x_{j,i}\cdot y_i, k\right) = 1 \\ |\omega\rangle & if\ \ f^*\left(i, x_{j,i}\cdot y_i, k\right) = 0 \end{cases}, \tag{10}$$

$$U_{\varphi_j} = 2|\varphi_j\rangle\langle\varphi_j| - I. \tag{11}$$

Similarly, call the resultant state $|R_1\rangle$.

Apply QFT^{-1} on the first register of $|R_1\rangle$. Call the resultant state $|R_2\rangle$.

Measure the first register of $|R_2\rangle$ to obtain $|T_j\rangle$ and compute $t_j = NN' sin^2\left(\frac{T_j}{M}\pi\right)$. }

Finally, Bob outputs $t = (t_1 + t_2) mod N$, i.e., an estimator of the scalar product of $\boldsymbol{X}$ and $\boldsymbol{Y}$ (Fig. 1).

3 Analysis

Correctness Given from Step 1 of the proposed protocol, $\boldsymbol{X} = \boldsymbol{X_1} + \boldsymbol{X_2}$(i.e., $x_i = x_{j,i} + x_{2,i}$ for any i), so $\sum_{i=0}^{N-1} x_{1,i} y_i mod\, N + \sum_{i=0}^{N-1} x_{2,i} y_i mod\, N = \sum_{i=0}^{N-1} x_i y_i mod\, N$, obviously. By Eq.(7) (or Eq.(5)), there are NN' components in the quantum state $|\varphi_j\rangle$, where $x_{j,i} y_i < N^2 < N'$. Furthermore, by the definition of f^* in Eq.(6), we can see that for each i, there are just $x_{j,i} y_i$ ks (i.e, k from 0 to $x_{j,i} y_i - 1$) among all N' ks (i.e, k from 0 to $N' - 1$) satisfying $f^*(i, x_{j,i} \cdot y_i, k) = 1$. So, there are $\sum_{i=0}^{N-1} x_{j,i} y_i mod\, N$ components in the quantum state $|\varphi_j\rangle$ in total, such that $f^*(i, x_{j,i} \cdot y_i, k) = 1$, and further the number of the components satisfying $f^*(i, x_{j,i} \cdot y_i, k) = 1$ will be estimated by Bob using quantum counting algorithm in Step 4. Accordingly, the final output, t (i.e., $t_1 + t_2$), is a right estimator of the scalar product of $\boldsymbol{X}$ and $\boldsymbol{Y}$.

Therefore, two parties honestly executing the protocol can ensure its correctness.

Alice's Privacy. In the proposed quantum SP2P-SP protocol, Alice only sends out two quantum states: $|\psi_{A_1}\rangle$ and $|\psi_{A_2}\rangle$ without any classical message, where $|\psi_{A_j}\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle$ for $j = 1, 2$. Although all classical information about her private vectors is embedded into the two states, no one can extract all this information by the basic principles of quantum mechanics. For a dishonest Bob, he can try to extract Alice's partial private information from the received states by the following possible attacks.

The first attack is to directly make a projective measurement on the received states $|\psi_{A_j}\rangle$s to steal Alice's private information.

On the one hand, if the dishonest Bob makes a projective measurement on one of the received states, e.g., $|\psi_{A_1}\rangle$, where $|\psi_{A_1}\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle |x_{j,i}\rangle$. Accordingly, he will get $|i\rangle \mid x_{1,i}\rangle$ for any i with the probability of $\frac{1}{N}$. Then the system A sent by Alice can be characterized by the quantum ensemble, $\mathcal{E} \equiv \{p_i, \rho_A(i)\}$, where p_i (i.e., $p_i = \frac{1}{N}$) is the probability of getting the measured result $(i, x_{1,i})$, and

$$\rho_A(i) = |i, x_{1,i}\rangle \langle i, x_{1,i}|. \tag{12}$$

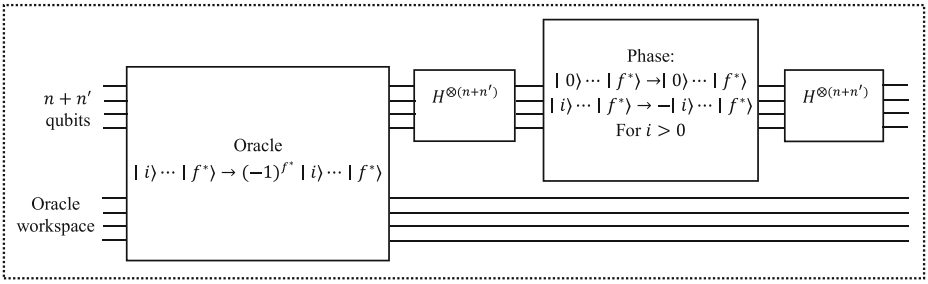

Fig. 1 Circuit for the iteration G in Step 4

Holevo's theorem [19] tells us that the accessible information available to the outsider by any measurement on ρ_A is bounded by the entropy

$$\begin{aligned} I \le \mathcal{X}(\varepsilon) &= S(\rho_A) - \frac{1}{N}\sum_{i=0}^{N-1} S(\rho_A(i)) \\ &\le \frac{1}{N}\sum_{i=0}^{N-1} S(\rho_A(i)) + H(P) \\ &= H(P), \end{aligned} \tag{13}$$

where $\rho_A = \sum_{i=0}^{N-1}\rho_A(i)/N$ is the average state of A. So $I \le n$. That is, Bob can extract at most n bits classical information from the received state by any possible local measurement.

On the other hand, if Bob makes a projective measurement on the state $|\psi_{A_j}\rangle$ (i.e., $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{j,i}\rangle$). Accordingly, he will get $x_{j,\,i}$ (n bits) for any i with the probability of $\frac{1}{N}$. However, he cannot get the ith component of Alice's private vector (i.e., x_i), only from a single measured result $x_{1,\,i}$ or $x_{2,\,i}$, not $x_{1,\,i}$ and $x_{2,\,i}$, due to $x_i = x_{1,\,i} + x_{2,\,i}$. Even if Bob measures both two received states $|\psi_{A_1}\rangle$ and $|\psi_{A_2}\rangle$, he will randomly get $x_{1,\,i}$ and x_{2,i^*}, respectively. By the randomness of the measurements, i and i^* are two random numbers, where the probability of satisfying $i = i^*$ is only $\frac{1}{N}$. Accordingly, the probability that Bob successfully gets a right component x_i by this attack is also $\frac{1}{N}$, which is equal to that of randomly guessing it. In addition, if Bob performs this attack, he will lose the chance to further compute the final scalar product, due to No-cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state.

The second attack is to count the number of $x_{j,\,i} \in (x_{j,\,0}, x_{j,i}, \ldots, x_{j,\,N-1})$ on $|\psi_{A_j}\rangle$ by quantum counting algorithm, such that $x_{j,\,i}$ satisfies certain feature, e.g., it is equal to a specific number. That is, it is to analyze certain statistics feature of Alice's auxiliary private vector. However, Bob cannot further get any secret information about Alice's original private vector from these statistics features because two auxiliary vectors are randomly generated by Alice.

In addition, the dishonest Bob still can perform a more complicated attack that he tries to compute the summation of both received quantum states by the help of a powerful oracle operator, since he knows that Alice uses the classical secret splitting technology to hide her private vector. Suppose that there is an oracle operator O, which is defined by,

$$O : |l_1\rangle \otimes |l_2\rangle \otimes |0\rangle \rightarrow |l_1\rangle \otimes |l_2\rangle \otimes |l_1 + l_2\rangle, \tag{14}$$

for any $l_j \in Z_N$. Then, after applying the oracle operator O on both received quantum states, the dishonest Bob will get,

$$\begin{aligned} & O\left[\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{1,i}\rangle \otimes \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{2,i}\rangle \otimes |0\rangle\right] \\ &= \frac{1}{N}\sum_{i_1,i_2}|i_1\rangle|i_2\rangle|x_{1,i_1}\rangle|x_{2,i_2}\rangle|x_{1,i_1} + x_{2,i_2}\rangle. \end{aligned} \tag{15}$$

In Eq. 14, if $i_1 = i_2 = i$, then $x_{1,i_1} + x_{2,i_2} = x_i$. However, due to the randomness of the measurement, the probability of extracting a private component of Alice's private vector (i.e., x_i) from the final quantum state in Eq.14 is also $\frac{1}{N}$.

What's more, suppose that the dishonest Bob can perform the following more stronger attack:

$$O'\left[\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{1,i}\rangle\otimes\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{2,i}\rangle\otimes|0\rangle\right] = \frac{1}{N}\sum_{i_1,i_2}|i_1\rangle|i_2\rangle|x_{1,i_1}\rangle|x_{2,i_2}\rangle|f(i_1,i_2)(x_{1,i_1}+x_{2,i_2})\rangle, \tag{16}$$

with

$$f(i_1,i_2)=\begin{cases}1 & if\ \ i_1=i_2\\ 0 & otherwise\end{cases}. \tag{17}$$

Furthermore, if Bob measures the final register (i.e., $|f(i_1,i_2)(x_{1,i_1}+x_{2,i_2})\rangle$) on the computational basis, then he will get one component x_i of Alice's private vector with the same probability of $1/N$ (i.e., $i=i_1=i_2$ and accordingly $x_i=x_{1,\,i}+x_{2,\,i}$) and get nothing with the probability of $1-1/N$.

In fact, if let $y_i=1$ and $y_j=0$ for all other js ($j\neq i$), then the dishonest Bob can always get the component x_i from the final computation result, since $\sum_{i=1}^{m}x_iy_i mod\ N=x_i$. Therefore, the information about Alice's private vector $\boldsymbol{X}$ obtained by a dishonest Bob is less than or equal to the possible information inferred from his private vector $\boldsymbol{Y}$ and the final scalar product, $\sum_{i=1}^{m}x_iy_i mod\ N$ (strong privacy).

In a word, Bob or an outside attacker can get at most one component (e.g., x_i) of Alice's private vector at the probability of $1/N$. If Alice splits her private vector $\boldsymbol{X}$ into m vectors, instead of two vectors, such that $\boldsymbol{X}=\boldsymbol{X}_1+\boldsymbol{X}_2+\ldots\boldsymbol{X}_m$, the probability of getting one component by Bob or any attacker will be reduced to $1/N^{m-1}$.That is, secret splitting (or sharing) can ensure Alice's privacy well.

Bob's Privacy. A dishonest Alice may try to learn about Bob's private vector by an entanglement-type of attack. i.e., she prepares an entangled state $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|\xi^A(i)\rangle|i\rangle|x_{j,i}\rangle$ instead of the initial state $\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{j,i}\rangle$, where she holds the first subsystem $|\xi^A(i)\rangle$ and sends the other subsystems to Bob. After Step 2, the whole quantum system will be in the following state,

$$\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|\xi^A(i)\rangle|i\rangle|x_{j,i}\rangle|y_i\rangle. \tag{18}$$

However, for different y_is, the reduced density matrixes of the subsystem held by Alice are same. e.g., suppose that the whole quantum system is in the state $|\psi_1\rangle=\frac{|0^A000\rangle+|1^A111\rangle}{\sqrt{2}}$ or $|\psi_2\rangle=\frac{|0^A001\rangle+|1^A110\rangle}{\sqrt{2}}$. Accordingly, the reduced density matrix of Alice is $\rho_1^A=Tr_B|\psi_1\rangle\langle\psi_1|=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)=\frac{I}{2}$ or $\rho_2^A=Tr_B|\psi_2\rangle\langle\psi_2|=\frac{1}{2}(|0\rangle\langle 0|+|1\rangle\langle 1|)=\frac{I}{2}$. i.e., $\rho_1^A=\rho_2^A$. Therefore, even if the dishonest Alice performs this attack, she still cannot distinguish or get any Bob's private information by measuring the subsystem held by herself because the reduced density matrix of the subsystem held by Alice is the completely (or maximally) mixed state.

In addition, Bob does not send out any quantum or classical message to Alice. So Alice cannot get any private information about Bob's private vector $\boldsymbol{Y}$ by no-signaling principle. That is, Bob's Privacy is unconditionally secure.

Performance. In our protocol, it only needs Alice to transmit two quantum messages $|\psi_{A_1}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{1,i}\rangle$ and $|\psi_{A_2}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle|x_{2,i}\rangle$ to Bob without any classical message. So the communication complexity of our protocol is $O(1)$, which achieves an exponential reduction, compared with corresponding classical protocols. In Step 4 of our protocol, it only needs to perform quantum measurements twice. That is, the measurement complexity of our protocol is also $O(1)$. Therefore, our protocol obtains lower communication and measurement complexities, compared with the related quantum protocols [11, 12].

Finally, to make our protocol work, the key step is to construct the efficient circuits implementing the oracle operators. In our protocol, we define four kinds of oracle operators. Similarly, using the techniques of reversible computation [20], we can construct a classical reversible circuit which takes (x, y) - representing an input register initially set to x and a one bit output register initially set to y - to $(x, y \otimes f(x))$, by modifying the usual (irreversible) classical circuit for doing the classical function $f(x)$.

4 Conclusion

In this paper, we present a strong privacy-preserving quantum protocol for secure two-party scalar product. The proposed protocol shows that although unconditionally secure two-party quantum computations are impossible in theory, probabilistic two-party quantum computation with strong privacy protections is possible, which is similar to the probabilistic clone of unknown quantum state. Furthermore, the proposed protocol achieves the communication (measurement) complexity of $O(1)$, and thus it is more suitable for applications with big data. In addition, our approach can be generalized theoretically to compute secure multiparty summation, so we hope that it can provide some new ideas to solve more secure multi-party computations in future.

Acknowledgment This work was supported by National Natural Science Foundation of China (No.61772001 and 61672010).

References

1. P. W. Shor. Algorithms for Quantum Computation – Discrete Logarithms and Factoring. *Proceedings of 35th Annual Symposium on the Foundations of Computer Science* (IEEE, New York, 1994), pp. 124-134.
2. L. K. Grover. A fast quantum mechanical algorithm for database search. *Proceedings of 28th Annual ACM Symposium on Theory of Computing* (ACM, New York, 1996), pp. 212-219.
3. C.H. Bennett & G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175-179.
4. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.* **70**, 1895 (1993)
5. Qin, H., Tang, W.K.S., Tso, R.: Rational quantum secret sharing. *Sci. Rep.* **8**, 11115 (2018)
6. Lo, H.K.: Insecurity of quantum secure computations. *Phys. Rev. A.* **56**, 1154 (1997)
7. Colbeck, R.: Impossibility of secure two-party classical computation. *Phys. Rev. A.* **76**, 062308 (2007)
8. Buhrman, H., Christandl, M., Schaffner, C.: Complete Insecurity of Quantum Protocols for Classical Two-Party Computation. *Phys. Rev. Lett.* **109**, 160501 (2012)
9. Shi, R.H., Mu, Y., Zhong, H., et al.: Quantum oblivious set-member decision protocol. *Phys. Rev. A.* **92**(2), 022309 (2015)

10. Shi, R.H., Mu, Y., Zhong, H., et al.: Quantum private set intersection cardinality and its application to anonymous authentication. *Inf. Sci.* **370-371**, 147–158 (2016)
11. He, L., Huang, L., Yang, W., X, R.: A protocol for the secure two-party quantum scalar product. *Phys. Lett. A*. **376**, 1323–1327 (2012)
12. Y. Wang, G. He. Quantum secure scalar product with continuous-variable clusters. *Proceedings of the 18th AQIS Conference* (8-12 September 2018, Nagoya, Japan). Available at http://www.ngc.is.ritsumei.ac.jp/~ger/static/AQIS18/OnlineBooklet/161.pdf (2018).
13. Shi, R.H., Mu, Y., Zhong, H., et al.: Secure Multiparty Quantum Computation for Summation and Multiplication. *Sci. Rep.* **6**(19655), (2016)
14. A. Majumder, S. Mohapatra, A. Kumar. Experimental Realization of Secure Multiparty Quantum Summation Using Five-Qubit IBM Quantum Computer on Cloud. arXiv:1707.07460v3 (2017).
15. He, G.P.: Practical quantum oblivious transfer with a single photon. *Laser Phys.* **29**(3), 035201 (2019)
16. G. Brassard, P. Høyer, and A. Tapp. Quantum Counting. *Proceedings of 25th International Colloquium on Automata, Languages and Programming*, LNCS 1443 (Springer-Verlag, Berlin Heidelberg, 1998), pp. 820-831.
17. Mosca, M.: Counting by quantum eigenvalue estimation. *Theor. Comput. Sci.* **264**, 139 (2001)
18. Diao, Z.J., Huang, C.F., Wang, K.: Quantum Counting: Algorithm and Error Distribution. *Acta. Appl. Math.* **118**, 147 (2012)
19. A. Holevo. Probabilistic and Statistical Aspects of Quantum Theory. *Publications of the Scuola Normale Superiore*, Springer, 2011.
20. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)