Shi and Li *EPJ Quantum Technology* (2022) 9:13
https://doi.org/10.1140/epjqt/s40507-022-00132-3

EPJ Quantum Technology
a SpringerOpen Journal

EPJ.org

RESEARCH Open Access

Privacy-preserving quantum protocol for finding the maximum value

Run-hua Shi[1*] and Yi-fei Li[1]

*Correspondence:
rhshi@ncepu.edu.cn
[1]School of Control and Computer Engineering, North China Electric Power University, Beijing City, 102206, China

Abstract

In this paper, we first define a primitive protocol of secure multiparty computations to privately compute the logic operator "OR" (SMC_OR). Accordingly, we design a feasible quantum SMC_OR protocol by using single photons, which can achieve information-theoretical security in the semi-honest model. Furthermore, we adopt the proposed quantum SMC_OR protocol to solve an interesting but important privacy-preserving problem, i.e., finding the maximum value among many secrets. Finally, we simulate the related quantum protocols in Qiskit and verify the correctness and the feasibility of the proposed protocols.

Keywords: Quantum cryptography; Quantum secure multiparty computations; Privacy-preserving

1 Introduction

Nowadays, quantum computations [1, 2] and quantum communications [3, 4] have received extensive attention and gained many promising achievements, e.g., quantum teleportation [5], quantum cryptography [6] and quantum artificial intelligence [7].

With the further development of quantum computing, classical cryptographic systems (e.g., RSA) faces enormous threatens and challenges. Fortunately, quantum cryptography brings new dawn, e.g., the first quantum key distribution protocol (i.e., the BB84 QKD protocol) [8], which can ensure information-theoretical security [9]. Furthermore, compared with classical cryptography, the biggest advantage of quantum cryptography is that both the sender and the receiver can easily detect any outsider's eavesdropping when transmitting quantum messages through quantum channels.

In classical settings, modern cryptography has many important functionalities and applications except for the basic encryption and decryption, e.g., ensuring message integrity and protecting user privacy. Similarly, quantum cryptography, which is a combination of modern cryptography and quantum mechanics, can theoretically ensure data security and protect user privacy. Therefore, quantum cryptography has a wide range of research, including quantum key distribution (QKD), quantum secret sharing (QSS), quantum secure direct communication (QSDC), quantum signature (QS), quantum privacy query (QPQ) and so on. However, except for QKD, there are few feasible quantum cryptographic protocols, which can be successfully implemented in large-scale networks.

Springer

In this paper, we focus on input privacy in a specific cryptographic task, in which a group of users try to compute the maximum value among their private inputs. Our primary goal is to protect user privacy by designing ingenious quantum cryptographic protocols. Furthermore, our secondary goal is to design quantum protocols by employing feasible quantum processing technologies, so that designed quantum protocols can be practically and effectively implemented. First, we define an interesting but important primitive protocol of secure multiparty computation, i.e., secure multiparty computation of OR (SMC_OR for short) and design the corresponding quantum SMC_OR protocol. What's more, we present an unconditionally (i.e., information-theoretically) secure quantum protocol for finding the maximum value among many secrets based on proposed quantum SMC_OR protocols, where each secret belongs to a different participant.

In classical setting, secure multiparty computation (SMC) is an important subfield of modern cryptography, which allows a number of mutually distrustful parties to jointly compute a function without leaking their respective private inputs. The first SMC problem was presented by Yao [10], i.e., the Millionaires' problem, in which two millionaires wish to know who is richer without disclosing their wealth. Privately finding the maximum value is the general case of the Millionaires' problem, in which a group of parties try to compute the maximum value (i.e., the greatest value) among their private inputs. Accordingly, a naive method to find the maximum value among many private inputs may adopt pairwise private comparison protocols [11], but this method reveals the rank order of all private inputs. Due to its importance, there appeared other better methods to privately compute the maximum value based on classical cryptographic algorithms, e.g., homomorphic encryption [12] and anonymous veto network [13]. However, the security of these algorithms is based on unproven computational assumptions, e.g., to prove the security of proposed algorithms in Ref. [13], the author assumes that the Decision Diffie-Hellman (DDH) problem is intractable. Furthermore, these computational assumptions are vulnerable to the attacks by quantum computers due to fast quantum algorithms [9]. Accordingly, these algorithms based on unproven computational assumptions cannot resist quantum attacks. What's more, compared with the classical related algorithms or protocols, the biggest advantage of using quantum cryptography to compute the maximum value is that it can easily detect any outsider's eavesdropping or any party's dishonesty.

Finding the maximum value among many secrets has important and wide applications in privacy-preserving fields, such as sealed-bid auction [14, 15], electronic voting [16, 17] and federated learning [18, 19]. For example, in sealed-bid auction, an auctioneer can get the highest bid by finding the maximum value among multiple private bids, so that it can ensure the anonymity because each bidder does not need to submit his private bid to the auctioneer. In quantum setting, there were quantum algorithms to find the maximum [20] or the minimum [21]. However, in these quantum algorithms there is not any privacy protection. To the best of our knowledge, there is not yet any quantum protocol for privately finding the maximum value.

Though near-term quantum computing devices have super-fast computing power, few users can own them due to their expensive costs. Furthermore, the emergence of various quantum cloud platforms (e.g., IBM quantum experience) makes it possible for ordinary users to perform quantum computing. In view of this, we introduce a quantum cloud in our proposed quantum protocols to make the quantum processing capacity required by all parties reach the minimum requirements, i.e., it only needs to perform single-photon

operators (Pauli operator and Hadamard gate operator). Furthermore, our proposed quantum protocols take single photons (i.e., BB84 states) as quantum resources and only need to perform single-photon operators and single-photon measurements, which are similar to the BB84 QKD protocol. Therefore, it is feasible to implement proposed protocols with present technologies.

2 Quantum SMC_OR protocol

In this section, we first give an informal definition of a primitive problem of secure multiparty computations, i.e., secure multiparty computation of OR (SMC_OR for short), and then present a feasible quantum protocol for SMC_OR, which will be utilized later in privacy-preserving quantum protocol for finding the maximum value (later called privacy-preserving QFMV protocol).

Definition 1 (SMC_OR) Suppose that there are m ($m > 2$) parties: $P_1, P_2, \ldots, P_m$, each of which has a private input $x_i \in \{0, 1\}$ ($i = 1, 2, \ldots, m$). After executing the SMC_OR protocol, the protocol outputs $x_1 \vee x_2 \vee \cdots \vee x_m$. Here "$\vee$" denotes a logical OR, i.e., $0 \vee 0 = 0$, $0 \vee 1 = 1$, $1 \vee 0 = 1$ and $1 \vee 1 = 1$. In addition, SMC_OR should satisfy the following requirements:

Correctness. If all parties honestly execute this protocol, then the final output is $x_1 \vee x_2 \vee \cdots \vee x_m$, i.e., the output is correct.

Fairness. Roughly speaking, no coalition of dishonest parties can harm any honest party without being detected. In other words, under no circumstances one party should have an advantage over another or other parties.

Privacy. Any other party except for the party P_i learns no information about x_i except the final output $x_1 \vee \ldots x_i \cdots \vee x_m$.

Security Model. In the following protocols, we only consider the honest-but-curious parties [14, 15], like the semi-honest model [13] in the classical settings, where adversaries may try to learn as much information as possible from a given protocol execution but are not able to deviate from the protocol steps. That is, in the semi-honest model, each participant follows the protocol specification but tries to deduce some private information about the other participants [13].

Furthermore, we assume that there is a semi-honest quantum cloud, who will prepare all quantum resources (i.e., single photons) and perform all single-photon measurements, and other parties with quantum-limited capabilities only need to forward single photons and perform simple single-photon operators. In addition, we assume that there is an authenticated quantum channel between any P_i and P_{i+1} ($i = 1, 2, \ldots, m$ and P_{m+1} is the quantum cloud). Finally, the quantum cloud is responsible to output $x_1 \vee x_2 \vee \cdots \vee x_m$.

In the semi-honest model, each participant follows the protocol specification but tries to deduce some private information about the other participants [13]. So, in the following protocols we mainly consider two privacy goals: (1) Preserving input privacy from anyone inside the group of participants, including the quantum cloud; (2) Preserving input privacy from outside passive attackers, i.e., outside eavesdropper.

Quantum SMC_OR Protocol

Step 1. All parties agree on a small integer k, e.g., $k = 10$, which is related to the probability of successfully outputting $x_1 \vee \cdots x_i \cdots \vee x_m$ (i.e., the error probability $\delta \approx \frac{1}{2^k}$, later see Theorem 1).

Step 2. Each party P_i ($i = 1, 2, \ldots, m$) generates a private array X_i of the length k by his private input x_i: If $x_i = 0$, then all $X_i[j]$s are equal to 0; If $x_i = 1$, then each $X_i[j]$ is equal to 0 or 1 randomly but there is at least one 1 among all $kX_i[j]$s. That is, if $x_i = 0$, then $X_i[1] \vee X_i[2] \vee \cdots \vee X_i[k] = 0$; if $x_i = 1$, then $X_i[1] \vee X_i[2] \vee \cdots \vee X_i[k] = 1$.

Step 3. Let $t = 2(k + q)$, where q is a secure parameter. Furthermore, each party P_i ($i = 1, 2, \ldots, m$) randomly generates two t-element arrays R_i and S_i, where $R_i[j] \in_R \{0, 1\}$ and $S_i[j] \in_R \{0, 1\}$ for $j = 1, 2, \ldots, t$.

Step 4. The quantum cloud prepares t single photons: $ph_1, ph_2, \ldots, ph_t$, each of which is randomly in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Furthermore, the quantum cloud records the initial states of t single photons. Finally, the quantum cloud sends all t single photons $ph_1, ph_2, \ldots, ph_t$ to the party P_1 through the authenticated quantum channel.

Step 5. The party P_1 executes the following procedures: {

For $j = 1$ to t do {

If $S_1[j] = 1$, then apply an H gate operator to the jth single photon ph_j;

If $R_1[j] = 1$, then apply a Pauli operator U_y to the jth single photon ph_j. } }

Here, H and U_y are defined by [9],

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{1}$$

$$U_Y = iY = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2}$$

Step 6. The party P_1 sends all t single photons $ph_1, ph_2, \ldots, ph_t$ to the party P_2 through the authenticated quantum channel.

Step 7. After receiving all photons sent from the party P_1, the party P_2 executes the similar procedures of the party P_1 and then sends all photons to the next party P_3 through the authenticated quantum channel. In total, the process is repeated m times. Finally, the party P_m sends t single photons $ph_1, ph_2, \ldots, ph_t$ back to the quantum cloud.

Please note that after receiving t single photons sent from the previous party, the party P_i executes the following procedures: {

For $j = 1$ to t do {

If $S_i[j] = 1$, then apply an H gate operator to the jth single photon ph_j;

If $R_i[j] = 1$, then apply a Pauli operator U_y to the jth single photon ph_j. } }

Step 8. After receiving all t single photons, the quantum cloud measures each photon ph_j in the initial basis for $j = 1, 2, \ldots, t$, and records all measured results.

Step 9. Post-processing: (1) Each party P_i ($i = 1, 2, \ldots, m$) opens his random bits $S_i[j]$s for $j = 1, 2, \ldots, t$. (2) All parties publicly select out the useful js from $j = 1$ to t, where the useful condition of j must satisfy $\sum_{i=1}^{m} S_i[j] \bmod 2 = 0$. Please note that the basis of the jth photon ph_j will not change when satisfying the useful condition (please see later correctness analysis for details). (3) All parties keep the useful events, in which the sequence number j satisfies the useful condition, and discard the rest (with the probability of $\frac{1}{2}$). (4) There are approximate $k + q$ (i.e., $\frac{1}{2}t$) useful events in total. All parties randomly select out exactly k useful events as encoding events to compute the final result and the remaining about q useful events as checking events to check any dishonesty or eavesdropping. (5) Suppose that there are q checking events. The parties open the corresponding sequence number js of all q checking events and ask the quantum cloud to announce the

initial quantum states and the measurement results of q checking events. After that, all parties open their respective random bits $R_i[j]$s (only) for all checking events. By all public $R_i[j]$s, the initial quantum states and the corresponding measurement results, all parties can determine whether there is any dishonest party or an outside eavesdropper. That is, if $\sum_i R_i[j] = 0$ ($\sum_i R_i[j] = 1$), the measurement result should be the same (opposite) as the initial quantum state; otherwise there is a dishonest party or an eavesdropping adversary. If no dishonesty or eavesdropping was found, the parties continue to execute the next step, otherwise abort.

Step 10. Suppose that k encoding events kept to compute the final result are corresponding to the l_1th, l_2th, ..., l_kth photon among all t photons, where $l_j \in \{1, 2, \ldots, t\}$ and $j \in \{1, 2, \ldots, k\}$. Then, all parties open the corresponding sequence number js of all k encoding events: $l_1, l_2, \ldots, l_k$. Each party P_i ($i = 1, 2, \ldots, m$) computes

$$X_i^*[l_j] = \big(X_i[j] + R_i[l_j]\big) \bmod 2, \tag{3}$$

for $j = 1, 2, \ldots, k$. Furthermore, each party P_i opens $X_i^*[l_j]$. Please note that $X_i^*[l_j] = (X_i[j] + R_i[l_j]) \bmod 2 = X_i[j] \oplus R_i[l_j]$, which is the one-time pad method to encrypt $X_i[j]$ since $R_i[l_j]$ is random and private.

Step 11. The quantum cloud computes $X^*[l_j]$ ($j = 1, 2, \ldots, k$) by

$$X^*[l_j] = \sum_{i=1}^{m} X_i^*[l_j] \bmod 2. \tag{4}$$

Furthermore, the quantum cloud performs the following procedures: {

(1) Let $w = 0$.

(2) For $j = 1$ to k do {

If the measured result of the l_jth photon ph_{l_j} is inconsistent with the initial state of the photon ph_{l_j} (later we will prove that it implies that $\sum_{i=1}^{m} R_i[l_j] \bmod 2 = 1$), then $w = (X^*[l_j] + 1) \bmod 2$; //$w = \sum_{i=1}^{m} X_i[j] \bmod 2$.

else $w = X^*[l_j]$. //$w = \sum_{i=1}^{m} X_i[j] \bmod 2$.

If $w = 1$, Return (w). }

Return (0).}

3 Privacy-preserving QFMV protocol

Similarly, we assume there are m ($m > 2$) parties: $P_1, P_2, \ldots, P_i, \ldots, P_m$ in the following privacy-preserving QFMV protocol, where each party P_i has a secret $Y_i \in Z_N$ and $n = \log N$ (i.e., Y_i is an n-bit integer). Similarly, $Y_i[j]$ represents the jth bit of Y_i. The goal of the protocol is to find the maximum value $Y_{\max}$ among all secrets $Y_1, Y_2, \ldots, Y_i, \ldots$, and Y_m (i.e., $Y_{\max} \in \{Y_1, Y_2, \ldots, Y_m\}$ but $Y_{\max} \geq Y_i$ for any i), while it must protect the privacy of all non-maximum secrets.

Step 1. Each party P_i ($i = 1, 2, \ldots, m$) generates an auxiliary array Y_i^* and sets $Y_i^* = Y_i$ initially.

Step 2. All parties jointly execute the following procedures: {

For $j = 1$ to n do {

(1) All parties execute a quantum SMC_OR protocol with the help of the quantum cloud, where each party P_i ($i = 1, 2, \ldots, m$) privately inputs $Y_i^*[j]$. Accordingly, the quantum cloud outputs and opens $W[j]$, where $W[j] = Y_1^*[j] \vee Y_2^*[j] \vee \cdots \vee Y_m^*[j]$.

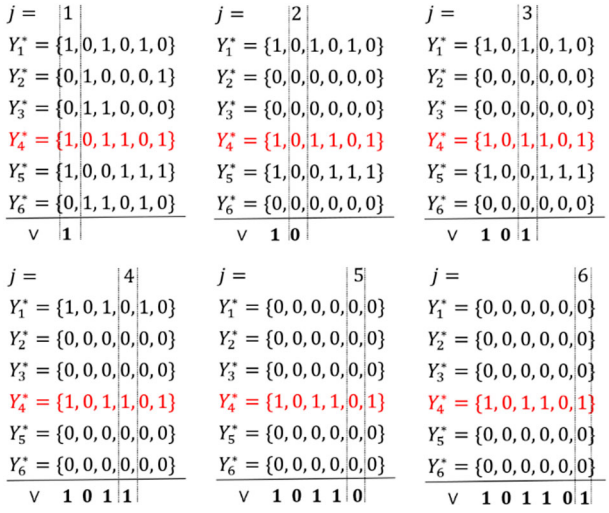

Figure 1 The Schematic of the proposed QFMV protocol

(2) Each party P_i ($i = 1, 2, \ldots, m$) renews the auxiliary array Y_i^* according to the previous output $W[j]$:

If $W[j] > Y_i^*[j]$ (i.e., $W[j] = 1$ and $Y_i^*[j] = 0$), then set $Y_i^* = \mathbf{0}$ (i.e., let all $Y_i^*[j]$s be equal to 0). // It implies that Y_i cannot be the maximum (please see Fig. 1).

(3) $j++.\}\}$

Step 4. After executing n quantum SMC_OR protocols, the protocol finally outputs $\{W[1], W[2], \ldots, W[n]\}$ as the bit string of the maximum value.

4 Analysis

4.1 Correctness

The core idea of the proposed privacy- preserving QFMV protocol is to calculate bitwise OR operators of all private bit strings from left to right, i.e., from high to low. Initially, each bit string Y_i^* represents a private secret, i.e., Y_i. As the calculations progress, increasingly, all parties, except one whose input is the maximum value, can determine that their private inputs are less than the maximum value, and accordingly, they will input 0 in later quantum SMC_OR protocols. That is, only the party with the maximum value retains all bits in his private bit string, while other parties renew their bits to ensure that each bit of them is less than or equal to the corresponding bit of the maximum value. So, it can finally output all bits of the maximum value. Here, we give a simple example, as shown in Fig. 1. From the example, we can see that the correctness of the proposed QFMV protocol is mainly guaranteed by quantum SMC_OR protocols. So, we further analyze the correctness of the quantum SMC_OR protocol as Theorem 1. In the following theorem, suppose that the number of one among m private inputs (i.e., $x_1, x_2, \ldots, x_m$) in the quantum SMC_OR protocol is p, where $p \leq m$.

Theorem 1 *If $p = 0$ or 1, then the quantum SMC_OR protocol is perfectly correct; If $p \geq 2$, then it may give a wrong output 0, but the error probability $\delta \approx \frac{1}{2^k}$, which is very small and negligible when k is large enough, e.g., $k = 10$.*

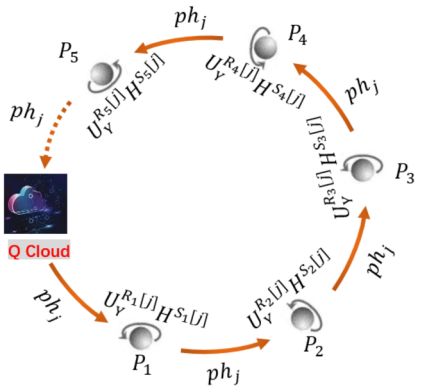

Figure 2 The transmitting schematic of the single photon

Proof (1) On the one hand, from Eqs. (1) and (2), we can easily get the following equations:

$$H^2 = U_Y^2 = I, \tag{5}$$

$$HU_YH = -U_Y, \tag{6}$$

$$HU_Y = -U_YH. \tag{7}$$

Furthermore, we consider all possible operators on a specific photon, e.g., ph_j, as shown in Fig. 2.

Suppose that the initial state of the photon ph_j is $|\psi\rangle_j$. By previously prescribed procedures, when the photon ph_j finally comes back to the quantum cloud, its final state $|\phi\rangle_j$ will be changed as

$$|\phi\rangle_j = U_Y^{R_m[j]}H^{S_m[j]}\cdots U_Y^{R_2[j]}H^{S_2[j]}U_Y^{R_1[j]}H^{S_1[j]}|\psi\rangle_j. \tag{8}$$

By Eqs. (5)–(7), we can further get

$$|\phi\rangle_j = (-1)^l U_Y^{\sum_i R_i[j]}H^{\sum_i S_i[j]}|\psi\rangle_j. \tag{9}$$

Here, $l = 0$ or $l = 1$. Furthermore, if j satisfies the useful condition, then $\sum_i S_i[j] = 0 \bmod 2$, so

$$|\phi\rangle_j = (-1)^l U_Y^{\sum_i R_i[j]}|\psi\rangle_j. \tag{10}$$

In addition, it gives

$$\begin{aligned} &U_Y|0\rangle \to |1\rangle, \\ &U_Y|1\rangle \to -|0\rangle, \\ &U_Y|+\rangle \to |-\rangle, \\ &U_Y|-\rangle \to -|+\rangle. \end{aligned} \tag{11}$$

By Eqs. (10) and (11), we further know that for any useful event, the final state will remain the same as the initial state except for a global phase if the number of performing U_Y is even, otherwise it will change, but it keeps the same basis.

In turn, if the measured result of the jth photon ph_j by the quantum cloud is inconsistent with the initial state of the photon ph_{l_j}, then $\sum_{i=1}^{m} R_i[j] \bmod 2 = 1$, and $\sum_{i=1}^{m} R_i[j] \bmod 2 = 0$ otherwise. That is, the single $R_i[j]$ is private, but the quantum cloud knows the summation of $\sum_{i=1}^{m} R_i[j] \bmod 2$.

Furthermore, by Eqs. (3) and (4), we can get

$$\begin{aligned} X^*[l_j] &= \sum_{i=1}^{m} X_i^*[l_j] \bmod 2 \\ &= \sum_{i=1}^{m} \big(X_i[j] + R_i[l_j]\big) \bmod 2 \\ &= \sum_{i=1}^{m} X_i[j] \bmod 2 + \sum_{i=1}^{m} R_i[j] \bmod 2. \end{aligned} \tag{12}$$

If $\sum_{i=1}^{m} R_i[j] \bmod 2 = 1$, $\sum_{i=1}^{m} X_i[j] \bmod 2 = (X^*[l_j] + 1) \bmod 2$, and $\sum_{i=1}^{m} X_i[j] \bmod 2 = X^*[l_j]$ otherwise. So, the equation of $w = \sum_{i=1}^{m} X_i[j] \bmod 2$ is always true. In turn, the quantum cloud can deduce the value of $\sum_{i=1}^{m} X_i[j] \bmod 2$ (i.e., w) by the public information and his recorded results.

(2) On the other hand, we further consider the following different cases that m inputs $x_1, \ldots x_i, \ldots, x_m$ have p ones (i.e., p is the number of ones in all x_is).

In the case of $p = 0$ (i.e., all x_is are equal to 0):

Accordingly, all $X_i[j]$s are equal to 0. That is, $w = \sum_{i=1}^{m} X_i[j] \bmod 2 = 0$ for all j. Since $x_1 \vee x_2 \vee \cdots \vee x_m = 0$, the output is correct.

In the case of $p = 1$:

There is just one X_{i^*} that $X_{i^*} \neq 0$, so there is at least one j, such that $w = \sum_{i=1}^{m} X_i[j] \bmod 2 = X_{i^*}[j] = 1$. That is, $x_1 \vee x_2 \vee \cdots \vee x_m = w = 1$. Therefore, the output is correct.

In the case of $p = 2$:

Suppose that $x_{i_1} = 1$ and $x_{i_2} = 1$. Accordingly, $X_{i_1} \neq \mathbf{0}$ and $X_{i_2} \neq \mathbf{0}$. Then, the total number of appropriate X_{i_1} and X_{i_2} is $(2^k - 1)(2^k - 1)$. Furthermore, the final output $w = 1$ if $X_{i_1} \neq X_{i_2}$, otherwise $w = 0$ (i.e., $X_{i_1} = X_{i_2}$). The number of possible X_{i_1} (i.e., $X_{i_1} \neq 0$) is $(2^k - 1)$. So, the error probability (i.e., $X_{i_1} = X_{i_2}$) is equal to

$$\begin{aligned} \delta &= \frac{(2^k - 1)}{(2^k - 1)(2^k - 1)}, \\ \delta &= \frac{1}{(2^k - 1)}. \end{aligned} \tag{13}$$

Obviously, when k is large enough, $\delta \approx 0$. For example, if $k = 6$, $\delta = 0.01587$; if $k = 10$, $\delta = 0.00098$.

In the case of $p = 3$:

We consider the following error combinations: k rows (corresponding to $j = 1, 2, \ldots, k$) and p columns (corresponding to p array X_is), where each column has at least one "1" (i.e., the corresponding $X_i \neq 0$) and each row has zero "1" or two "1"s, i.e., $w = \sum_{i=1}^{m} X_i[j] \bmod 2 = 0$. However, $x_1 \vee x_2 \vee \cdots \vee x_m = 1$. Furthermore, by the possible 1s in each row, we can deduce that the error probability satisfies the following condition:

$$\delta < \frac{(C_3^0 + C_3^2)^k}{(2^k - 1)(2^k - 1)(2^k - 1)},$$

$$\delta < \frac{4^k}{(2^k-1)(2^k-1)(2^k-1)} \approx \frac{1}{2^k}. \tag{14}$$

Similarly, when k is large enough, $\delta \approx 0$. For example, if $k = 6$, $\delta < 0.01638$; if $k = 10$, $\delta < 0.00098$.

By analogy, we can easily deduce that other more general cases for any p:

$$\begin{aligned} \delta &< \frac{(C_p^0 + C_p^2 + C_p^4 + \cdots + C_p^{2\lfloor p/2 \rfloor})^k}{(2^k-1)^p}, \\ \delta &< \frac{(2^{p-1})^k}{(2^k-1)^p} \approx \frac{1}{2^k}. \end{aligned} \tag{15}$$

Please note that $C_p^0 + C_p^1 + C_p^2 + \cdots + C_p^p = 2^p$ and $C_p^i = C_{p-1}^{i-1} + C_{p-1}^i$. Therefore, when k is large enough, δ is negligible. That is, the proposed quantum SMC_OR protocol is approximatively correct. □

4.2 Security

According to the proposed QFMV protocol, all parties jointly compute the bitwise OR operators of their respective private inputs (see Fig. 1). So, the security of the proposed QFMV protocol is guaranteed by that of the proposed quantum SMC_OR protocol. In the following theorem, we will prove that our proposed quantum SMC_OR protocol is information-theoretically secure in the semi-honest model.

Theorem 2 *The proposed quantum SMC_OR protocol is information-theoretically secure, when all parties honestly execute the protocol.*

Proof Before publishing the random bit $S_i[j]$, each party P_i performs two quantum operators $U_Y^{R_i[j]} H^{S_i[j]}$ on the jth photon ph_j, that is, he encrypts each transmitted qubit (e.g., the single-photon ph_j) by using two random and secret bits (i.e., privately performing two quantum operators $U_Y^{R_i[j]} H^{S_i[j]}$ on the photon ph_j). Similarly, it is a perfect quantum encryption [22], which is information-theoretically secure.

By Ref. [22], the quantum protocol is information-theoretically secure if for every input state ρ_{in}, the output state ρ_{out} is a totally mixed state. The relation of the input state ρ_{in} and the output state ρ_{out} is as follows:

$$\rho_{\text{out}} = \sum_k p_k U_k \rho_{\text{in}} U_k^\dagger = \frac{1}{2^t} I. \tag{16}$$

Here ρ_{in} is the density matrix of all possible t-qubit input states and U_k is the corresponding unitary operator applied to the input state.

For simplicity, we only analyze an arbitrary photon, e.g., ph_j, in our protocol. Accordingly, we can get

$$\begin{aligned} \rho_{\text{in}}(ph_j) &= \left[\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right] \\ &= \frac{1}{4}\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right] \end{aligned}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{I}{2}, \tag{17}$$

$$R_i[j], S_i[j] \in_R \{0,1\}. \tag{18}$$

So, after the party P_i performing the corresponding operators, the output state should be in

$$\begin{aligned}
\rho_{\text{out}}(ph_j) &= \frac{1}{4}\left[U_Y^0 H^0\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\
&\quad + \frac{1}{4}\left[U_Y^0 H^1\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\
&\quad + \frac{1}{4}\left[U_Y^1 H^0\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\
&\quad + \frac{1}{4}\left[U_Y^1 H^1\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\
&= \frac{1}{4}\left[\left(\frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right)\right] \\
&\quad + \frac{1}{4}\left[\left(\frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|-\rangle\langle -|\right) + \frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|\right] \\
&\quad + \frac{1}{4}\left[\left(\frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|-\rangle\langle -| + \frac{1}{4}|+\rangle\langle +|\right)\right] \\
&\quad + \frac{1}{4}\left[\left(\frac{1}{4}|-\rangle\langle -| + \frac{1}{4}|+\rangle\langle +| + \frac{1}{4}|1\rangle\langle 1| + \frac{1}{4}|0\rangle\langle 0|\right)\right] \\
&= \frac{1}{4}[|0\rangle\langle 0| + |1\rangle\langle 1| + |+\rangle\langle +| + |-\rangle\langle -|)] \\
&= \frac{1}{4}\left[\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}\right] \\
&= \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{I}{2}.
\end{aligned} \tag{19}$$

From Eq. (19), we can see that the output of the single-photon ph_j after the party P_i performing private operators is just a totally mixed state. So, anyone including the quantum cloud or the next party P_{i+1} cannot get any private information about the party P_i's bits $R_i[j]$ and $S_i[j]$. That is, it is a perfect quantum encryption.

After completing the tests of q checking events, each party P_i computes and opens $X_i^*[l_j] = (X_i[j] + R_i[l_j]) \bmod 2$, where $R_i[l_j]$ is completely random and private. Clearly, it is a classical one-time pad.

In short, perfect quantum encryption and classical one-time pad can ensure the information-theoretical security of the proposed quantum protocols in the semi-honest model.

Furthermore, a dishonest party (e.g., P_{i-1}) can perform a collusion attack to eavesdrop on partial private information of the party P_i with the next party P_{i+1} as follows:

After the dishonest party P_{i-1} receives all t single photons, he prepares t two-photon Bell states and sends t photons of Bell states to the party P_i instead of the original t single photons. Without loss of generality, we only analyze a Bell state of two photons, e.g.,

$\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}$. For example, the dishonest party P_{i-1} sends the photon b to the party P_i instead of the real photon ph_j, while he keeps the photon a in hands. Accordingly, the party P_i performs the following operators $U_Y^{R_i[j]}H^{S_i[j]}$ on the photon b:

$$U_Y^0 H^0 \frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}} = \frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}, \tag{20}$$

$$U_Y^0 H^1 \frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}} = \frac{|0+\rangle_{ab}+|1-\rangle_{ab}}{\sqrt{2}}, \tag{21}$$

$$U_Y^1 H^0 \frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}} = \frac{|01\rangle_{ab}-|10\rangle_{ab}}{\sqrt{2}}, \tag{22}$$

$$U_Y^1 H^1 \frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}} = \frac{|0-\rangle_{ab}+|1+\rangle_{ab}}{\sqrt{2}}. \tag{23}$$

Later, the party P_i sends the photon b to the next party P_{i+1}. To implement the collusion attack, the party P_{i+1} does nothing except send the photon b to the party P_{i-1}. Finally, the party P_{i-1} performs a Bell-basis measurement on the two photons (a, b) so that it can deduce partial private information of the party P_i. For example, if his measured result is $\frac{|00\rangle_{ab}+|11\rangle_{ab}}{\sqrt{2}}$, then he can deduce that $R_i[j] = 0$ and $S_i[j] = 0$.

In particular, to resist this collusion attack, we add the tests of q checking events in our proposed protocol. Obviously, checking events can ensure the honesty of all parties and resist the outsider's eavesdropping, which is similar to the decoy technology in QKD [23].

On the other hand, if the dishonest parties perform this attack, the final output must be wrong. So, in order to verify whether the final output is the maximum value among many secrets, we can add a commit protocol in the initial phase as follows:

Each party P_i $(i = 1, 2, \ldots, m)$ randomly selects an integer $R_i \in Z_N$ and computes $C_i = H(R_i \oplus H(R_i \oplus Y_i))$, where Y_i is his secret and $H(\cdot)$ is a hash function with strong collision-resistant. Then the party P_i submits C_i to the quantum cloud by the classical channels. That is, the party P_i commits Y_i to the quantum cloud, but no one can get Y_i only from C_i without R_i.

Later, when the quantum cloud outputs the maximum value Y_{max}, the party P_{max} with the maximum value Y_{max} opens his secrets Y_{max} and R_{max}. Finally, the quantum cloud can verify its correctness by determining whether the following equation is true or not:

$$C_{max} = H\big(R_{max} \oplus H(R_{max} \oplus Y_{max})\big). \tag{24}$$

If there is no any party to claim the maximum value, it shows the output result is wrong.

According to the above analysis, if all parties honestly execute the protocol, it will output the final result rightly. In turn, any eavesdropping or dishonesty can be easily detected by public comparisons in checking events. Accordingly, no coalition of dishonest parties can harm any honest party without being detected. Furthermore, all parties in our protocol are perfect peer and execute the same procedures. Therefore, the proposed quantum SMC_OR protocol can achieve the fairness.

In addition, like most existing multiparty quantum computations, our proposed quantum SMC_OR protocol needs authenticated quantum channels, which can ensure the authenticity of quantum resources and participant identities. In principle, we may combine quantum authentication technologies [24] with classical authentication technologies [25] to implement various authentications in quantum channels. □

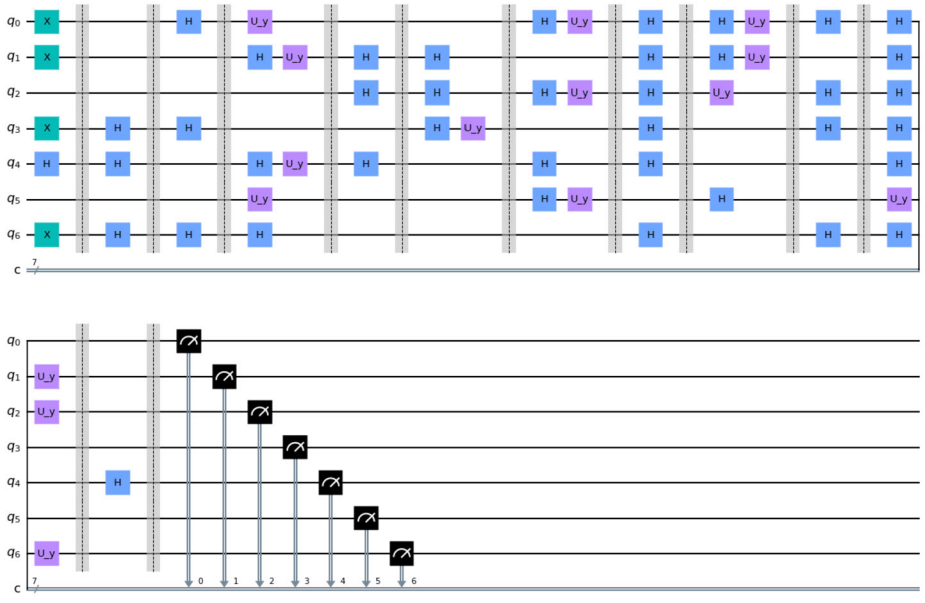

Figure 3 Quantum circuits of an instance of SMC_OR

4.3 Performance

The proposed quantum SMC_OR protocol takes single photons as quantum resources and accordingly needs single-photon-based operators (i.e., U_Y and H) and measurements. Suppose that there are m parties. Then, it needs to transmit $2(k+q)m$ qubits. So, the communicational complexity is $O(km)$. Furthermore, we assume that the bit length of each secret in the proposed QFMV protocol is n. So, it needs to call the proposed quantum SMC_OR protocol n times. Accordingly, our proposed QFMV protocol's communicational complexity is $O(kmn)$.

Furthermore, we simulate the proposed quantum SMC_OR protocol in Qiskit of IBM (Qiskit-0.23.2; Python-3.8.6; OS-Linux). First, we verify the correctness of this protocol in different instances, i.e., the different parameters: k, p and m. For example, $k = 7$, $p = 5$ and $m = 11$. The detailed circuits of this instance are shown in Fig. 3. Then, we focus on the error rate (i.e., the error probability δ) of proposed SMC_OR protocol with different values of k and p.

The curve charts in Fig. 4 show the relationships between the error rate and the parameter p when k takes different values. In our simulation experiments, suppose that there are 10 parties and they jointly compute the SMC_OR protocol 60000 times for each k, where each input is random in each time. From Fig. 4, we can see that the error rate mainly depends on the values of k when $p \geq 2$, and it is approximatively equal to 0 when $k = 10$. In short, our simulation experiments verify the correctness and the feasibility of the proposed quantum SMC_OR protocol.

At present, we do not consider quantum noise and loss of photons in our proposed quantum protocols. Obviously, we can increase the number of transmitting single photons (i.e., t) in practical applications and adopt classical error-correction technology to avoid these problems. In addition, when the parties are far apart, we may deploy a quantum repeater at each party, which is used to forward private and unknown states of photons based on teleportation.

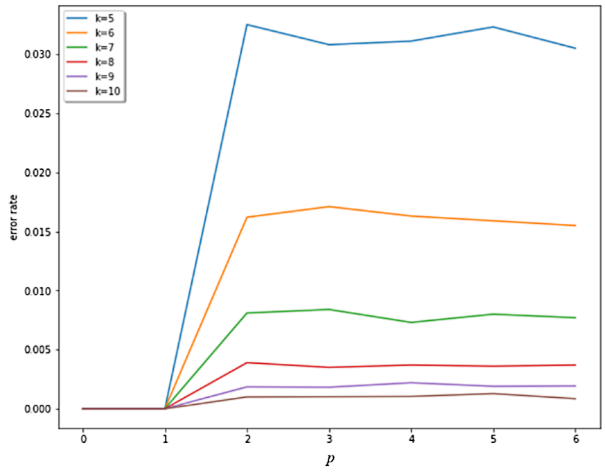

Figure 4 Curve charts of the error rate with different parameters

In a word, it is feasible to implement our proposed quantum protocols with the present quantum technologies.

5 Conclusion

In this paper, we first designed a feasible quantum protocol with the help of a quantum cloud to privately compute the logic operator "OR", which takes single photons as quantum resources and only needs to perform single-photon operators and measurements. Furthermore, we first presented a novel quantum approach to privately find the maximum value among many secrets based on the proposed quantum SMC_OR protocol.

In our proposed quantum protocols, we build a perfect quantum encryption and combine the perfect quantum encryption with the classical one-time pad to perfectly protect the privacy of each input. Therefore, there are good application prospects of our proposed protocols in emerging computations, e.g., outsourcing quantum cloud computing and quantum federated learning. Especially, as a building block, quantum SMC_OR protocol can be utilized to privately compute more complex Boolean functions.

In a word, the proposed quantum protocols show that we can also design sophisticated and flexible cryptographic protocols based on quantum physics as mathematic cryptography, not just QKD. In future work, we will further focus on the feasibility of proposed quantum protocols, e.g., considering weak coherent pulses instead of single photons.

Acknowledgements
The authors would like to thank the editor and the referees for carefully reading the paper, and for their useful comments which helped improve the paper.

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

Availability of data and materials
Not applicable.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Authors' contributions
RHS contributed to the initiation of the research and was a major contributor in writing the manuscript. YFL implemented circuit simulations and contributed to the comment and revision of the manuscript. All authors read and approved the final manuscript.

Publisher's Note

Received: 15 September 2021 Accepted: 30 April 2022 Published online: 12 May 2022

References

1. Arute F, Arya K, Babbush R et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019;574:505–10.
2. Zhong HS, Wang H, Deng YH et al. Quantum computational advantage using photons. Science. 2020;370:1460–3.
3. Gibney E. One giant step for quantum Internet. Nature. 2016;535:478–9.
4. Castelvecchi D. The quantum Internet has arrived (and it hasn't). Nature. 2018;554:289–92.
5. Marzolino U, Buchleitner A. Quantum teleportation with identical particles. Phys Rev A. 2015;91(3):032316.
6. Price AB, Rarity JG, Erven C. A quantum key distribution protocol for rapid denial of service detection. EPJ Quantum Technol. 2020;7:8.
7. Costa NF, Omar Y, Sultanov A et al. Benchmarking machine learning algorithms for adaptive quantum phase estimation with noisy intermediate-scale quantum sensors. EPJ Quantum Technol. 2021;8:16.
8. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proc. IEEE international conference on computers, systems, and signal processing. 1984. p. 175–9.
9. Nielsen MA, Chuang IL. Quantum computation and quantum information: 10th anniversary edition. Cambridge: Cambridge University Press; 2011.
10. Yao A. Protocols for secure computations. In: Proceedings of 23th annual symposium on foundations of computer science (FOCS '82). Chicago, USA. New York: IEEE Comput. Soc.; 1982. p. 160–4.
11. Li L, Shi RH. A novel and efficient quantum private comparison scheme. J Korean Phys Soc. 2019;75(1):15–21.
12. Kreitz G, Dam M, Wikström D. Practical private information aggregation in large networks. In: Aura T, Järvinen K, Nyberg K, editors. Information security technology for applications. NordSec 2010. Lecture notes in computer science. vol. 7127. Berlin: Springer; 2012.
13. Ashouri-Talouki M. An efficient privacy-preserving P2P protocol for computing maximum value in the presence of active adversaries. Peer-to-Peer Netw Appl. 2018;11:34–43.
14. Shi RH. Quantum sealed-bid auction without a trusted third party. IEEE Trans Circuits Syst I. 2021;68(10):4221–31.
15. Shi RH. Anonymous quantum sealed-bid auction. IEEE Trans Circuits Syst II. 2022;69(2):414–8.
16. Vaccaro JA, Spring J, Chefles A. Quantum protocols for anonymous voting and surveying. Phys Rev A. 2007;75(1):012333.
17. Bao N, Halpern NY. Quantum voting and violation of Arrow's impossibility theorem. Phys Rev A. 2017;95(6):062306.
18. Chen SY, Federated YS. Quantum Machine Learning. 2021. 2103.12010.
19. Hui C, Liu S, Zhao R, Xiong X. IFed: a novel federated learning framework for local differential privacy in power Internet of Things. Int J Distrib Sens Netw. 2020;16(5):155014772091969.
20. Ahuja A, Kapoor S. A Quantum Algorithm for finding the Maximum. 1999. quant-ph/9911082v1.
21. Dürr C, Høyer P. A quantum algorithm for finding the minimum. 1999. quant-ph/9607014v2.
22. Boykin PO, Roychowdhury V. Optimal encryption of quantum bits. Phys Rev A. 2003;67(4):042317.
23. Hwang WY. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91:057901.
24. Shi RH, Mu Y, Zhong H, Zhang S, Cui J. Quantum private set intersection cardinality and its application to anonymous authentication. Inf Sci. 2016;370–371:147–58.
25. Shi RH. Quantum multiparty privacy set intersection cardinality. IEEE Trans Circuits Syst II. 2021;68(4):1203–7.