Secure and Efficient Two-Party Quantum Scalar Product Protocol With Application to Privacy-Preserving Matrix Multiplication

Wen-Jie Liu and Zi-Xian Li

***Abstract*— Secure two-party scalar product (S2SP) is a promising research area within secure multiparty computation (SMC), which can solve a range of SMC problems, such as intrusion detection, data analysis, and geometric computations. However, existing quantum S2SP protocols are not efficient enough, and the complexity is usually close to exponential level. In this paper, a novel secure two-party quantum scalar product (S2QSP) protocol based on Fourier entangled states is proposed to achieve higher efficiency. Firstly, the definition of unconditional security under malicious models is given. And then, an honesty verification method called Entanglement Bondage is proposed, which is used in conjunction with the modular summation gate to resist malicious attacks. The property of Fourierentangled states is used to calculate the scalar product with polynomial complexity. The unconditional security of our protocol is proved, which guarantees the privacy of all parties. In addition, we design a privacy-preserving quantum matrix multiplication protocol based on S2QSP protocol. By transforming matrix multiplication into a series of scalar product processes, the product of two private matrices is calculated without revealing any privacy. Finally, we show our protocol's feasibility in IBM Qiskit simulator.**

***Index Terms*— Quantum computation, quantum communication, secure multi-party computation, scalar product, matrix multiplication.**

I. Introduction

SECURE Multi-party Computation (SMC) enables multiple parties who do not trust each other to collaboratively compute a target function using their respective private data, while preserving the privacy of all participants. Since Yao [1] first proposed this concept in 1982, the main solutions for SMC proposed by classical cryptographers include Garbled Circuit [2], Oblivious Transfer [3], [4], [5], Secret Sharing [6], [7], [8], [9], Homomorphic Encryption [10], [11], [12], etc. However, protocols with higher generality typically exhibit greater complexity. As a result, researchers often focus on developing specialized SMC protocols tailored to specific problems. Secure Two-party Scalar Product (S2SP) is a research area that investigates how two parties can securely compute the scalar product of their respective private vectors. Many SMC problems, such as intrusion detection [13], [14], [15], data analysis [16], [17], [18], [19], and geometry computation [20], [21], [22], can be reduced to S2SP, which makes it a crucial building block for general secure computation. However, current classical S2SP schemes either exhibit high complexity or rely on the Computational Hardness Assumption for their security. Thus, there is an urgent requirement for a novel scheme that achieves both high security and computational efficiency.

In recent years, there has been a growing interest in utilizing quantum mechanisms with potential for unconditional security to achieve secure multiparty computation (SMC), which is referred to as quantum SMC (QSMC) [23], [24], [25], [26], [27]. However, existing Secure Two-party Quantum Scalar Product (S2QSP) protocols are not efficient enough. In 2012, He et al. [28] pioneered a S2QSP protocol, which requires a non-colluding third party to distribute entangled states among the two participants. Furthermore, it demands significant entanglement resources, which may exceed the required level when operating on sparse private input vectors. In 2018, Wang and He [29] proposed a new S2QSP scheme using classical cryptography and continuous-variable clusters. Their scheme no longer needs a third party, but still needs massive redundant quantum resources and measurement operations. In 2019, Shi and Zhang [30] proposed a strong privacy-preserving S2QSP protocol using Grover's algorithm [31] with constant communication complexity. However, while Grover's algorithm provides a quadratic speedup, its computational complexity remains close to exponential. As a result, existing S2QSP protocols only offer unconditional security with limited improvement in computational efficiency.

Compared with S2QSP, people have more fully studied two QSMC problems, i.e., Secure Multi-party Quantum Summation or Multiplication (SMQS or SMQM), where several parties can secretly add or multiply up their private integers. In 2013, Yang et al. [32] proposed a secret sharing scheme based on Quantum Fourier Transform $\mathcal{QFT}$. It takes advantage of a property of d-level cat state [33], i.e., the ability to keep the sum unchanged after applying the Modular Summation Gate $\mathcal{SUM}$. Based on this scheme, people have proposed several SMQS protocols [34], [35], [36], [37], [38], [39]. However, these protocols are limited to SMQS. In 2016, Shi et al. [40] provided another way. They transformed the calculation from the bit domain to the phase domain, then used the Rotation Gate $\mathcal{ROT}$ to perform the addition. This idea is inspired by Draper's Transform Adder [41]. Here, SMQM is implemented by using the Modular Multiplication Gate $\mathcal{MUL}$. In addition, they

Manuscript received 9 April 2023; revised 26 June 2023; accepted 12 July 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62071240, in part by the Innovation Program for Quantum Science and Technology under Grant 2021ZD0302900, and in part by the Research Innovation Program for College Graduates of Jiangsu Province, China, under Grant KYCX23_1370. This article was recommended by Associate Editor N. Karimian. *(Corresponding author: Wen-Jie Liu.)*

The authors are with the School of Software, Nanjing University of Information Science and Technology, Nanjing 210044, China (e-mail: wenjiel@163.com; zixianli157@163.com).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSI.2023.3295891.

Digital Object Identifier 10.1109/TCSI.2023.3295891

used Bitwise XOR Gate $\mathcal{XOR}$ (or $\mathcal{CNOT}$ gate) to construct the d-level cat state, and applied again when returning to untie the entanglement, and check the honesty of the other party. Considering that the states appearing in the protocol have exceeded the category of cat states, we define them as a more generalized state called Fourier Entangled (FE) State.

Although SMQS and SMQM protocols using FE states are efficient, they cannot be directly applied to scalar product computations due to the interference between addition and multiplication in such calculations. However, we discover the following insight: Shi et al.'s method [40] allows both addition and multiplication to be performed simultaneously without interference, as addition is performed in the phase domain and multiplication is performed in the bit domain. In this paper, we propose a novel secure quantum scalar product protocol based on this nature, to achieve higher computational efficiency. To transform this idea into a sufficiently secure S2QSP protocol, we first use $\mathcal{SUM}$ to impose several random number in the bit domain to prevent the measurement attack. What's more, we apply a bi-particle version of $\mathcal{SUM}$ ($\mathcal{BSUM}$) to entangle all particles, so as to prevent verify the honesty of the sender. We refer to this operation as Entanglement Bondage, and design an corresponding honesty test to check the sender's honesty. In this way, the two parties will get an almost fair position, and can resist against forgery attacks without the assistance of a third party. It is worth noting that since $\mathcal{QFT}$ is one of the few quantum algorithms that can achieve exponential acceleration, our S2QSP scheme can calculate scalar products with the highest known efficiency, namely polynomial complexity.

Our contributions in this paper are summarized below.

1) Based on the conceptions of Leakage Degree and Negligibility, the definition of unconditional security under the malicious model is given in detail.
2) An honesty verification method called Entanglement Bondage is proposed, which is used in conjunction with the modular summation gate to resist various malicious attacks.
3) Based on the property of Fourier Entangled state and the methods in 2), we propose a S2QSP protocol with polynomial complexity. and prove its unconditional security.
4) Based on the proposed S2QSP protocol, we present a privacy-preserving matrix multiplication protocol, as an extended application of it.
5) Finally, we verify the feasibility of the proposed S2QSP protocol in IBM Qiskit simulator.

The rest of this paper is arranged as follows. In Section II, we define the notations we used, give the quantum operations to be used, and introduce the Fourier entangled state. In Section III, we define unconditional security in the malicious model, propose the entanglement bondage, then present our protocol. We analyze our protocol in Section IV, and give an application of it in Section V. We conclude in Section VI.

II. Preliminary

A. Definitions of Notations

Table I shows the definitions of notations used.

TABLE I
Definitions of Notations

Symbols	Meanings
$\imath$	Imaginary unit
n	Dimension of input vector
$\mathbf{x} = (x_1, x_2, \cdots, x_n)$	Alice's input vector
$\mathbf{y} = (y_1, y_2, \cdots, y_n)$	Bob's input vector
v	Bob's input random integer
u	Alice's output
$d, D = 2^d$	Particle's qubit number and dimension
a^{-1}	Multiplicative inverse of a mod D
$\oplus$	Bitwise XOR
ω	$e^{\frac{\imath 2\pi}{D}} = \cos(\frac{2\pi}{D}) + \imath \sin(\frac{2\pi}{D})$
$m, N = 2^m$	Output's bit number and modulus
$[N]$	Set $\{0, 1, \cdots, N-1\}$
$[N]^o$	Set composed of odd numbers in $[N]$
$a \mid b$	a is a factor of b
$a \equiv b (\mod D)$	$D \mid (a-b)$
$\lvert\psi\rangle_h$	Particle h is in state $\lvert\psi\rangle$
$\mathcal{U}_h$	Quantum gate $\mathcal{U}$ performed on particle h
$a \parallel b$	String connected by two strings a, b
(h, t)	System composed of particles h and t
$\lfloor a \rfloor, \lceil a \rceil$	Round integer a up and down respectively
$\lvert A \rvert$	Cardinality of set A
$g : A \to B$	Function g from set A to set B
$g^{-1}(b)$	Solution set $\{a \mid g(a) = b, a \in A\}$
$Im(g)$	Image set $\{b \mid g(a) = b, a \in A\}$
$\Pr(A)$	Probability of event A
$H(A, B), H(A : B), H(A \mid B)$	Joint entropy, mutual information and conditional entropy of random variables A, B [42]
Z_A, Z_B	View of Alice, Bob respectively
X_A, X_B	Privacy of Alice, Bob respectively
I_A, I_B	Leakage degree of Alice, Bob's privacy respectively

B. Quantum Operations

Taking two d-qubits particles $h = (h_{d-1}, h_{d-2}, \cdots, h_0)$ and $t = (t_{d-1}, t_{d-2}, \cdots, t_0)$ as example, the quantum gates used in this paper are as follows (where addition and multiplication are all performed mod D).

1) Quantum Fourier Transform $\mathcal{QFT}$ and its inverse:

$$\mathcal{QFT}_h : |a\rangle_h \to \frac{1}{\sqrt{D}} \sum_{j \in [D]} \omega^{aj} |j\rangle_h, \tag{1}$$

$$\mathcal{QFT}_h^\dagger : |a\rangle_h \to \frac{1}{\sqrt{D}} \sum_{j \in [D]} \omega^{-aj} |j\rangle_h. \tag{2}$$

2) Rotation Gate $\mathcal{ROT}(b)$ where $b \in [D]$:

$$\mathcal{ROT}(b)_h : |a\rangle_h \to \omega^{ab} |a\rangle_h. \tag{3}$$

3) Modular Summation Gate $\mathcal{SUM}(b)$ where $b \in [D]$:

$$\mathcal{SUM}(b)_h : |a\rangle_h \to |a+b\rangle_h. \tag{4}$$

Note that $-b \equiv D - b \pmod D$.

4) Modular Multiplication Gate $\mathcal{MUL}(b)$ where $b \in [D]^o$:

$$\mathcal{MUL}(b)_h : |a\rangle_h \to |ab\rangle_h. \tag{5}$$

Note that b is odd, so it is coprime with $D = 2^d$ and then has a unique multiplicative inverse b^{-1} mod D.

5) Bi-particle Modular Summation Gate $\mathcal{BSUM}$:

$$\mathcal{BSUM}_{(h,t)} : |a\rangle_h |b\rangle_t \to |a\rangle_h |b+a\rangle_t. \tag{6}$$

6) Bitwise XOR Gate $\mathcal{XOR}$:

$$\mathcal{XOR}_{(h,t)} : |a\rangle_h |b\rangle_t \to |a\rangle_h |b \oplus a\rangle_t. \tag{7}$$

C. Fourier Entangled State

Definition 1 (Fourier Entangled (FE) State): Let $X \in S_X$ be a secret, $C \in S_C$ be a random variable independent of X, $\forall x \in S_X, \forall C \in S_C, \Pr(X = x) = p_x = \frac{1}{|S_X|}$, Pr $(C = c) = p_c = \frac{1}{|S_C|}$. Given two quantum systems P, Q

with l_1, l_2 qubits respectively, and one $D = 2^d$-dim FE state is as:

$$|\psi(x,c)\rangle_{(P,Q)} = \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jh(x,c)} |f(j,x,c)\rangle_P |g(j,x,c)\rangle_Q , \quad (8)$$

where $f : [D] \times S_X \times S_C \to [2^{l_1}]$, $g : [D] \times S_X \times S_C \to [L]$, $L = 2^{l_2}$. $\forall j', j \in [D], \langle f(j',x,c)|f(j,x,c)\rangle = \delta_{j'j}$.

We call the systems P and Q local systems. We generally consider attacks on Q, not P. The function $h(x,c)$ is called Phase domain, correspondingly, the functions $f(j,x,c), g(j,x,c)$ are Bit domain. The information these functions contain are called Phase-information and Bit-information respectively.

Assume an FE state $\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_P |ja_1\rangle_{Q_1} |ja_2\rangle_{Q_2}$, where $a_1, a_2 \in [D]^o$, and it has the following properties:

Property 1 (Addition-Multiplication Independence): If using $\mathcal{ROT}(b_1)$ on Q_1, it will be attached a phase factor $\omega^{ja_1b_1}$. If using $\mathcal{ROT}(b_2)$ on Q_2, there is a new factor $\omega^{ja_2b_2}$. Therefore, the total phase is $\omega^{j(a_1b_1+a_2b_2)}$.

Property 2 (Addend's Disappearance): Apply $\mathcal{SUM}(c)$ on Q_1, then apply $\mathcal{ROT}(b)$ on $|ja_1 + c\rangle_{Q_1}$. Since the global phase factor ω^{bc} does not affect any measurement results [42], it can be omitted, i.e., the addend c does not affect the phase.

III. Proposed Protocol

In this section, we first define the unconditional security under the malicious model, then briefly introduce Entanglement Bondage we will use in the protocol. We provide the specific protocol process at the end.

A. Unconditional Security Under the Malicious Model

Definition 2 (Malicious Adversary Model): In this model, attacks other than a) forging input, b) not participating in the protocol, and c) terminating the protocol halfway should be all defensed or detected.

In addition, the following assumptions are also made to simplifies the analysis:

1) Malicious adversaries do not input, but only steal, since the information it inputs will interfere with its attack.
2) Malicious adversaries are to obtain information, not just destroy. We mainly ensure the privacy of valid information.
3) If either party is malicious, the other is not, since a protocol executed between malicious participants is meaningless.

Considering the particularity of quantum protocols, we use information theory language to define unconditional security under this model. Assume that in a two-party protocol Π, there is an honest party HP and a malicious party MP respectively. Denote the privacy of HP is a random variable X, with a Shannon entropy $H(X) = m_X$. Denote the expected result MP should get as F. Then

Definition 3 (Leakage Degree): Under an attack AT, the view obtained by MP is a random variable Z. Mutual information $I = H(Z : X)$ measures the information increment to X when Z is known. Stipulate that if attack AT is detected by HP, $H(Z : X) = 0$, since the attack has failed. If MP cannot get F after its attack, then the **leakage degree** of X is defined as $H(Z : X)$; Otherwise, it equals to the **conditional mutual information** [43] $H(Z : X|F)$, which measures how much information MP will obtain other than F.

Definition 4 (Negligibility): A function $\mu(m_X) : \mathbb{N} \to [0, 1]$ is said to be **negligible**, if there is no positive polynomial $poly(m_X)$ about m_X so that $\mu(m_X) = \Omega(1/poly(m_X))$.

Definition 5 (Unconditional Security Under the Malicious Model): Protocol Π is said to has unconditional security under the malicious model, if in one run of Π, the leakage degree of any party's privacy is negligible under all known malicious attacks.

B. Entanglement Bondage

Assume that in a quantum protocol, MP should send several particles t_1, t_2, g to HP, which are FE-entangled as $\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_{t_1} |ja_1\rangle_{t_2} |ja_2\rangle_g$, $a_1, a_2 \in [D]^o$. However, MP can perform a **forgery attack**, i.e., it doesn't entangle t_1, t_2, g. Now HP wants to verify MP's honesty, without disrupting the superposition state of the particles. HP applies $\mathcal{MUL}, \mathcal{BSUM}$ to add the state j, ja_1 to ja_2:

$$ja_2 \to jk_1 + jk_2a_1 + jk_3a_2 = j(k_1 + k_2a_1 + k_3a_2), \quad (9)$$

where $k_1, k_2, k_3 \in [D]^o$. This process is called **Entanglement Bondage**. If MP is dishonest, then this step will entangle the three particles. Under the entanglement, MP cannot steal information without being detected.

After the above steps, HP can perform an honesty test as follows. HP sends k_1, k_2, k_3 to MP, and MP will return an answer $r = (k_1 + k_2a_1 + k_3a_2)^{-1}$, since the add of any three odds is also an odd. HP applies $\mathcal{MUL}(r)$ on g, then $bra\,j(k_1 + k_2a_1 + k_3a_2)_g \to |j\rangle_g$. Now HP can perform $\mathcal{XOR}$ on t_1, g, then $|j\rangle_g \to |0\rangle_g$. HP can verify the correctness of the state prepared by MP by measuring g. If g is in state $|0\rangle$, then MP passes; Otherwise, MP's cheating is detected. This process is actually a zero-knowledge proof, through which HP can verify whether MP really prepared the correct quantum state as promised, without measuring the state itself. The effectiveness of this mechanism can be seen in Section IV-B.

C. Specific Protocol Process

Definition 6 (Secure Two-Party Scalar Product (S2SP)): Alice and Bob each have an n-dim vector $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{y} = (y_1, y_2, \cdots, y_n)$ respectively, where $x_i, y_i \in [N]$, $N = 2^m$. Alice is to get $u = \mathbf{x} \cdot \mathbf{y} + v \bmod N = \sum_{i=1}^{n} x_i y_i + v \bmod N$, while $v \in [N]$ is known only by Bob. A secure protocol should meet the following requirements:

- Alice's Privacy: Bob learns no information about $\mathbf{x}$.
- Bob's Privacy: Alice learns no information about $\mathbf{y}, v$ other than $u = \mathbf{x} \cdot \mathbf{y} + v \bmod N$.

Protocol 1: Secure Two-party Quantum Scalar Product Protocol (S2QSPP).

1) Preparation Stage:

Step 1 Alice and Bob set $d = m + 2$ and $D = 2^d$.

Step 2 Alice assigns $p_i = 2x_i + 1$ for each $i = 1, 2, \cdots, n$.

Step 3 Bob selects randomly $v_1, v_2, \cdots, v_{n-1} \in [N]$, and then sets $v_n = \frac{4v - 4\sum_{i=1}^{n-1} v_i \bmod D}{4}$, i.e., $4\sum_{i=1}^{n} v_i \equiv 4v (\bmod D)$. He assigns $q_i = 2y_i + 1$ and $s_i = 4v_i - 2y_i - 1 \bmod D$.

2) Operation Stage: For each $i = 1, 2, \cdots, n$, do the following steps (all arithmetic operations are performed mod D here):

Step 1 (*Alice's Inputing*) Alice prepares 4 d-qubit particles h, t_1, t_2, g initialized as $|0\rangle$. She selects $c_1, c_2, c_4 \in [D]$ and $c_3 \in [D]^o$ randomly, then does the following:

$$\begin{aligned}&|0\rangle_h |0\rangle_{t_1} |0\rangle_{t_2} |0\rangle_g \\ &\xrightarrow{\mathcal{QFT}_h} \frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |0\rangle_{t_1} |0\rangle_{t_2} |0\rangle_g \\ &\xrightarrow{\mathcal{XOR}_{(h,t_1)}\mathcal{XOR}_{(h,t_2)}\mathcal{XOR}_{(h,g)}} \\ &\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |j\rangle_{t_1} |j\rangle_{t_2} |j\rangle_g \\ &\xrightarrow{\mathcal{MUL}(p_i)_{t_2}\mathcal{MUL}(c_3)_g} \\ &\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |j\rangle_{t_1} |jp_i\rangle_{t_2} |jc_3\rangle_g \\ &\xrightarrow{\mathcal{SUM}(c_1)_{t_1}\mathcal{SUM}(c_2)_{t_2}\mathcal{SUM}(c_4)_g} \frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h \\ &|j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} |jc_3+c_4\rangle_g . \end{aligned} \tag{10}$$

Now the particles h, t_1, t_2, g are in an FE state. Alice then sends t_1, t_2, g to Bob.

Step 2 (*Entanglement Bondage*) Bob selects $k_1, k_2, k_3 \in [D]^o$ randomly, then does the following:

$$\begin{aligned}&\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} |jc_3+c_4\rangle_g \\ &\xrightarrow{\mathcal{MUL}(k_1)_{t_1}\mathcal{MUL}(k_2)_{t_2}\mathcal{MUL}(k_3)_g} \\ &\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |jk_1+c_1k_1\rangle_{t_1} |jp_ik_2+c_2k_2\rangle_{t_2} \\ &|jc_3k_3+c_4k_3\rangle_g \\ &\xrightarrow{\mathcal{BSUM}_{(t_1,g)}\mathcal{BSUM}_{(t_2,g)}} \\ &\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |jk_1+c_1k_1\rangle_{t_1} |jp_ik_2+c_2k_2\rangle_{t_2} \\ &|j\,(k_1+p_ik_2+c_3k_3)+(c_1k_1+c_2k_2+c_4k_3)\rangle_g \\ &= \frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |jk_1+c_1k_1\rangle_{t_1} |jp_ik_2+c_2k_2\rangle_{t_2} \\ &|jr_1+r_2\rangle_g \\ &\xrightarrow{\mathcal{MUL}(k_1^{-1})_{t_1}\mathcal{MUL}(k_2^{-1})_{t_2}} \frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |j+c_1\rangle_{t_1} \\ &|jp_i+c_2\rangle_{t_2} |jr_1+r_2\rangle_g , \end{aligned} \tag{11}$$

where $r_1 = k_1 + p_ik_2 + c_3k_3$, $r_2 = c_1k_1 + c_2k_2 + c_4k_3$.

Step 3 (*Bob's Inputing*) Bob does the following:

$$\begin{aligned}&\frac{1}{\sqrt{D}} \sum_{j\in[D]} |j\rangle_h |j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} |jr_1+r_2\rangle_g \\ &\xrightarrow{\mathcal{ROT}(s_i)_{t_1}\mathcal{ROT}(q_i)_{t_2}} \frac{1}{\sqrt{D}} \omega^{(j+c_1)s_i} \omega^{(jp_i+c_2)q_i} \\ &\sum_{j\in[D]} |j\rangle_h |j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} |jr_1+r_2\rangle_g \\ &= \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} \\ &|jr_1+r_2\rangle_g , \end{aligned} \tag{12}$$

where $M_i = s_i + p_iq_i$. We can omit the global phase $\omega^{c_1s_i+c_2q_i}$.

Step 4 (*Alice's Honesty Test*) Bob now verifies Alice's honesty as follows:

a) (*Question*) Bob tells Alice the values of k_1, k_2, k_3.
b) (*Answer*) Alice calculates $r_3 = r_1^{-1}$ and $r_4 = c_1 - r_2r_3$, then tells Bob the values of r_3, r_4.
c) (*Verification*) Bob does the following:

$$\begin{aligned}&\frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} \\ &|jp_i+c_2\rangle_{t_2} |jr_1+r_2\rangle_g \\ &\xrightarrow{\mathcal{MUL}(r_3)_g} \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} \\ &|jp_i+c_2\rangle_{t_2} |j+r_2r_3\rangle_g \\ &\xrightarrow{\mathcal{SUM}(r_4)_g} \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} \\ &|jp_i+c_2\rangle_{t_2} |j+c_1\rangle_g \\ &\xrightarrow{\mathcal{XOR}_{(t_1,g)}} \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} \\ &|jp_i+c_2\rangle_{t_2} |0\rangle_g , \end{aligned} \tag{13}$$

and measures g. Alice passes only if he gets $|0\rangle_g$.

If the test is passed, then Bob returns t_1, t_2 to Alice.

Step 5 (*Bob's Honesty Test A*) Alice now verifies Bob's honesty as follows:

$$\begin{aligned}&\frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j+c_1\rangle_{t_1} |jp_i+c_2\rangle_{t_2} \\ &\xrightarrow{\mathcal{SUM}(-c_1)_{t_1}\mathcal{SUM}(-c_2)_{t_2}} \\ &\frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j\rangle_{t_1} |jp_i\rangle_{t_2} \\ &\xrightarrow{\mathcal{MUL}(p_i^{-1})_{t_2}} \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h |j\rangle_{t_1} |j\rangle_{t_2} \\ &\xrightarrow{\mathcal{XOR}_{(h,t_1)}\mathcal{XOR}_{(h,t_2)}} \frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h \\ &|0\rangle_{t_1} |0\rangle_{t_2} , \end{aligned} \tag{14}$$

and measures t_1, t_2. Bob passes the test only if Alice gets $|0\rangle_{t_1} |0\rangle_{t_2}$.

Step 6 (*Alice's Result*) Alice preforms $\mathcal{QFT}^\dagger$ on h:

$$\frac{1}{\sqrt{D}} \sum_{j\in[D]} \omega^{jM_i} |j\rangle_h \xrightarrow{\mathcal{QFT}_h^\dagger} |M_i\rangle_h \mod D, \tag{15}$$

and measures h to obtain the result $M_i = s_i + p_iq_i$.

The quantum circuit of all the steps is shown in figure 1.

3) Output Stage: Alice calculates as $Output = \frac{\sum_{i=1}^{n}(M_i-2x_i) \mod D}{4}$.

IV. Protocol Analysis

A. Correctness

$$Output = \frac{\sum_{i=1}^{n}(M_i-2x_i) \mod D}{4}$$

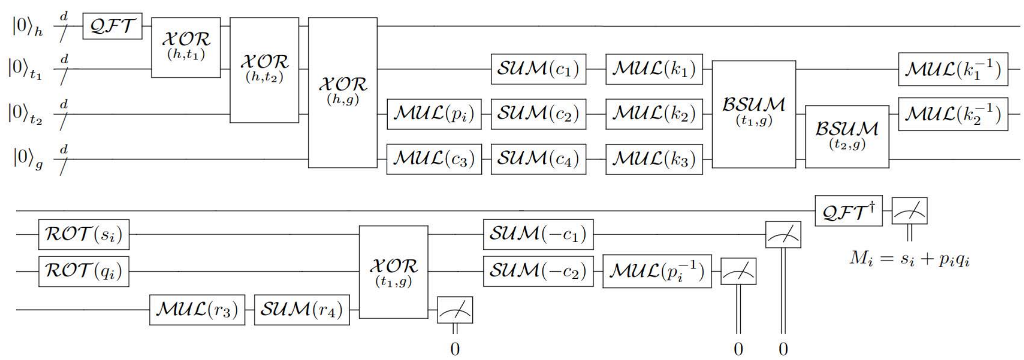

Fig. 1. The quantum circuit of Operation stage.

$$\begin{aligned}
&= \frac{\sum_{i=1}^{n}(s_i + p_i q_i - 2x_i) \mod D}{4} \\
&= \frac{\sum_{i=1}^{n}(4v_i + 4x_i y_i) \mod D}{4} \\
&= \frac{4\sum_{i=1}^{n} v_i + 4\sum_{i=1}^{n} x_i y_i \mod D}{4} \\
&= \frac{4v + 4\sum_{i=1}^{n} x_i y_i \mod D}{4} \\
&= \frac{4(v + \sum_{i=1}^{n} x_i y_i) - a2^d}{4} \\
&= \frac{4(v + \sum_{i=1}^{n} x_i y_i - a2^m)}{4} \\
&= v + \sum_{i=1}^{n} x_i y_i - a2^m,
\end{aligned} \tag{16}$$

where $4(v + \sum_{i=1}^{n} x_i y_i) - a2^d \in [D]$ and $d = m + 2$, thus $v + \sum_{i=1}^{n} x_i y_i - a2^m \in \left[\frac{D}{4}\right] = [N]$. I.e.,

$$\begin{aligned}
Output &= v + \sum_{i=1}^{n} x_i y_i - a2^m \\
&= v + \sum_{i=1}^{n} x_i y_i \mod D = u.
\end{aligned} \tag{17}$$

B. Security

Since all the interactions occur in Operation stage, an attacker may try the following possible attacks.

1) Measurement Attack

Measurement attack is to directly perform a local general measurement on the attacker's own particles. "General quantum measurement" is equivalent to a combination of introducing auxiliary systems, performing unitary operations and projective measurements [42].

2) Entangle-measure Attack

After receiving a particle t, the attacker can prepare an auxiliary particle e and perform a unitary operation

$$\mathcal{U}_\varepsilon : |j\rangle_t |0\rangle_e \rightarrow \sqrt{\eta_j}\,|j\rangle_t |\varepsilon(j)\rangle_e + \sqrt{1-\eta_j}\,|V(j)\rangle_{(t,e)}, \tag{18}$$

where η is the probability that $|j\rangle_t$ is not changed. Then he sends t back, and monitors its movement by measuring e.

3) Forgery Attack

Forgery attack is to send a particle in a forged rather than correct state to steal information, as a type of malicious attack.

4) Intercept-Resend Attack

Similar to forgery attack, intercept-resend attack means to obtain information from a particle after receiving it, and then return a forged particle back.

5) False Verification Information Attack

This attack may occur in Step 4 of Operation stage, which means to send fake verification information, such as k_1, k_2, k_3 and r_3, r_4.

6) External Attack

External attack means that any eavesdropper Eve wants to steal Alice or Bob's privacy.

7) Semi-honest attack

If the attacker is semi-honest, it may try to deduce information other than the expected result it should get, from all the values it can obtain during the protocol.

We has the following theorem.

Theorem 1: Protocol 1 holds unconditional security under the malicious model, i.e., it can resist the above attacks.

Proof:

1) Measurement Attack

First, we give the following Lemma 1. It is proved in Appendix A-A, relying on the use of partial trace $tr_P(\cdot)$.

Lemma 1 (Security of Phase-information): Under the entanglement of an FE state as Definition 1, any attacker who only owns local system Q cannot extract the phase-information.

• **Alice's Privacy:** Denote $X_A = x_i$. To steal the largest information, Bob can wait for r_3, r_4, then measure t_1, t_2, g. For the leakage degree of Alice's privacy $I_A = H(Z_B : X_A)$, we have the following Lemma 2. Its proof relies on the Holevo bound [44], see Appendix A-B for details.

Lemma 2 (Security of Bit-information): Under the measurement attack, $I_A = 0$, i.e., Bob cannot obtain any valid information about X_A. Besides, this effect cannot be achieved without particle g.

• **Bob's Privacy:** Denote $X_B = (y_i, v_i)$. Until Step 5, Bob owns a local system (t_1, t_2, g) of the FE state. By Lemma 1, Alice cannot obtain any information about q_i, s_i, because they are all on the phase. I.e., The leakage degree of Bob's privacy $I_A = H(Z_A : X_B) = 0$.

2) Entangle-Measure Attack

• **Alice's Privacy:** Denote $X_A = x_i$. After Bob resent, it is possible to obtain information by measuring only in Step 6, since only now Alice carries on operations. Because Alice performs an honest test on the sent particles t_1, t_2 in Step 5, if they are no longer in their original states, the attack will be detected. Therefore, η_j should be set to 1, i.e., $\mathcal{U}_\varepsilon : |j\rangle_t |0\rangle_e \rightarrow |j\rangle_t |\varepsilon(j)\rangle_e$.

Assume that Bob owns all particles t_1, t_2, g, e to steal the largest information, and performs $\mathcal{U}_\varepsilon$. Note that the Holevo bound of Bob's particle now equals to that in measurement attack, i.e., $H(Z_B : X_A) = 0$ (see the proof of Lemma 2), because $\mathcal{U}_\varepsilon$ is a local quantum operation and does not increase the Holevo bound (Chapter 12 Problem 12.1 of [42]). If he returns any particle, he cannot steal more, since discarding quantum systems is also a kind of quantum operations and does not increase the Holevo bound. Alice's any operations in Step 6 are equivalent to local quantum measurement, which doesn't affect Bob's measurement results by the principle of implicit measurement (Chapter 4.4 of [42]). Therefore, it also does not increase the Holevo bound of Bob's particles. In this way, we can immediately deduce that $I_A = 0$, consistent with the measurement attack.

- **Bob's Privacy:** Alice cannot perform entangle-measure attacks, since she may only send particles once.

3) Forgery Attack

- **Alice's Privacy:** Since Alice won't return the particles sent by Bob, Bob cannot perform forgery attacks.
- **Bob's Privacy:** Denote $X_B = (y_i, v_i)$. Since Bob's information only exists on the phase domain, the only known way to obtain it is to use $\mathcal{QFT}^\dagger$. By Lemma 1, it is impossible to obtain phase-information under entanglement, then particles t_1, t_2 must be non-entangled. Accordingly, we have the following Lemma 3. We prove it by using the Holevo bound [44] in Appendix A-C.

Lemma 3 (Security Under Forgery Attack): Due to the entanglement bondage in Step 2 and the test in Step 4, the leakage degree of Bob's privacy under the forgery attack is $I_B < \frac{d^2+d-2}{2 \cdot 2^d} = O\left(\frac{d^2}{2^d}\right)$, with an asymptotic coefficient $\frac{1}{2}$.

I_B is negligible, since 2^d is exponential level. When d reaches its minimum value, i.e., $d = 1 + 2 = 3$, then $\frac{d^2+d-2}{2 \cdot 2^d} = \frac{5}{8}$. This bound will soon approach 0 as d increases.

4) Intercept-Resend Attack

- **Alice's Privacy:** If Bob sends any forged particle back in Step 4, then as in the measurement attack, the leakage degree of Alice's privacy $I_A = 0$.
- **Bob's Privacy:** Similar to forgery attacks, it is impossible for Alice to perform this attack.

5) False Verification Information Attack

- **Alice's Privacy:** If Bob did not send the correct k_1, k_2, k_3, we have $I_A = 0$, just like the measurement attack.
- **Bob's Privacy:** Similarly, if Alice sends incorrect r_3, r_4, then $I_B = 0$, and Bob can detect it in Step 4 c).

6) External Attack

According to the analysis above, if Eve intercepts the particles sent by Alice to Bob, obviously she will get nothing. Similarly, if she intercepts the particles returned by Bob to Alice, she cannot get Bob's privacy.

7) Semi-honest Attack

- **Alice's Privacy:** If Bob is semi-honest, then all he can learn are r_3, r_4. He won't obtain any information, as well as in the measurement attack.
- **Bob's Privacy:** Denote $X_B = (\mathbf{y}, v)$. If Alice is semi-honest, all she can learn are $M_i \equiv p_i q_i + s_i \equiv 4x_i y_i + 4v_i (\bmod D)$. She may try to learn any information other than $u = \sum_{i=1}^{n} x_i y_i + v \bmod N$. We have the following Lemma 4, and prove it in Appendix A-D, by directly calculate the Shannon entropy.

Lemma 4 (Security Under Semi-Honest Attack): Even if Alice knows all M_i, the leakage degree of Bob's privacy $I_B = 0$.

In total, Protocol 1 has unconditional security under the malicious model. ∎

C. Performance

We take the basic 1-, 2- and 3-qubit quantum gates as the measurement unit of computational complexity, such as Hadamard Gate $\mathcal{H} : |a\rangle \to \frac{|0\rangle + (-1)^a |1\rangle}{\sqrt{2}}$, Controlled-X Gate $\mathcal{CNOT} : |a\rangle |b\rangle \to |a\rangle |b \oplus a\rangle$, Z-axis Rotation Gate $\mathcal{P}(i) : |a\rangle \to e^{\frac{\imath 2\pi 2^i}{D} a} |a\rangle$ $(i \in [d])$, it's controlled version $\mathcal{CP}(i) : |a\rangle |b\rangle \to e^{\frac{\imath 2\pi 2^i}{D} ab} |a\rangle |b\rangle$, and Toffoli Gate $\mathcal{T} : |a\rangle |b\rangle |c\rangle \to |a\rangle |b\rangle |c \oplus a \cdot b\rangle$, etc.

TABLE II

PERFORMANCE COMPARISON

Protocols	Third Party	Quantum Resource	Computational Complexity	Communication Complexity
He[28]	✓	Qubit	$O\left(4^m n \log^2 n\right)$	$O\left(4^m n \log^2 n\right)$
Wang[29]	×	Qumode	$O\left(n 2^{4m}\right)$	$O\left(2^{4m}\right)$
Shi[30]	×	Qubit	$O\left(\sqrt{2^m}\right)$	$O\left(m\right)$
Our	×	Qubit	$O\left(nm^2\right)$	$O\left(nm\right)$

In general, the complexity of the gates in Section II-B are all below $O(d^2)$ (see Appendix B-A for details). Since $d = O(m)$, the total complexity of Protocol 1 is $O(nm^2)$. Since there are only 4 d-qubit particles are sent for each $i = 1, 2, \cdots, n$, the communication complexity is $O(nm)$.

We use m, n to represent the bit number and dimension of input vectors respectively. See Table II for the comparison between our protocol and the previous. In [28], $O\left(4^m n \log^2 n\right)$ entanglements should have been prepared and sent. In [29], for real vectors $\mathbf{x}$, $\mathbf{y}$, $\langle \mathbf{x} | \mathbf{y} \rangle$ was evaluated with accuracy ϵ. Its computational and communication complexity are $O(n\epsilon^{-2})$ and $O(2\epsilon^{-2} + n^2)$ respectively. Let $|\mathbf{x}|$, $|\mathbf{y}| = \Theta\left(2^m\right)$, then $\epsilon = \Theta(2^{-2m})$ is needed for the error of $\mathbf{x} \cdot \mathbf{y}$ to be less than 1. Grover's algorithm was used in [30], with complexity $O\left(\sqrt{2^m}\right)$. It can be seen that our protocol is polynomial in terms of computational and communication complexity, while the previous protocols have at least one complexity close to exponential. In addition, our protocol does not require a third party. The above proves its advantages.

D. Experiment

We verify the correctness and the feasibility of our protocol by circuit simulation experiments in IBM Qiskit simulator (Qiskit-0.41.0; Python-3.7; OS-Windows). Without loss of generality, let's set $m = 2$ (i.e., $d = 4$). The circuits of all quantum gates we used are described in figure 2. Because the complexity of classical simulation is sensitive to qubits' number, we use Draper's adder [41], as shown in figure 2(c) and 2(e). It requires no auxiliary qubits, but has higher complexity $O(d^2)$. Besides, we design a special circuit for module multiplication on $[D]$ as shown in figure 2(d) to further reduce qubits. See Appendix B-B for details of this design. Finally, we omit the measurement of particles t_1, t_2, g and only focus on the output results on particle h. The total circuit of Protocol 1 is shown in figure 3. We execute the experiment two times. Table III shows the first input and output, with the selection of the intermediate parameters $v_i, c_1, c_2, c_3, c_4, k_1, k_2, k_3$. Similarly, table IV describe the second experiment. Each quantum program for $i = 1, 2, 3, 4$ is executed 1000 times, and figure 4 shows the results. It can be seen that our protocol can be run successfully with 100% probability, so it is correct and feasible.

V. APPLICATION

In this section, we present an application of Protocol 1, i.e., a Privacy-preserving Two-party Matrix Multiplication (P2MM) protocol. This problem has been extensively studied

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

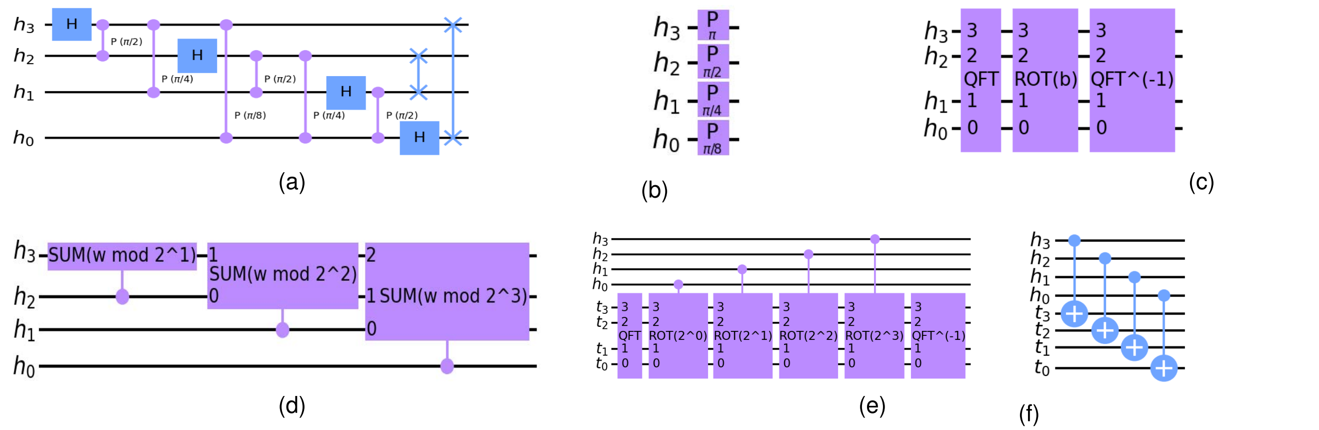

Fig. 2. The circuits of quantum gates. a), b), c), d), e), f) are circuits of $\mathcal{QFT}$, $\mathcal{ROT}$, $\mathcal{SUM}$, $\mathcal{MUL}$, $\mathcal{BSUM}$, $\mathcal{XOR}$, respectively.

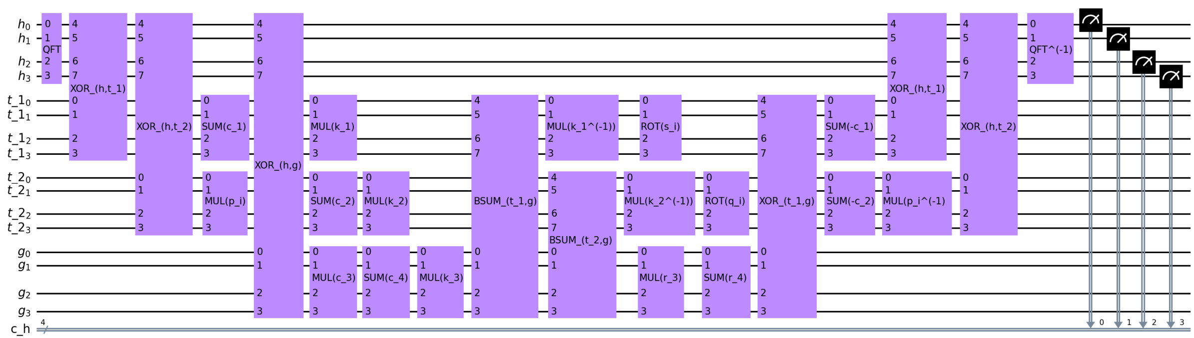

Fig. 3. The total circuit of our protocol.

TABLE III

PARAMETER OF THE FIRST EXPERIMENT

External Parameter		Input				Intermediate Parameter																	Output	
m	N	i	x_i	y_i	v	d	D	v_i	p_i	q_i	s_i	c_1	c_2	c_3	c_4	k_1	k_2	k_3	r_1	r_2	r_3	r_4	M_i	u
2	4	1	1	0	1	4	16	0	3	1	15	2	15	9	12	5	9	5	13	13	5	1	2	0
		2	0	3				11	1	7	5	10	6	11	3	15	5	7	1	9	1	1	12	
		3	1	1				15	3	3	9	10	11	3	2	1	1	1	7	7	7	9	2	
		4	2	3				13	5	7	5	4	9	1	6	7	9	15	3	7	11	7	8	

TABLE IV

PARAMETER OF THE SECOND EXPERIMENT

External Parameter		Input				Intermediate Parameter																	Output	
m	N	i	x_i	y_i	v	d	D	v_i	p_i	q_i	s_i	c_1	c_2	c_3	c_4	k_1	k_2	k_3	r_1	r_2	r_3	r_4	M_i	u
2	4	1	2	3	3	4	16	14	5	7	1	7	3	5	1	1	7	5	13	1	5	2	4	2
		2	3	1				10	7	3	5	1	14	5	11	5	11	7	5	12	13	5	10	
		3	1	2				15	3	5	7	14	12	1	9	1	3	3	13	13	5	13	6	
		4	0	1				0	1	3	13	4	1	1	1	13	3	15	15	6	15	10	0	

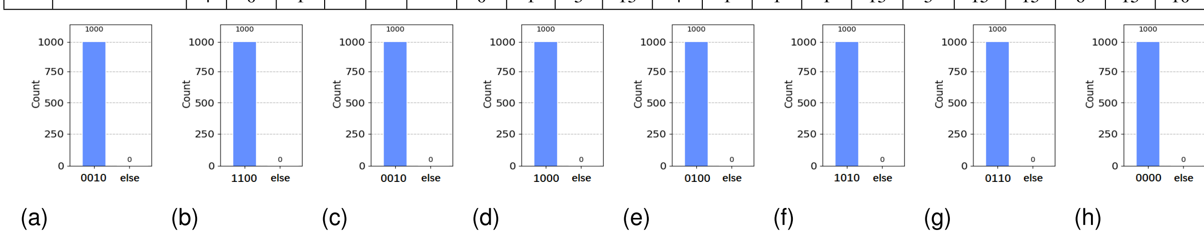

Fig. 4. a), b), c), d) are the results M_i for $i = 1, 2, 3, 4$ of the first experiment, respectively. Similarly, e), f), g), h) are the results of the second experiment.

in classical SMC. The complex matrix computation is mainly realized by generating product triples, among which cryptographic techniques such as oblivious transfer [45], [46], homomorphic encryption [47], [48], [49] and so on are widely used. We point out that since we have implemented a highly efficient two-party scalar product protocol, we no longer need to perform these computationally expensive processes. To our knowledge, this is the first quantum solution to solve this problem.

A. Proposed P2MM Protocol

Firstly, we provide a precise definition of the problem.

Definition 7 (Privacy-Preserving Two-Party Matrix Multiplication (P2MM)): Alice and Bob have two $k \times n$ matrix

$$\mathbf{A} = (a_{ij})_{k\times n} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{pmatrix} \tag{19}$$

This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination.

and $\mathbf{B} = (b_{ij})_{k\times n}$, respectively, where $a_{ij}, b_{ij} \in [N]$, $N = 2^m$. Alice is to get $\mathbf{U} = \mathbf{A}\cdot\mathbf{B}+\mathbf{V}$, while $\mathbf{V} = (v_{ij})_{k\times n}$, $v_{ij} \in [N]$ is a random matrix known only by Bob. Neither Alice nor Bob can get more information. Here we omit " mod N".

The main scheme for calculating the matrix product of two participants is as follows: By using the formula of matrix multiplication, the calculation of $k\times n$ matrices is transformed into kn times vector scalar product process, which are solved using our proposed S2QSP protocol.

Protocol 2: Privacy-preserving Two-party Quantum Matrix Multiplication Protocol (P2QMMP).

For each $1 \le i \le k, 1 \le j \le n$, Alice and Bob do the following steps:

Step 1 Alice separately extracts the i-th n-dimensional row vector of matrix $\mathbf{A}$, i.e.,

$$\mathbf{x}_i = (a_{i1}, a_{i2}, \cdots, a_{in}), \tag{20}$$

as her input vector.

Step 2 Similarly, Bob separately extracts the j-th n-dimensional column vector of matrix $\mathbf{B}$, i.e.,

$$\mathbf{y}_j = (b_{1j}, b_{2j}, \cdots, b_{nj}). \tag{21}$$

Then he takes out the element v_{ij} in the i-th row and j-column of matrix $\mathbf{V}$. The vector $\mathbf{y}_j$ and integer v_{ij} are his inputs.

Step 3 Now the two vectors $\mathbf{x}_i, \mathbf{y}_j$, and the random integer v_{ij} are valid inputs of Protocol 1. Alice and Bob execute Protocol 1, where parameter N, m and n are all set to the same as here.

Step 4 After all the steps of Protocol 1 are completed, Alice can obtain a corresponding result

$$Output_{ij} = \mathbf{x}_i \cdot \mathbf{y}_j + v_{ij}. \tag{22}$$

After executing $m\times n$ times the above steps, Alice now has $m\times n$ integers $Output_{ij}$, for $1 \le i \le k, 1 \le j \le n$. She now assembles the result matrix by these integers as

$$Output = (Output_{ij})_{k\times n}. \tag{23}$$

B. Protocol Analysis

1) Correctness:

$$\begin{aligned}
&Output\\
&= \begin{pmatrix} \mathbf{x}_1\cdot\mathbf{y}_1 + v_{11} & \cdots & \mathbf{x}_1\cdot\mathbf{y}_n + v_{1n}\\ \mathbf{x}_2\cdot\mathbf{y}_1 + v_{21} & \cdots & \vdots\\ \vdots & \ddots & \vdots\\ \mathbf{x}_k\cdot\mathbf{y}_1 + v_{k1} & \cdots & \mathbf{x}_k\cdot\mathbf{y}_n + v_{kn}\end{pmatrix}\\
&= \begin{pmatrix} \mathbf{x}_1\cdot\mathbf{y}_1 & \mathbf{x}_1\cdot\mathbf{y}_2 & \cdots & \mathbf{x}_1\cdot\mathbf{y}_n\\ \mathbf{x}_2\cdot\mathbf{y}_1 & \mathbf{x}_2\cdot\mathbf{y}_2 & \cdots & \vdots\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{x}_k\cdot\mathbf{y}_1 & \mathbf{x}_k\cdot\mathbf{y}_2 & \cdots & \mathbf{x}_k\cdot\mathbf{y}_n\end{pmatrix} + \mathbf{V}\\
&= \begin{pmatrix} \sum_{i=1}^n a_{1i}b_{i1} & \sum_{i=1}^n a_{1i}b_{i2} & \cdots & \sum_{i=1}^n a_{1i}b_{in}\\ \sum_{i=1}^n a_{2i}b_{i1} & \sum_{i=1}^n a_{2i}b_{i2} & \cdots & \vdots\\ \vdots & \vdots & \ddots & \vdots\\ \sum_{i=1}^n a_{ki}b_{i1} & \sum_{i=1}^n a_{ki}b_{i2} & \cdots & \sum_{i=1}^n a_{ki}b_{in}\end{pmatrix} + \mathbf{V}\\
&= \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n}\\ a_{21} & a_{22} & \cdots & \vdots\\ \vdots & \vdots & \ddots & \vdots\\ a_{k1} & a_{k2} & \cdots & a_{kn}\end{pmatrix}\cdot\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n}\\ b_{21} & b_{22} & \cdots & \vdots\\ \vdots & \vdots & \ddots & \vdots\\ b_{k1} & b_{k2} & \cdots & b_{kn}\end{pmatrix}\\
&\quad + \mathbf{V} = \mathbf{A}\cdot\mathbf{B} + \mathbf{V}.
\end{aligned} \tag{24}$$

2) Security:

Theorem 2: Protocol 2 has unconditional security under the malicious model.

Proof: For each $1 \le i \le k$, $1 \le j \le n$, Alice and Bob execute one time Protocol 1, and then Alice gets $Output_{ij} = \mathbf{x}_i \cdot \mathbf{y}_j + v_{ij}$, Bob only gets v_{ij}. Since Protocol 1 is secure enough with high probability (see Section IV-B), the result Alice can only obtain is $Output_{ij}$. Since $Output_{ij}$ is part of the result matrix $\mathbf{U}$, i.e. it can be regressed from $\mathbf{U}$, it does not provide any information beyond what Alice deserves. Similarly, Bob is unable to receive any improper benefits. Therefore, Protocol 2 is at least as secure as Protocol 1. ■

3) Performance: Obviously, the computational and communication complexity of Protocol 2 are $O(kn \cdot nm^2) = O(kn^2m^2)$ and $O(kn \cdot nm) = O(kmn^2)$, since Protocol 1 is executed kn times.

VI. Conclusion

In this paper, we propose a secure and efficient two-party quantum scalar product protocol, where several special properties of Fourier entangled states are used for calculation and security. Our protocol does not require any third parties, and has unconditional security under the malicious adversary model. It has polynomial level computational and communication complexity, which is the most efficient than the state-of-the-art protocols. Furthermore, based on the proposed S2QSP protocol, we present a privacy-preserving matrix multiplication protocol as its extended application.

However, because our protocol involves high-dimensional entangled states, it will be relatively fragile under noise. The transmission error may be reduced by high-dimensional error correction code. Besides, there is a future research direction on how to extend the protocol to multi-party scenario, which can achieve a wider application.

Declarations

- **Conflict of interest** The authors declare that they have no conflict of interest.
- **Ethical statement** Articles do not rely on clinical trials.
- **Data availability** Data sharing does not applicable to this article as no datasets were generated or analysed during the current study.

Appendix A
Proof of Lemmas

A. Proof of Lemma 1

Let's assume that there is an attacker who dose not know the values of X, C. He may perform any type of measurement on local system Q to obtain a measure result Z. First, we calculate the global density operator as

$$\begin{aligned}
\rho_{xc}^{(P,Q)} &= |\psi(x,c)\rangle\langle\psi(x,c)|_{(P,Q)}\\
&= \frac{1}{D}\sum_{j',j\in[D]} \omega^{(j'-j)h(x,c)} \left|f(j',x,c)\right\rangle\langle f(j,x,c)|_A\\
&\quad \left|g(j',x,c)\right\rangle\langle g(j,x,c)|_Q .
\end{aligned} \tag{25}$$

Remember $\langle f(j',x,c)|f(j,x,c)\rangle = \delta_{j'j}$. Then

$$\begin{aligned}\rho_{xc}^{Q} &= tr_P\left(\rho_{xc}^{(P,Q)}\right)\\ &= \frac{1}{D}\sum_{j',j\in[D]}\omega^{(j'-j)h(x,c)} tr\left(\left|f(j',x,c)\right\rangle\langle f(j,x,c)|_P\right)\\ &\quad \left|g(j',x,c)\right\rangle\langle g(j,x,c)|_Q\\ &= \frac{1}{D}\sum_{j',j\in[D]}\omega^{(j'-j)h(x,c)}\delta_{j'j}\left|g(j',x,c)\right\rangle\langle g(j,x,c)|_Q\\ &= \frac{1}{D}\sum_{j\in[D]}|g(j,x,c)\rangle\langle g(j,x,c)|_Q. \end{aligned} \tag{26}$$

In this formula functions $h(x,c)$, $f(j,x,c)$ disappear. Thus the attacker cannot obtain any phase-information. ■

B. Proof of Lemma 2

We first deduce a general upper bound of information disclosure. Follow Definition 1 and Lemma 1, then we have

Proposition 1 (Upper Bound of Information Disclosure): Under the attack described in Section A-A,

$$H(Z:X) \le \log_2|S_X| - \frac{\sum_{b\in[L]}\beta_b\log_2\beta_b - |S_X|\sum_{b\in[L]}\alpha_{bx}\log_2\alpha_{bx}}{D|S_X||S_C|}, \tag{27}$$

where $\alpha_{bx} = \left|g_x^{-1}(b)\right| = |\{(j,c)|g(j,x,c)=b\}|$ and $\beta_b = \left|g^{-1}(b)\right| = |\{(j,x,c)|g(j,x,c)=b\}|$.

Proof: As is deduced in Section A-A,

$$\rho_{xc}^{Q} = \frac{1}{D}\sum_{j\in[D]}|g(j,x,c)\rangle\langle g(j,x,c)|_Q. \tag{28}$$

Remember $p_x = \frac{1}{|S_X|}$, $p_c = \frac{1}{|S_C|}$. Then

$$\begin{aligned}\rho_x^Q &= \sum_{c\in S_C}\frac{1}{|S_C|}\rho_{xc}^Q\\ &= \frac{1}{|S_C|}\sum_{c\in S_C}\frac{1}{D}\sum_{j\in[D]}|g(j,x,c)\rangle\langle g(j,x,c)|_Q\\ &= \frac{1}{D|S_C|}\sum_{b\in[L]}\sum_{g(j,x,c)=b}|b\rangle\langle b|_Q\\ &= \frac{1}{D|S_C|}\sum_{b\in[L]}\alpha_{bx}|b\rangle\langle b|_Q. \end{aligned}\tag{29}$$

Remember that $g:[D]\times S_X\times S_C\to[L]$. Then we can get its Von Neumann entropy

$$\begin{aligned} S\left(\rho_x^Q\right) &= -\sum_{b\in[L]}\frac{\alpha_{bx}}{D|S_C|}\log_2\frac{\alpha_{bx}}{D|S_C|}\\ &= \sum_{b\in[L]}\frac{\alpha_{bx}}{D|S_C|}\left(\log_2(D|S_C|)-\log_2\alpha_{bx}\right)\\ &= \frac{\sum_{b\in[L]}\alpha_{bx}}{D|S_C|}\log_2(D|S_C|) - \frac{1}{D|S_C|}\sum_{b\in[L]}\alpha_{bx}\log_2\alpha_{bx}\\ &= \log_2(D|S_C|) - \frac{1}{D|S_C|}\sum_{b\in[L]}\alpha_{bx}\log_2\alpha_{bx}, \end{aligned}\tag{30}$$

where $\sum_{b\in[L]}\alpha_{bx} = |[D]\times S_C| = D|S_C|$. Now

$$\begin{aligned}\rho^Q &= \sum_{x\in S_X}\frac{1}{|S_X|}\rho_x^Q\\ &= \frac{1}{|S_X|}\sum_{x\in S_X}\frac{1}{|S_C|}\sum_{c\in S_C}\frac{1}{D}\sum_{j\in[D]}|g(j,x,c)\rangle\langle g(j,x,c)|_Q\\ &= \frac{1}{D|S_X||S_C|}\sum_{b\in[L]}\beta_b|b\rangle\langle b|_Q. \end{aligned}\tag{31}$$

Similar, its entropy is

$$\begin{aligned} S\left(\rho^B\right) &= -\sum_{b\in[L]}\frac{\beta_b}{D|S_X||S_C|}\log_2\frac{\beta_b}{D|S_X||S_C|}\\ &= \log_2(D|S_X||S_C|) - \frac{1}{D|S_X||S_C|}\sum_{b\in[L]}\beta_b\log_2\alpha_b, \end{aligned}\tag{32}$$

where $\sum_{b\in[L]}\beta_b = |[D]\times S_X\times S_C| = D|S_X||S_C|$. Now

$$\begin{aligned} &H(Z:X)\\ &\le S\left(\rho^B\right) - \sum_{x\in S_X}p_x S\left(\rho_x^B\right)\\ &= \log_2(D|S_X||S_C|) - \frac{1}{D|S_X||S_C|}\sum_{b\in[L]}\beta_b\log_2\alpha_b\\ &\quad - |S_X|\frac{1}{|S_X|}\left(\log_2(D|S_C|) - \frac{1}{D|S_C|}\sum_{b\in[L]}\alpha_{bx}\log_2\alpha_{bx}\right)\\ &= \log_2|S_X|\\ &\quad - \frac{\sum_{b\in[L]}\beta_b\log_2\beta_b - |S_X|\sum_{b\in[L]}\alpha_{bx}\log_2\alpha_{bx}}{D|S_X||S_C|}. \end{aligned}\tag{33}$$

By the Holevo bound [44]. ■

Now we can prove Lemma 2.

Proof: [Proof of Lemma 2] For convenience, we take the classical information $r_3 = r_1^{-1}$, $r_4 = c_1 - r_2 r_3$ as quantum information $|r_3\rangle_{e_1}|r_4\rangle_{e_2}$. Denote $\mathbf{c} = (c_1, c_2, c_3, c_4)$. Now Bob owns system $Q = (t_1, t_2, g, e_1, e_2)$, and we have a function

$$g_B(j, x_i, \mathbf{c}) = j + c_1 \parallel jp_i + c_2 \parallel jc_3 + c_4 \parallel r_1^{-1} \parallel c_1 - r_2 r_3, \tag{34}$$

and its value $b = b_1 \parallel b_2 \parallel b_3 \parallel r_3 \parallel r_4$, i.e.,

$$\begin{cases} j + c_1 = b_1\\ jp_i + c_2 = b_2\\ jc_3 + c_4 = b_3\\ (k_1 + p_i k_2 + c_3 k_3)^{-1} = r_3\\ c_1 - (k_1 c_1 + k_2 c_2 + k_3 c_4) r_3 = r_4, \end{cases}\tag{35}$$

or,

$$\begin{cases} c_1 = b_1 - j\\ c_2 = b_2 - jp_i\\ jc_3 + c_4 = b_3\\ k_3 c_3 = r_3^{-1} - k_1 - p_i k_2\\ \left(k_1 - r_3^{-1}\right)c_1 + k_2 c_2 + k_3 c_4 = -r_4 r_3^{-1}. \end{cases}\tag{36}$$

Take c_1, c_2, c_3, c_4 as unknowns. We have its augmented matrix as

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & b_1 - j \\ 0 & 1 & 0 & 0 & b_2 - jp_i \\ 0 & 0 & j & 1 & b_3 \\ 0 & 0 & k_3 & 0 & r_3^{-1} - k_1 - p_i k_2 \\ k_1 - r_3^{-1} & k_2 & 0 & k_3 & -r_4 r_3^{-1} \end{array}\right]. \tag{37}$$

It can be Gaussian eliminated to

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & b_1 - j \\ 0 & 1 & 0 & 0 & b_2 - jp_i \\ 0 & 0 & 1 & 0 & k_3^{-1}\left(r_3^{-1} - k_1 - p_i k_2\right) \\ 0 & 0 & 0 & 1 & b_3 - jk_3^{-1}\left(r_3^{-1} - k_1 - p_i k_2\right) \\ 0 & 0 & 0 & 0 & \left(k_1 - r_3^{-1}\right) b_1 + k_2 b_2 + k_3 b_3 + r_4 r_3^{-1} \end{array}\right]. \tag{38}$$

In order for the equation system to have a solution, there must be

$$\left(k_1 - r_3^{-1}\right) b_1 + k_2 b_2 + k_3 b_3 + r_4 r_3^{-1} = 0. \tag{39}$$

$\forall b_1, b_2, b_3 \in [D], r_3 \in [D]^o$, we have

$$r_4 = -r_3 \left[\left(k_1 - r_3^{-1}\right) b_1 + k_2 b_2 + k_3 b_3\right], \tag{40}$$

thus $|Im(g_B)| = D^3 \cdot \frac{D}{2} = \frac{D^4}{2}$. If (40) is satisfied, then the general solution of (36) is

$$\begin{cases} c_1 = b_1 - j \\ c_2 = b_2 - jp_i \\ c_3 = k_3^{-1}\left(r_3^{-1} - k_1 - p_i k_2\right) \\ c_4 = b_3 - jk_3^{-1}\left(r_3^{-1} - k_1 - p_i k_2\right). \end{cases} \tag{41}$$

We have $S_{x_i} = [N]$, $S_{\mathbf{c}} = [D]^3 \times [D]^o$. $\forall (j, x_i) \in [D] \times [N]$, we can uniquely identify a solution of $\mathbf{c}$ as above. Therefore, if $b \in Im(g_B)$, then $\alpha_{bx_i} = D$, $\beta_b = DN$; Otherwise, $\alpha_{bx_i} = \beta_b = 0$. By (27), we have

$$\begin{aligned} &H(Z_B : X_A) \\ &\quad \le \log_2 \left|S_{x_i}\right| \\ &\qquad - \frac{\sum_{b\in[L]} \beta_b \log_2 \beta_b - \left|S_{x_i}\right| \sum_{b\in[L]} \alpha_{bx_i} \log_2 \alpha_{bx_i}}{D\left|S_{x_i}\right| |S_{\mathbf{c}}|} \\ &\quad = \log_2 N - |Im(g_B)| \frac{DN \log_2 (DN) - ND \log_2 D}{DN \frac{D^4}{2}} \\ &\quad = m - (d+m) + d = 0. \end{aligned} \tag{42}$$

Therefore, we prove that $I_A = H(Z_B : X_A) = 0$, i.e., no information about x_i can be stolen.

On the other hand, if particle g is not involved, i.e., $c_3 = c_4 = 0$, then Bob has $k_1 + p_i k_2 = r_3^{-1}$, and gets $p_i = k_2^{-1}\left(r_3^{-1} - k_1\right)$. Therefore, its existence is necessary. ■

C. Proof of Lemma 3

Similar, we first need the following proposition.

Proposition 2 (Solution of Modular Multiplication Equation): Let $D = 2^d$, where d is a positive integer. Assume there are three random integers $a, b, c \in [D]$, where $a = 2^{d_1} w_1, b = 2^{d_2} w_2, c = 2^{d_3} w_3$, and $d_1, d_2, d_3 \in [d+1], w_i \in \left[2^{d-d_i}\right]^o$. Denote $0 = D = 2^d \times 1$. We have

1) The necessary and sufficient condition for $ab \equiv c(\bmod D)$ is: $d_1 + d_2 \ge d_3$ if $d_3 = d$; $d_1 + d_2 = d_3$ and $w_1 w_2 \equiv w_3(\bmod 2^{d-d_3})$ if $d_3 < d$.
2) Given a, c, select b randomly, denote $p = \Pr(ab \equiv c(\bmod D))$. Then, $p = \frac{1}{2^{d-d_1}}$ if $d_3 \ge d_1$; $p = 0$ if $d_3 < d_1$.

Proof:

1) $ab \equiv c(\bmod D)$ is equivalent to $2^{d_1+d_2} w_1 w_2 = 2^{d_3} w_3 + k2^d$, where k is an integer. If $d_3 = d$, then $w_3 = 1$, and $2^{d_1+d_2} w_1 w_2 = (k+1)2^d$, $d_1 + d_2 \ge d$; conversely, if $d_1 + d_2 \ge d$, then $2^{d_1+d_2} w_1 w_2 = (k+1)2^d \equiv c(\bmod D)$. If $d_3 < d$, then $2^{d_1+d_2} w_1 w_2 = 2^{d_3}\left(w_3 + k2^{d-d_3}\right)$, where $w_3 + k2^{d-d_3}$ is odd. Therefore,we have $d_1 + d_2 = d_3$, $w_1 w_2 = w_3 + k2^{d-d_3}$, i.e., $w_1 w_2 \equiv w_3(\bmod 2^{d-d_3})$.
2) a) If $d_3 = d$, then

$$\begin{aligned} p_1 &= \Pr(ab \equiv c(\bmod D) | d = d_3) \\ &= \Pr(d_1 + d_2 \ge d_3) = \Pr(d_2 \ge d - d_1) \\ &= \Pr\left(2^{d-d_1} | b\right) = \frac{2^{d-(d-d_1)}}{2^d} = \frac{1}{2^{d-d_1}}. \end{aligned} \tag{43}$$

Note that there are $2^{d-(d-d_1)}$ multiples of 2^{d-d_1} in $[D]$.
b) If $d > d_3 \ge d_1$, the conditions are $d_2 = d_3 - d_1$ and $w_2 \equiv w_1^{-1} w_3(\bmod 2^{d-d_3})$, where $w_1^{-1} \in \left[2^{d-d_3}\right]^o$ is the multiplicative inverse of $w_1 \bmod 2^{d-d_3}$. First, $d_2 = d_3 - d_1$ means that $2^{d_3-d_1} | b$ and $2^{d_3-d_1+1} \nmid b$. Of the $2^{d-(d_3-d_1)}$ multiples of $2^{d_3-d_1}$, half are multiples of $2^{d_3-d_1+1}$, thus

$$\begin{aligned} p_{2a} &= \Pr(d_2 = d_3 - d_1) \\ &= \frac{2^{d-(d_3-d_1)} 2^{-1}}{2^d} = \frac{1}{2^{d_3-d_1+1}}, \end{aligned} \tag{44}$$

If $d_2 = d_3 - d_1$, we need

$$w_2 = w_1^{-1} w_3 + k2^{d-d_3} \in \left[2^{d-d_3+d_1}\right]^o, \tag{45}$$

i.e., $1 \le w_1^{-1} w_3 + k2^{d-d_3} \le 2^{d-d_3+d_1} - 1$. No matter how much $w_1^{-1} w_3$ equals, we can assume that

$$l2^{d-d_3} + 1 \le w_1^{-1} w_3 \le (l+1)2^{d-d_3} - 1, \tag{46}$$

where l is an integer. Then, we can deduce that

$$\begin{aligned} &-(l+1)2^{d-d_3} + 1 \le -w_1^{-1} w_3 \le k2^{d-d_3} \\ &\le 2^{d-d_3+d_1} - 1 - w_1^{-1} w_3 \le 2^{d-d_3+d_1} - 1 - l2^{d-d_3} - 1 \\ &= 2^{d-d_3}(2^{d_1} - l) - 2, \end{aligned} \tag{47}$$

thus $-l \le k \le 2^{d_1} - l - 1$, i.e., k has 2^{d_1} possible values. Then

$$\begin{aligned} p_{2b} &= \Pr\left(w_2 = w_1^{-1} w_3 + k2^{d-d_3} | d_2 = d_3 - d_1\right) \\ &= \frac{2^{d_1}}{2^{d-d_3+d_1-1}} = \frac{1}{2^{d-d_3-1}}. \end{aligned} \tag{48}$$

Note that there are half odd integers in $\left[2^{d-d_3+d_1}\right]$. Now

$$\begin{aligned} p_2 &= \Pr(ab \equiv c(\bmod D) | d > d_3 \ge d_1) = p_{2a} \cdot p_{2b} \\ &= \frac{1}{2^{d_3-d_1+1}} \cdot \frac{1}{2^{d-d_3-1}} = \frac{1}{2^{d-d_1}} = p_1. \end{aligned} \tag{49}$$

Thus $p = p_1 = p_2 = \frac{1}{2^{d-d_1}}$.

c) If $d_3 < d_1$, then $d_1 + d_2 \neq d_3$, thus $p = 0$.

In total, we prove this proposition. ■

Now we can prove Lemma 3.

Proof: [Proof of Lemma 3:] There are three possible cases:

a) Using t_1 to steal s_i and t_2 to steal q_i simultaneously.

Assume that Alice prepares $\frac{1}{\sqrt{D}}\sum_{j\in[D]}|j\rangle_{t_1}$, $\frac{1}{\sqrt{D}}\sum_{j\in[D]}|j\rangle_{t_2}$. For convenience, we set h, g in $|0\rangle$, since they are used to protect herself, not Bob. In Step 2 of Operation stage, the state will be

$$\begin{aligned}&\frac{1}{D}\sum_{j,j'\in[D]}|j\rangle_{t_1}\left|j'\right\rangle_{t_2}|0\rangle_g\\ &\quad\to\frac{1}{D}\sum_{j,j'\in[D]}|jk\rangle_{t_1}\left|j'\right\rangle_{t_2}\left|jk_1+j'k_2\right\rangle_g.\end{aligned}\tag{50}$$

Now t_1, t_2, g are entangled. In Step 4 of Operation stage, no matter what value r_3, r_4 she sends are, the total state will be

$$\begin{aligned}&\frac{1}{D}\sum_{j,j'\in[D]}\omega^{js_i+j'q_i}|j\rangle_{t_1}\left|j'\right\rangle_{t_2}\left|jk_1+j'k_2\right\rangle_g\\ &\quad\to\frac{1}{\sqrt{D}}\sum_{j\in[D]}\omega^{js_i}|j\rangle_{t_1}\frac{1}{\sqrt{D}}\sum_{j'\in[D]}\omega^{j'q_i}\\ &\qquad\left|j'\right\rangle_{t_2}\left|(jk_1r_3+j'k_2r_3+r_4)\oplus j\right\rangle_g.\end{aligned}\tag{51}$$

Now Bob will measure g. For each $j \in [D]$, we have

$$\begin{aligned}&\Pr\left((jk_1r_3+j'k_2r_3+r_4)\oplus j=0\right)\\ &\quad=\Pr\left(jk_1r_3+j'k_2r_3+r_4=j\right)\\ &\quad=\Pr\left(j'=(k_2r_3)^{-1}(j(1-k_1r_3)-r_4)\right)=\frac{1}{D}.\end{aligned}\tag{52}$$

Thus, he will find Alice's attack easily, with probability $1-\frac{1}{D}$.

b) Using t_1 to steal s_i only.

Similarly, Alice prepares $\frac{1}{\sqrt{D}}\sum_{j\in[D]}|j\rangle_{t_1}$, $|0\rangle_{t_2}$, $|0\rangle_g$. In Step 2 of Operation stage, it will be

$$\frac{1}{\sqrt{D}}\sum_{j\in[D]}|j\rangle_{t_1}|0\rangle_{t_2}|0\rangle_g\to\frac{1}{\sqrt{D}}\sum_{j\in[D]}|j\rangle_{t_1}|0\rangle_{t_2}|jk_1\rangle_g,\tag{53}$$

and in Step 4 of Operation stage, it will be

$$\begin{aligned}&\frac{1}{\sqrt{D}}\sum_{j\in[D]}\omega^{js_i}|j\rangle_{t_1}|jk_1\rangle_g\\ &\quad\to\frac{1}{\sqrt{D}}\sum_{j\in[D]}\omega^{js_i}|j\rangle_{t_1}|(jk_1r_3+r_4)\oplus j\rangle_g.\end{aligned}\tag{54}$$

When Bob measure g, he will get $|0\rangle$ if $jk_1r_3+r_4 = j$, i.e., $j(1-k_1r_3) = r_4$. Let $S_J = \{j \mid j(1-k_1r_3) = r_4,\ j \in [D]\}$. Bob can find the cheating with probability $1-\frac{|S_J|}{D}$, and ignore it with $\frac{|S_J|}{D}$. If he ignores, the state of t_1 will be

$$\left|\psi_{s_i}\right\rangle=\frac{1}{\sqrt{|S_J|}}\sum_{j\in S_J}\omega^{js_i}|j\rangle.\tag{55}$$

t_1 will return to Alice in Step 5 of Operation stage. Now the density operator is

$$\rho_{s_i}=\left|\psi_{s_i}\right\rangle\left\langle\psi_{s_i}\right|=\frac{1}{|S_J|}\sum_{j',j\in S_J}\omega^{(j'-j)s_i}\left|j'\right\rangle\langle j|\tag{56}$$

Since $\rho_{s_i} = \left|\psi_{s_i}\right\rangle\left\langle\psi_{s_i}\right|$, $S\left(\rho_{s_i}\right) = 0$. For Alice who has no knowledge of odd integer $s_i = 4v_i - 2y_i - 1 \bmod D$, s_i can be considered to follow the uniform distribution on $[D]^o$, i.e., $p_{s_i} = \frac{2}{D}$. Let $s_i = 2a + 1$, then the total operator is

$$\begin{aligned}\rho&=\sum_{s_i\in[D]^o}\frac{2}{D}\rho_{s_i}\\ &=\frac{2}{D|S_J|}\sum_{j\in S_J}\sum_{j'\in S_J}\sum_{s_i\in[D]^o}\omega^{(j'-j)s_i}\left|j'\right\rangle\langle j|.\end{aligned}\tag{57}$$

Note that if $j' = j$ then $\sum_{s_i\in[D]^o}\omega^{(j'-j)s_i} = \frac{D}{2}$; Or, if $j' - j \equiv \frac{D}{2}(\bmod D)$, then

$$\sum_{s_i\in[D]^o}\omega^{(j'-j)s_i}=\sum_{s_i\in[D]^o}e^{\iota\pi s_i}=\sum_{s_i\in[D]^o}(-1)=-\frac{D}{2};\tag{58}$$

Otherwise,

$$\begin{aligned}\sum_{s_i\in[D]^o}\omega^{(j'-j)s_i}&=\sum_{a\in\left[\frac{D}{2}\right]}e^{\frac{\iota 2\pi}{D}\cdot(j'-j)(2a+1)}\\ &=\omega^{j'-j}\sum_{a\in\left[\frac{D}{2}\right]}e^{\frac{\iota 2\pi}{D}\cdot 2(j'-j)a}\\ &=\omega^{j'-j}\frac{1-e^{\iota 2\pi(j'-j)}}{1-e^{\frac{\iota 2\pi}{D}\cdot 2(j'-j)}}\\ &=0.\end{aligned}\tag{59}$$

Since k_1r_3 is odd, we have $D|(1-k_1r_3)\frac{D}{2}$, thus

$$(1-k_1r_3)\left(j+\frac{D}{2}\right)\equiv(1-k_1r_3)j\equiv r_4(\bmod D).\tag{60}$$

I.e., if $j \in S_J$ then $j + \frac{D}{2} \bmod D \in S_J$. Now we can calculate the eigenvalue of ρ. By (57), we have

$$\rho=\frac{1}{|S_J|}\sum_{j\in S_J}\left(|j\rangle-\left|j+\frac{D}{2}\right\rangle\right)\langle j|.\tag{61}$$

$\forall j \in S_J$, denote $\left|\phi_{j\pm}\right\rangle = |j\rangle \pm \left|j+\frac{D}{2}\right\rangle$, then

$$\rho\left|\phi_{j+}\right\rangle=0\left|\phi_{j+}\right\rangle,\ \rho\left|\phi_{j-}\right\rangle=\frac{2}{|S_J|}\left|\phi_{j+}\right\rangle.\tag{62}$$

I.e., ρ has $\frac{|S_J|}{2}$ non-zero eigenvalues $\frac{2}{|S_J|}$. Then

$$S(\rho)=-\frac{|S_J|}{2}\cdot\frac{2}{|S_J|}\log_2\frac{2}{|S_J|}=\log_2|S_J|-1.\tag{63}$$

If Alice measures t_1 to obtain any result Z_A, then

$$\begin{aligned}&H\left(Z_A:s_i|\text{Alice passes the test}\right)\\ &\quad\le S(\rho)-\sum_{s_i\in[D]^o}p_{s_i}S\left(\rho_{s_i}\right)=\log_2|S_J|-1\end{aligned}\tag{64}$$

Since the probability she pass Bob's honesty test is $\frac{|S_J|}{D}$, then the leakage degree of Bob's privacy, i.e., the average information Alice obtains is

$$I_B=H(Z_A:s_i)\le\sum_{|S_J|}\frac{|S_J|}{D}p_{|S_J|}\log_2|S_J|-1.\tag{65}$$

Let's find $p_{|S_J|}$. Let $1-k_1k_3 = 2^{d_l}w_l$, $r_4 = 2^{d_r}w_r$, $j = 2^{d_j}w_j$. By Proposition 2, $j(1-k_1r_3) = r_4$ only if $d_r \geq d_l$, with probability $\frac{1}{2^{d-d_l}}$, i.e., $|S_J| = \frac{2^d}{2^{d-d_l}} = 2^{d_l}$; Otherwise, if $d_r < d_l$, then $|S_J| = 0$. To maximize I_B, Alice should set $d_r = d$, i.e., $r_4 = 0$, so that $d_r \geq d_l$ always holds. Note that $1-k_1r_3$ is a random even, if $d_l < d$, then

$$p_{|S_J|} = \Pr\left(2^{d_l}|(1-k_1r_3),\ \ 2^{d_l+1} \nmid (1-k_1r_3)\right) = \frac{2^{d-d_l-1}}{2^{d-1}} = \frac{1}{2^{d_l}}; \tag{66}$$

If $d_l = d$, then $1-k_1r_3 = 0$, and $p_{|S_J|} = \frac{2}{2^{d-1}}$. Therefore,

$$p_{|S_J|} = \begin{cases} \dfrac{1}{|S_J|}, & \text{if } |S_J| < D \\ \dfrac{2}{|S_J|}, & \text{if } |S_J| = D. \end{cases} \tag{67}$$

Now by (65), we have

$$\begin{aligned} I_B &\leq \sum_{|S_J|} \frac{|S_J|}{D} p_{|S_J|} \log_2 |S_J| - 1 \\ &= \sum_{d_l=1}^{d-1} \frac{2^{d_l}}{D} \cdot \frac{1}{2^{d_l}} \left(\log_2 2^{d_l} - 1\right) \\ &\quad + \frac{2^d}{D} \cdot \frac{2}{2^d} \left(\log_2 2^d - 1\right) \\ &= \frac{1}{D} \sum_{d_l=1}^{d-1} (d_l - 1) + \frac{2}{D}(d-1) \\ &= \frac{1}{D} \frac{(d-1)(d-2) + 4(d-1)}{2} \\ &= \frac{1}{D} \frac{(d-1)(d+2)}{2} = \frac{d^2+d-2}{2 \cdot 2^d} = O\left(\frac{d^2}{2^d}\right). \end{aligned} \tag{68}$$

c) Using t_2 to steal q_i only.
This case is almost identical to b). We can calculate the total density operator $\rho = \sum_{y_i \in [N]} \frac{1}{N} \rho_y$, and find that the upper bound in this case equals to the one in b) if $1-k_2r_3 \not\equiv 0(\bmod D)$, because if $j - j' \equiv \text{odd}(\bmod D)$, then j, j' cannot satisfy $j(1-k_2r_3) \equiv r_4(\bmod D)$ at the same time. In this case, we have $I_B = H(Z_A : s_i) = O\left(\frac{d^2}{2^d}\right)$.
If $1-k_2r_3 \equiv 0(\bmod D)$ with probability $\frac{2}{D}$, we can deduce a new upper bound d, since at most d bits of classical information can be extracted from the d-qubit state [42]. Considering the probability $\frac{1}{2^{d-1}}$, the average upper bound is

$$I_B \leq \left(1 - \frac{1}{2^{d-1}}\right) O\left(\frac{d^2}{2^d}\right) + \frac{1}{2^{d-1}} d \leq O\left(\frac{d^2}{2^d}\right). \tag{69}$$

In total, the leakage degree of Bob's privacy is $I_B = O\left(\frac{d^2}{2^d}\right)$, where the asymptotic coefficient is $\frac{1}{2}$. ∎

D. Proof of Lemma 4

Denote random variables $M = (M_1, M_2, \cdots, M_n)$ and $X_B = (\mathbf{y}, v)$. At first, we have [43]

$$I_B = H(M : X_B|u) = H(X_B : M, u) - H(X_B : u). \tag{70}$$

Since u is a function of X_B (and M, since Alice can calculate u only with M), we have $H(X_B : u) = H(u)$, $H(u|X_B) = 0$ and $H(M,u) = H(M)$ (Theorem 11.3 of Ref. [42]). By the chaining rule for conditional entropies (Theorem 11.4 of Ref. [42]), $H(M,u|X_B) = H(u|M,X_B) + H(M|X_B) = H(M,X_B) - H(X_B)$. Then

$$\begin{aligned} I_B &= H(M : X_B|u) = H(X_B : M, u) - H(X_B : u) \\ &= H(M,u) - H(M,u|X_B) - H(u) \\ &= H(M) - H(M,X_B) + H(X_B) - H(u) \\ &= H(X_B) - H(X_B|M) - H(u). \end{aligned} \tag{71}$$

Note that $\hat{M}_i \equiv M_i - 2x_i \equiv 4v_i + 4x_iy_i(\bmod D)$ and M_i correspond one-to-one, then $H(X_B|\hat{M}) = H(X_B|M)$, where $\hat{M} = (\hat{M}_1, \cdots, \hat{M}_n)$. $\forall \hat{M}_i \in 4[N]$, $y_i \in [N]$, only if v_i satisfy $4v_i \equiv \hat{M}_i - 4x_iy_i(\bmod D)$, $4v \equiv 4\sum_{i=1}^n v_i(\bmod D)$ is valid. Therefore, there is only one possible $4v \in [D]$, and thus one $v \in [N]$. Then we have $p(X_B|\hat{M}) = \frac{1}{N^n}$. On the other hand, $\forall y_i, v \in [N]$, if $v_1, v_2, \cdots, v_{n-1} \in [N]$ have been selected, then $4v_n \equiv 4v - 4\sum_{i=1}^{n-1} v_i(\bmod D)$ is determined, and so is $\hat{M}$. Therefore, $p(\hat{M}|X_B) = \frac{1}{N^{n-1}}$. By $p(X_B) = \frac{1}{N^{n+1}}$, we have

$$\begin{aligned} &H(X_B|\hat{M}) \\ &= -\sum_{X_B \in [N]^{n+1}} \sum_{\hat{M} \in 4[N]^n} p(X_B, \hat{M}) \log_2 p(X_B|\hat{M}) \\ &= -\sum_{X_B \in [N]^{n+1}} \sum_{v_1, v_2, \cdots, v_{n-1} \in [N]} p(\hat{M}|X_B) p(X_B) \log_2 p(X_B|\hat{M}) \\ &= -N^{n+1} N^{n-1} \frac{1}{N^{n-1}} \frac{1}{N^{n+1}} \log_2 \frac{1}{N^n} = nm. \end{aligned} \tag{72}$$

Similarly, because $\forall u \in [N]$, we can randomly select $\mathbf{y} \in [N]^n$, then $v = u - \mathbf{x} \cdot \mathbf{y}$. That is, each u corresponds to N possible values of y, i.e., $p(u) = \frac{1}{N}$. Then $H(X_B) = (n+1)m$, $H(u) = m$, and $I_B = (n+1)m - nm - m = 0$. ∎

Appendix B
Implementation of Quantum Gates

Here we analyze the complexity of the quantum operations we used, and how to implement them in simulation.

A. Complexity Analysis

1) As shown in figure 2(a), A $\mathcal{QFT}$ (or $\mathcal{QFT}^\dagger$) gate can be decomposed into $O\left(d^2\right)$ $\mathcal{H}$ and $\mathcal{CP}$ gates [42].
2) Let $a = \sum_{i \in [d]} a_i 2^i$, $b = \sum_{k \in [d]} b_k 2^k$. As shown in figure 2(b), we have $\mathcal{ROT}_h = \prod_{i,k \in [d]} \mathcal{P}(i+k)_{h_i}^{b_i}$, where b_i means the controlling bit, i.e., if $b_i = 1$, perform $\mathcal{P}(i+k)_{h_i}$, otherwise do nothing. Because

$$\begin{aligned} \prod_{i,k \in [d]} \mathcal{P}(i+k)_{h_i}^{b_i} |a\rangle_h &= \prod_{i,k \in [d]} e^{\frac{\imath 2\pi 2^{i+k} a_i b_i}{D}} |a\rangle_h \\ &= e^{\frac{\imath 2\pi \sum_{i,k \in [d]} 2^{i+k} a_i b_i}{D}} |a\rangle_h = e^{\frac{\imath 2\pi ab}{D}} |a\rangle_h \\ &= \mathcal{ROT}_h |a\rangle_h. \end{aligned} \tag{73}$$

Thus, the complexity of $\mathcal{ROT}$ gate is also $O\left(d^2\right)$.
3) As elementary arithmetic gates, the complexity of $\mathcal{SUM}$ and $\mathcal{BSUM}$ are both $O(d)$, if we only use $\mathcal{T}$ and $\mathcal{CNOT}$ gates corresponding to classical AND and XOR gate. Generally, it requires an auxiliary qubit as a carrier.
4) To realize $\mathcal{MUL}$, introduce an auxiliary register $|0\rangle_t$, then

$$|a\rangle_h |0\rangle_t \xrightarrow{\mathcal{SUM}(2^0 b)_t^{h_0}} |a\rangle_h \left|2^0 a_0 b\right\rangle_t \xrightarrow{\mathcal{SUM}(2^1 b)_t^{h_1}}$$

$$\cdots \xrightarrow{\mathcal{SUM}(2^{d-1}b)_t^{h_{d-1}}} = |a\rangle_h |ab\rangle_t , \tag{74}$$

where $\mathcal{SUM}^{h_i}$ means $\mathcal{SUM}$ is controlled by qubit h_i. We denote the above gate as $\mathcal{BMUL}(b)_{(h,t)}$. To realize $\mathcal{MUL}$, use $\mathcal{SWAP}_{(h,t)} = \mathcal{XOR}_{(h,t)}\mathcal{XOR}_{(t,h)}\mathcal{XOR}_{(h,t)} : |a\rangle_h |b\rangle_t \rightarrow |b\rangle_h |a\rangle_t$. Then

$$\begin{aligned} &|a\rangle_h |0\rangle_t \xrightarrow{\mathcal{BMUL}(b)_{(h,t)}} |a\rangle_h |ab\rangle_t \xrightarrow{\mathcal{BMUL}(-b^{-1})_{(t,h)}} \\ &|0\rangle_h |ab\rangle_t \xrightarrow{\mathcal{SWAP}_{(h,t)}} |ab\rangle_h |0\rangle_t , \end{aligned} \tag{75}$$

as Shor described [50]. Its complexity is $O(d^2)$.

5) Obviously, an $\mathcal{XOR}$ gate can decomposed into d $\mathcal{CNOT}$ gates, as shown in figure 2(f). Thus its complexity is $O(d)$.

B. Implementation of Quantum Gates

To save valuable qubit resources, we use Draper's Transform Adder [41] to implement $\mathcal{SUM}$ and $\mathcal{BSUM}$. It need no auxiliary qubits, but increases the complexity. In this method, we have $\mathcal{SUM}(b) = \mathcal{QFT}^{\dagger}\mathcal{ROT}(b)\mathcal{QFT}$ and $\mathcal{BSUM}_{(h,t)} = \mathcal{QFT}_t^{\dagger}\mathcal{BROT}_{(h,t)}\mathcal{QFT}_t$, with complexity $O(d^2)$. The gate $\mathcal{BROT}$ is defined as $\mathcal{BROT}_{(h,t)} : |a\rangle_h |b\rangle_t \rightarrow \omega^{ab} |a\rangle_h |b\rangle_t$, by replacing $\mathcal{P}(i+k)_{h_i}^{b_i}$ with $\mathcal{CP}(i+k)_{(h_i,t_i)}$ in $\mathcal{ROT}_h$. The circuit of them are shown in figure 2(c) and 2(e) respectively.

In addition, the general $\mathcal{MUL}$ gate needs $O(d)$ auxiliary qubits. Here we point out that for the special modulus $D = 2^d$, we can design a special circuit which requires no auxiliary qubits. To illustrate our design idea, we first define a new gate $\mathcal{SUM}(b \bmod 2^l)$ as a $\bmod 2^l$ summation gate on register $(h_{d-1}, h_{d-2}, \cdots, h_{d-l})$. E.g., $\mathcal{SUM}(b \bmod 2^2)$ will change $|a_{d-1}\rangle |a_{d-2}\rangle$ to $\left|\sum_{i\in[2]} 2^i a_{i+d-2} + b \bmod 2^2\right\rangle$. Denote $w = \frac{b-1}{2}$ (must be an integer). We have

$$\begin{aligned} \mathcal{MUL}(b) = {} & \mathcal{SUM}(w \bmod 2^{d-1})^{h_0}\mathcal{SUM}(w \bmod 2^{d-2})^{h_1} \\ & \cdots \mathcal{SUM}(w \bmod 2^2)^{h_{d-3}}\mathcal{SUM}(w \bmod 2^1)^{h_{d-2}}, \end{aligned} \tag{76}$$

as shown in figure 2(d). Now we prove its correctness.

Proof: We have

$$\begin{aligned} ab &\equiv a(2w+1) \equiv a + 2w\sum_{i=0}^{d-1} 2^i a_i \\ &\equiv a + \sum_{i=1}^{d} 2^i w a_{i-1} (\bmod 2^d) \\ &\equiv a + \sum_{i=1}^{d-1} 2^i w a_{i-1} (\bmod 2^d). \end{aligned} \tag{77}$$

Let $a^{(0)} = a$ and $a^{(l+1)} = a^{(l)} + w a_{d-1-l} 2^{d-l} \bmod D$, then we have $a^{(d)} = a^{(d-1)} + w a_0 2^0 \bmod D = ab$. Let $a^{(l+1)} = \sum_{i=0}^{d-1} a_i^{(l+1)} 2^i$, $a^{(l)} = \sum_{i=0}^{d-1} a_i^{(l)} 2^i$, then

$$\begin{aligned} \sum_{i=0}^{d-1} a_i^{(l+1)} 2^i &= a^{(l)} + w a_{d-1-l} 2^{d-l} \bmod D \\ &= \sum_{i=0}^{d-1} a_i^{(l)} 2^i + w a_{d-1-l} 2^{d-l} \bmod D \\ &= \sum_{i=0}^{d-l-1} a_i^{(l)} 2^i + \sum_{i=d-l}^{d-1} a_i^{(l)} 2^i + w a_{d-1-l} 2^{d-l} - k2^d \\ &= \sum_{i=0}^{d-l-1} a_i^{(l)} 2^i + 2^{d-l}\left(\sum_{i=0}^{l-1} a_{i+d-l}^{(l)} 2^l + w a_{d-1-l} - k2^l\right) \\ &= \sum_{i=0}^{d-l-1} a_i^{(l)} 2^i \\ &\quad + 2^{d-l}\left(\sum_{i=0}^{l-1} a_{i+d-l}^{(l)} 2^l + w a_{d-1-l} \bmod 2^l\right), \end{aligned} \tag{78}$$

where k is integer. Note that $a_i^{(l+1)} = a_i^{(l)}$, $0 \le i \le d-l-1$, thus

$$\begin{aligned} \sum_{i=0}^{d-l-1} a_i^{(l+1)} 2^i &= \sum_{i=0}^{d-l-1} a_i^{(l)} 2^i \\ &= \cdots = \sum_{i=0}^{d-l-1} a_i^{(0)} 2^i = \sum_{i=0}^{d-l-1} a_i 2^i. \end{aligned} \tag{79}$$

Therefore,

$$\begin{aligned} a^{(l+1)} = {} & \sum_{i=0}^{d-l-1} a_i^{(l)} 2^i \\ & + 2^{d-l}\left(\sum_{i=0}^{l-1} a_{i+d-l}^{(l)} 2^l + w a_{d-1-l}^{(l)} \bmod 2^l\right), \end{aligned} \tag{80}$$

which means that we can add w on $|a_{d-1}\rangle \cdots |a_{d-l}\rangle \bmod 2^l$ if $a_{d-l-1} = 1$, for each $l = 0, 1, \cdots, d-1$. That's why (76) and the circuit in figure 2(d) are correct. ∎

Acknowledgment

The opinions expressed here are entirely that of the authors. No warranty is expressed or implied. User assumes all risk.

References

[1] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci.*, Chicago, IL, USA, Nov. 1982, pp. 160–164.

[2] A. C. Yao, "How to generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci.*, Toronto, ON, Canada, Oct. 1986, pp. 162–167.

[3] S. Even, O. Goldreich, and A. Lempel, "A randomized protocol for signing contracts," *Commun. ACM*, vol. 28, no. 6, pp. 637–647, Jun. 1985.

[4] G. Brassard, C. Crepeau, and J.-M. Robert, "All-or-nothing disclosure of secrets," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Heidelberg, Germany, 1987, pp. 234–238.

[5] C. Peikert, V. Vaikuntanathan, and B. Waters, "A framework for efficient and composable oblivious transfer," in *Proc. Annu. Int. Cryptol. Conf.*, Berlin, Heidelberg, Germany, 2008, pp. 554–571.

[6] O. Goldreich, S. Micali, and A. Wigderson, "How to play any mental game," in *Proc. 19th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, 1987, pp. 218–229.

[7] M. Ben-Or, S. Goldwasser, and A. Wigderson, "Completeness theorems for non-cryptographic fault-tolerant distributed computation," in *Proc. 20th Annu. ACM Symp. Theory Comput.*, 1988, pp. 351–371.

[8] D. Beaver, "Efficient multiparty protocols using circuit randomization," in *Proc. Adv. Cryptol. (CRYPTO)*, Berlin, Heidelberg, Germany, 1992, pp. 420–432.

[9] L. Xiong, W. Zhou, Z. Xia, Q. Gu, and J. Weng, "Efficient privacy-preserving computation based on additive secret sharing," 2020, *arXiv:2009.05356*.

[10] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 469–472, Jul. 1985.

[11] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proc. Adv. Cryptol. (EUROCRYPT)*, Berlin, Heidelberg, Germany, 1999, pp. 223–238.

[12] D. Ivan, G. Martin, and K. Mikkel, "Homomorphic encryption and secure comparison," *Int. J. Appl. Cryptogr.*, vol. 1, no. 1, pp. 22–31, 2008.

[13] H. Huang, T. Gong, P. Chen, R. Malekian, and T. Chen, "Secure two-party distance computation protocol based on privacy homomorphism and scalar product in wireless sensor networks," *Tsinghua Sci. Technol.*, vol. 21, no. 4, pp. 385–396, Aug. 2016.

[14] H. Zhu, F. Wang, R. Lu, F. Liu, G. Fu, and H. Li, "Efficient and privacy-preserving proximity detection schemes for social applications," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2947–2957, Aug. 2018.

[15] S. K. Shen, B. Yang, K. G. Qian, Y. M. She, and W. Wang, "On improved DV-Hop localization algorithm for accurate node localization in wireless sensor networks," *Chin. J. Electron.*, vol. 28, no. 3, pp. 658–666, 2019.

[16] W. L. Du and M. J. Atallah, "Privacy-preserving cooperative statistic analysis," in *Proc. Annu. Comput. Secur. Appl. Conf.*, New Orleans, LA, USA, 2001, pp. 102–110.

[17] J. Vaidya and C. Clifton, "Privacy preserving association rule mining in vertically partitioned data," in *Proc. 8th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining*, Jul. 2002, pp. 639–644.

[18] B. Goethals, S. Laur, H. Lipmaa, and T. Mielikäinen, "On private scalar product computation for privacy-preserving data mining," in *Proc. Inf. Secur. Cryptol. (ICISC)*, Berlin, Heidelberg, Germany, 2005, pp. 104–120.

[19] D. H. Tran, W. K. Ng, H. W. Lim, and H. L. Nguyen, "An efficient cacheable secure scalar product protocol for privacy-preserving data mining," in *Proc. Data Warehousing Knowl. Discovery*, Berlin, Heidelberg, Germany, 2011, pp. 354–366.

[20] M. J. Atallah and W. Du, "Secure multi-party computational geometry," in *Proc. 7th Int. Workshop Algorithms Data Struct.*, Providence, RI, USA, 2001, pp. 165–179.

[21] T. Thomas, "Secure two-party protocols for point inclusion problem," *Int. J. Netw. Secur.*, vol. 9, no. 1, pp. 1–7, 2009.

[22] B. Yang, Z. Shao, and W. Zhang, "Secure two-party protocols on planar convex hulls," *J. Inf. Comput. Sci.*, vol. 9, no. 4, pp. 915–929, 2012.

[23] W. Liu, Y. Xu, J. C. N. Yang, W. Yu, and L. Chi, "Privacy-preserving quantum two-party geometric intersection," *Comput., Mater. Continua*, vol. 60, no. 3, pp. 1237–1250, 2019.

[24] L. Li and R.-H. Shi, "A novel and efficient quantum private comparison scheme," *J. Korean Phys. Soc.*, vol. 75, no. 1, pp. 15–21, Jul. 2019.

[25] R.-H. Shi, B. Liu, and M. Zhang, "Secure two-party integer comparison protocol without any third party," *Quantum Inf. Process.*, vol. 20, no. 12, p. 402, Dec. 2021.

[26] R.-H. Shi and Y.-F. Li, "Quantum private set intersection cardinality protocol with application to privacy-preserving condition query," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 6, pp. 2399–2411, Jun. 2022.

[27] R.-H. Shi and Y.-F. Li, "Quantum protocol for secure multiparty logical AND with application to multiparty private set intersection cardinality," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 12, pp. 5206–5218, Dec. 2022.

[28] L.-B. He, L.-S. Huang, W. Yang, and R. Xu, "A protocol for the secure two-party quantum scalar product," *Phys. Lett. A*, vol. 376, no. 16, pp. 1323–1327, Mar. 2012.

[29] Y. Wang and G. He, "Quantum secure scalar product with continuous-variable clusters," in *Proc. 18th AQIS Conf.*, Nagoya, Japan, 2018, pp. 1–3. [Online]. Avaliable: http://www.ngc.is.ritsumei.ac.jp /∼ger/static/AQIS18/OnlineBooklet/161.pdf

[30] R.-H. Shi and M. Zhang, "Strong privacy-preserving two-party scalar product quantum protocol," *Int. J. Theor. Phys.*, vol. 58, no. 12, pp. 4249–4257, Dec. 2019.

[31] L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett.*, vol. 79, no. 2, pp. 325–328, Jul. 1997.

[32] W. Yang, L. Huang, R. Shi, and L. He, "Secret sharing based on quantum Fourier transform," *Quantum Inf. Process.*, vol. 12, no. 7, pp. 2465–2474, Jul. 2013.

[33] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, "Entanglement swapping of generalized cat states and secret sharing," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 4, Apr. 2002, Art. no. 042320.

[34] H.-Y. Yang and T.-Y. Ye, "Secure multi-party quantum summation based on quantum Fourier transform," *Quantum Inf. Process.*, vol. 17, no. 6, p. 129, Jun. 2018.

[35] Z. Ji, H. Zhang, H. Wang, F. Wu, J. Jia, and W. Wu, "Quantum protocols for secure multi-party summation," *Quantum Inf. Process.*, vol. 18, no. 6, p. 168, Jun. 2019.

[36] K. Sutradhar and H. Om, "A generalized quantum protocol for secure multiparty summation," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 12, pp. 2978–2982, Dec. 2020.

[37] K. Sutradhar and H. Om, "Hybrid quantum protocols for secure multi-party summation and multiplication," *Sci. Rep.*, vol. 10, no. 1, p. 9097, Jun. 2020.

[38] K. Sutradhar and H. Om, "A cost-effective quantum protocol for secure multi-party multiplication," *Quantum Inf. Process.*, vol. 20, no. 11, p. 380, Nov. 2021.

[39] X. Yi, C. Cao, L. Fan, and R. Zhang, "Quantum secure multi-party summation protocol based on blind matrix and quantum Fourier transform," *Quantum Inf. Process.*, vol. 20, no. 7, p. 249, Jul. 2021.

[40] R.-H. Shi, Y. Mu, H. Zhong, J. Cui, and S. Zhang, "Secure multiparty quantum computation for summation and multiplication," *Sci. Rep.*, vol. 6, no. 1, p. 19655, Jan. 2016.

[41] T. G. Draper, "Addition on a quantum computer," 2000, *arXiv:0008033*.

[42] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[43] A. D. Wyner, "A definition of conditional mutual information for arbitrary ensembles," *Inf. Control*, vol. 38, no. 1, pp. 51–59, Jul. 1978.

[44] A. S. Holevo, "Statistical problems in quantum physics," in *Proc.2nd Jpn.-USSR Symp. Probab. Theory*, Berlin, Heidelberg, Germany, 1973, pp. 104–119.

[45] M. Keller, E. Orsini, and P. Scholl, "MASCOT: Faster malicious arithmetic secure computation with oblivious transfer," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, New York, NY, USA, Oct. 2016, pp. 830–842.

[46] R. Cramer, I. Damgård, D. Escudero, D. Escudero, P. Scholl, and C. P. Xing, "SPD $\mathbb{Z}_{2^k}$: Efficient MPC mod 2^k for dishonest majority," in *Proc. Annu. Int. Cryptol. Conf.* Cham, Switzerland: Springer, 2018, pp. 769–798.

[47] M. Keller, V. Pastro, and D. Rotaru, "Overdrive: Making SPDZ great again," in *Proc. Adv. Cryptol. (EUROCRYPT)*. Cham, Switzerland: Springer, 2018, pp. 158–189.

[48] D. Rathee, T. Schneider, and K. K. Shukla, "Improved multiplication triple generation over rings via RLWE-based AHE," in *Proc. Int. Conf. Cryptol. Netw. Secur.* Cham, Switzerland: Springer, 2019, pp. 347–359.

[49] H. Chen, M. Kim, I. Razenshteyn, D. Rotaru, Y. S. Song, and S. Wagh, "Maliciously secure matrix multiplication with applications to private deep learning," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* Cham, Switzerland: Springer, 2020, pp. 31–59.

[50] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, Los Alamitos, CA, USA, 1994, pp. 124–134.

Wen-Jie Liu was born in 1979. He received the Ph.D. degree. He is an Associate Professor. His main research interests include quantum cryptographic communication, quantum secure multiparty computation, quantum algorithm, and quantum machine learning.

Zi-Xian Li was born in 2000. He is currently pursuing the M.S. degree. His main research interests include quantum cryptographic communication and quantum secure multiparty computation.