Quantum Information Processing (2018) 17:199
https://doi.org/10.1007/s11128-018-1967-x

Rational protocol of quantum secure multi-party computation

Zhao Dou[1] · **Gang Xu**[1] · **Xiu-Bo Chen**[1,2] · **Xin-Xin Niu**[1,2] · **Yi-Xian Yang**[1,2]

Received: 11 January 2018 / Accepted: 19 June 2018 / Published online: 29 June 2018

Abstract
In a rational protocol, players are supposed to be rational, rather than honest, semi-honest or dishonest. This kind of protocols is practical and important, but seldom researched in quantum computation field. In this paper, a multifunctional rational quantum secure multi-party computation protocol is investigated. Firstly, a rational quantum summation protocol is proposed. Secondly, the protocol is generalized to a rational quantum multi-party computation protocol. The computation which is homomorphic can be resolved by our protocol. Thirdly, from the view of utilities, correctness, Nash equilibrium and fairness, analyses show that our protocol is rational. Besides, our protocol is also proved to be secure, efficient and practical. Our research will promote the development of rational quantum multi-party protocol.

Keywords Quantum secure multi-party computation · Rational player · Multifunctional function · Homomorphic computation

1 Introduction

In secure multi-party computation (MC) problem, each player has an input which cannot be revealed to anyone else. Players want to compute the value of function in private. This kind of problem is first proposed by Yao [1]. He introduced the two-party millionaire problem, where two millionaires want to compare their values of assets without the help of any others. Another important problem is multi-party summation [2–4], in which players need to compute the summation of their private inputs. With the

✉ Gang Xu
gangxu_bupt@163.com

1 Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

2 Guizhou Provincial Key Laboratory of Public Big Data, GuiZhou University, Guiyang 550025, Guizhou, China

development of cloud computing [5], security of computation and secure MC attract a great deal of attention.

Because of the uncertainty principle, no-cloning theorem and entanglement, quantum cryptography provides the possibility of designing an unconditional secure protocol [6, 7]. Quantum version solutions of secure MC problem are researched widely [8–12]. For example, in 2007, Du et al. [10] proposed an n-party quantum addition module $n+1$ protocol based on non-orthogonal states. After that, a quantum addition module 2 protocol via multi-particle entangled states was investigated by Chen et al. [11]. Recently, a secure summation and a secure multiplication protocols were given by Shi et al. [12]. The module of Shi et al.'s protocol is 2^m. Here m is the number of bits.

In common protocols, players are supposed to be honest, semi-honest or dishonest. Players under different assumptions have different behavior patterns. In other word, their behaviors are limited by these assumptions, instead of free. Therefore, these protocols are not reasonable enough. Another weakness of common protocols is that fairness is usually not concerned. For example, in an MC protocol, one player may obtain the result but not inform it to the others. In this case, the other players have no choice to obtain the result. This case is unfair for them. Under the circumstances, rational protocols were introduced. In this kind of protocols, players are supposed to be rational and will perform the protocol for their own benefits. They may cooperate with the others faithfully, send false information, perform false operations or give up. The only principle is to maximize their benefits. In addition, a rational protocol should be fair for players. The probabilities of each player gaining the result should be equal.

In 2004, Halpern et al. [13] designed a rational three-party secret sharing protocol. Each player can generate a random bit 0 or 1 with probability α or $1-\alpha$, respectively, and choose a strategy according to this bit. The expected running rounds are $5/\alpha^3$. Authors proved that there exists no deterministic rational MC protocol at the same time. In 2015, Zhang et al. proposed a verifiable rational secret sharing scheme [14]. A non-interactively verifiable proof is provided for the correctness of players' share. After that, Wang et al. [15] represented the research status of rational secure multi-party computing and some typical protocols. In 2016, Wang et al. [16] utilized fuzzy theory to research rational computing protocol. Compared with previous protocols, round complexity can be reduced in Wang et al.'s [16].

In 2015, Maitra et al. [17] firstly introduced rational players into quantum protocol and investigated rational quantum secret sharing (QSS) protocol. A (3, 7) threshold protocol was proposed at first. Then, it was generalized to (k, n) version. Actually, the shared secret is a quantum state in their protocol. This kind of QSS is usually called as quantum state sharing (QSTS). After that, Dou et al. [18] also proposed a rational QSTS protocol. Concretely, authors improved Li et al.'s QSTS protocol [19] to the rational version. Since only one player can get the state, i.e., the result, QSTS protocol is different from the others. Therefore, the definitions of utilities, correctness and fairness of rational QSTS were creatively given. Besides that, assumptions in this protocol are more practical and reasonable than previous ones.

In this paper, we follow the research on rational quantum protocol and design a rational quantum MC protocol. We focus on a kind of MC problems which are homomorphic, including but not limited to summation, multiplication, anonymous ranking. Firstly, a rational summation protocol is given as an example. Just like Halpern et al.'s protocol [13], players in our protocol also need to generate some random bits and determine their strategies thereafter. An improvement is that punishment is introduced into protocol to make players tend to send their inputs. Secondly, multi-party problems which can be computed by our protocol are discussed. If the key computation of a solution for a problem is homomorphic [20], this solution can be modified into a rational protocol. This problem can be resolved by our protocol further. Thirdly, utilities, correctness, Nash equilibrium, and fairness are analyzed. In order to achieve the last three characteristics, players can choose suitable coefficients. Our protocol satisfies all the criteria of rational protocol actually. Last but not least, another three analyses are also given. We analyze the security, calculate probabilities of the best and worst cases, and compare our protocol with Halpern et al.'s [13] and Maitra et al.'s [17]. These show that our protocol is secure, efficient and multifunctional. What's more, no presupposition holds when analyzing players' decision.

The structure of this paper is organized as follows. Preliminaries about rational MC and homomorphic function are given in Sect. 2. After that, we describe the proposed protocol in Sect. 3. Detailed analyses about our protocol are shown in Sect. 4. Finally, conclusions are given in Sect. 5.

2 Preliminaries

2.1 Rational multi-party computation

For an n-party game $\Gamma = (\{P_i\}_{i=1}^n, \{A_i\}_{i=1}^n, \{U_i\}_{i=1}^n)$, P_i denotes the ith player, $a_i \in A_i$ is one of his strategies. A_i is his strategy set further. Let $A = A_1 \times A_2 \times \cdots \times A_n$, then $\boldsymbol{a} = (a_1, a_2, \ldots, a_n) \in A$ denotes a strategy vector of this game, $\boldsymbol{o}(\boldsymbol{a}) = (o_1, o_2, \ldots, o_n)$ is the corresponding outcome, $U_i(\boldsymbol{a})$ is P_i's utility in this case. What's more, if P_i prefers $\boldsymbol{a}$ than $\boldsymbol{a}'$, then $U_i(\boldsymbol{a}) > U_i(\boldsymbol{a}')$. Besides that, for any given strategy vector $\boldsymbol{a}$, we define $\boldsymbol{a}_{-i} = (a_1, a_2, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$, and can get $(a_i', \boldsymbol{a}_{-i}) = (a_1, a_2, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$ naturally.

In rational MC problem, we also introduce a symbol $\text{info}_i(\boldsymbol{a})$ to describe whether the player P_i can get the computation result in strategy vector $\boldsymbol{a}$. Here $\text{info}_i(\boldsymbol{a}) = 1$ if P_i can obtain the result, $\text{info}_i(\boldsymbol{a}) = 0$ if not. Three notes, which will be mentioned in following sections, are shown here.

(N1) If $\text{info}_i(\boldsymbol{a}) > \text{info}_i(\boldsymbol{a}')$, then $U_i(\boldsymbol{a}) > U_i(\boldsymbol{a}')$.
(N2) If $\text{info}_i(\boldsymbol{a}) = \text{info}_i(\boldsymbol{a}')$, $\text{info}_j(\boldsymbol{a}) \geq \text{info}_j(\boldsymbol{a}')$ for all the $j \neq i$, and $\text{info}_k(\boldsymbol{a}) > \text{info}_k(\boldsymbol{a}')$ for at least one player P_k, then $U_i(\boldsymbol{a}) < U_i(\boldsymbol{a}')$.
(N3) If $\text{info}_i(\boldsymbol{a}) = \text{info}_i(\boldsymbol{a}')$, $\text{info}_j(\boldsymbol{a}) \leq \text{info}_j(\boldsymbol{a}')$ for all the $j \neq i$, and $\text{info}_k(\boldsymbol{a}) < \text{info}_k(\boldsymbol{a}')$ for at least one player P_k, then $U_i(\boldsymbol{a}) > U_i(\boldsymbol{a}')$.

Definition 1 (*Pure Strategy Nash Equilibrium* [21]) A strategy vector $\boldsymbol{a}$ in the game Γ is a *pure strategy Nash equilibrium*, if we have

$$U_i(a_i', \boldsymbol{a}_{-i}) \leq U_i(\boldsymbol{a}) \tag{1}$$

for each player P_i and his any other strategy a_i'.

Definition 2 (*Mixed Strategy* [21]) In game Γ, a player P_i has a strategy set $A_i = \{a_{i1}, a_{i2}, \ldots, a_{iK}\}$. A *mixed strategy* of P_i is denoted as $\Pr_i = \{p_{i1}, p_{i2}, \ldots, p_{iK}\}$, which means that P_i chooses a_{ij} with probability p_{ij}, $0 \leq p_{ij} < 1$, and $\sum_{j=1}^{K} p_{ij} = 1$. The mixed strategies of all the other players are denoted as $\Pr_{-i} = (\Pr_1, \Pr_2, \ldots, \Pr_{i-1}, \Pr_{i+1}, \ldots, \Pr_n)$, the mixed strategies of all the players are denoted as $\Pr = (\Pr_1, \Pr_2, \ldots, \Pr_n)$ further.

Definition 3 (*Mixed Strategy Nash Equilibrium* [21]) A strategy vector Pr in the game Γ is a *mixed strategy Nash equilibrium*, if we have

$$U_i(\Pr_i', \Pr_{-i}) \leq U_i(\Pr) \tag{2}$$

for each player P_i and his any other strategy $\Pr_i'$.

Besides that, utilities, correctness, and fairness of rational multi-party protocol are described and analyzed in Sect. 4.

2.2 Homomorphic function

For a multivariate function $y = f(x_1, x_2, \ldots, x_n)$, $x_i \in A_i$, domain of function f is $A_1 \times A_2 \times \cdots \times A_n$. Accordingly, range is $f(A_1 \times A_2 \times \cdots \times A_n)$.

The addition in domain and range are denoted as $\circ$ and $\odot$, respectively. The function f is homomorphic if for any $x_i, x_i' \in A_i$, $y = f(x_1, x_2, \ldots, x_n)$, $y' = f(x_1', x_2', \ldots, x_n')$, we have

$$y'' = f(x_1 \circ x_1', x_2 \circ x_2', \ldots, x_n \circ x_n') = y \odot y'. \tag{3}$$

Thus, another way to compute y is:

$$\begin{aligned} y &= y'' \odot y'^{-1} \\ &= f(x_1 \circ x_1', x_2 \circ x_2', \ldots, x_n \circ x_n') \odot [f(x_1', x_2', \ldots, x_n')]^{-1}. \end{aligned} \tag{4}$$

Here y'^{-1} is the inverse element of y' in range.

3 The proposed rational quantum multi-party computation protocol

At first, a new rational multi-party summation protocol based on common protocols is investigated in Sect. 3.1. In order to solve more MC problems, this protocol is modified to a multifunctional rational MC protocol in Sect. 3.2.

3.1 A new rational quantum summation protocol

Suppose that there are n players who want to compute the summation of their private data. For the ith player P_i, his secret can be written as a d-ary number $M_i \in \{0, \ldots, d-$

1}, where $i \in \{1, 2, \ldots, n\}$, d is a prime number. The jth round processes of our protocol are shown as follows:

[S-1] In the jth round, he generates a random number $R_{ij} \in \{0, \ldots, d-1\}$ and computes $MR_{ij} = M_i \oplus_d R_{ij}$, here $\oplus_d$ denotes the addition module d.
[S-2] Then, a common quantum summation protocol is performed. All the players compute the summation of MR_{ij}. The result is denoted as S_{1j}. Here any protocol could be employed as long as it is secure and correct.
[S-3] P_i chooses a bit c_{ij}. The probability of $c_{ij} = 0$ is α, and the probability of $c_i = 1$ is $1-\alpha$ accordingly. Then, he randomly generates $n-2$ bits $c_{ij}^{(1)}, \ldots, c_{ij}^{(i-1)}$, $c_{ij}^{(i+1)}, \ldots, c_{ij}^{(n-1)}$ and computes $c_{ij}^{(n)} = c_{ij} \oplus c_{ij}^{(1)} \oplus \cdots \oplus c_{ij}^{(i-1)} \oplus c_{ij}^{(i+1)} \oplus \cdots \oplus c_{ij}^{(n-1)}$, here $\oplus$ denotes the addition module 2.
[S-4] P_i sends $c_{ij}^{(k)}$ to P_k for $k \in \{1, \ldots, i-1, i+1, \ldots, n\}$. Then, P_i computes $q_{ij} = c_{1j}^{(i)} \oplus c_{2j}^{(i)} \oplus \cdots \oplus c_{(i-1)j}^{(i)} \oplus c_{(i+1)j}^{(i)} \oplus \cdots \oplus c_{nj}^{(i)}$, and publishes it. Each player can compute $q_j = \oplus_{i=1}^{n} q_{ij} = \oplus_{i=1}^{n} c_{ij}$ by himself. If $q_j = c_{ij} = 0$, then player P_i sends R_{ij} to the others. If $q_j = 0$ but $c_{ij} = 1$, P_i does nothing. Otherwise, $q_j = 1$, then all the players come to the next round.
[S-5] After that, if $q_j = 0$ but neither of players collects all the n random numbers $R_{1j}, R_{2j}, \ldots, R_{nj}$, all of them publish their bits $c_{ij}^{(k)}$, and check which player (named as P_m) should send his R_{mj}. The player who did not publish R_{mj} in this round needs to send his random number before the others in the next λ rounds. Here λ is a constant.
Otherwise, at least one player has collected all, he can obtain the summation of R_{ij}. The result is denoted as S_{2j}. Finally, the player can compute the summation of their secret M_i as $S_j = S_{1j} \ominus_d S_{2j}$. Here $\ominus_d$ is the subtraction module d.

3.2 Multifunctional rational protocol of quantum secure multi-party computation

Next, the rational multi-party summation protocol will be generalized to a rational MC protocol.

A MC problem could be regarded as a multivariate function $y = f(x_1, x_2, \ldots, x_n)$. Inputs and output correspond to independent variables and dependent variable, respectively. As one of the MC problems, multi-party summation also could be denoted as function $y = x_1 \oplus_d x_2 \oplus_d \cdots \oplus_d x_n$ which is homomorphic. Therefore, from the view of multivariate function, operation $M_i \oplus_d R_{ij}$ in our protocol corresponds to operation $x_i \circ x_i'$ in Sect. 2.2. Likewise, $S_{1j} \ominus_d S_{2j}$ corresponds to $y'' \odot y'^{-1}$.

Furthermore, in order to modify the protocol in Sect. 3.1 to a rational MC protocol, calculations players need to make should be changed from $M_i \oplus_d R_{ij}$ to $x_i \circ x_i'$ in step [S-1], and from $S_{1j} \ominus_d S_{2j}$ to $y'' \odot y'^{-1}$ in step [S-5]. Since Eq. (4) holds only for homomorphic function, our protocol could be employed to resolve the problem which could be regarded as homomorphic function.

Next, we will discuss common MC problems which could satisfy above requirement. As we have shown, multi-party summation is one of them. Addition of inputs x_i could be computed by equation

$$x_1 + x_2 + \cdots + x_n = \left(x_1 + x_1'\right) + \left(x_2 + x_2'\right) + \cdots + \left(x_n + x_n'\right) - \left(x_1' + x_2' + \cdots + x_n'\right). \tag{5}$$

Similarly, multi-party multiplication also belongs to this set. Multiplication could be computed by

$$x_1 x_2 \ldots x_n = \left(x_1 x_1'\right)\left(x_2 x_2'\right) \ldots \left(x_n x_n'\right) / \left(x_1' x_2' \ldots x_n'\right). \tag{6}$$

Since d is a prime number, $x_1' x_2' \ldots x_n' \equiv 0 \bmod d$ only if one of $x_i' = 0$. In order to avoid this case, we can let $x_i' \neq 0$.

If we reread existing quantum MC protocols, and check the key of their solutions, we can find some other examples. In many quantum millionaire protocols [8, 9], problem is resolved by subtraction essentially. The third party needs to compute $x_i - x_j$ to determine which input is bigger. Subtraction is the inverse operation of addition, so this problem could be resolved by our protocol. Another example is quantum anonymous ranking protocols [22, 23]. In these protocols, if a player holds a value, he will add 1, i.e., perform an operation on the corresponding particle. In the end, players can obtain the number of addition which is applied to each value and the rank of each value further.

Actually, as Shi et al. mentioned in Ref. [12], summation and multiplication are both fundamental primitives of secure MC. Many computations could be performed on the basis of them, such as average, maximum and minimum. In other words, our protocol is multifunctional and has a wide range of applications.

4 Analyses

In this section, some analyses about the protocol are given. Utilities, correctness, Nash equilibrium, fairness are analyzed. These show that our protocol is rational. Furthermore, security, probabilities of two protocol outcomes and comparison are also analyzed. Our protocol is also secure, efficient and practical.

The processes of our protocol can be divided as two parts: steps [S-1]–[S-2] which are based on common secure quantum multi-party computation protocol and steps [S-3]–[S-5] which could be regarded as rational classical secret sharing protocol. These two parts can be called as quantum stage and classical stage, respectively. They will be mentioned next.

4.1 Utilities

In quantum stage, a player will be chosen to compute and publish the value of summation. His role is different from the others'. We can denote this player as P_1. Concretely, P_1 will determine whether compute and publish the value of S_{1j}, while the others will choose whether encode their MR_{ij} $(i \neq 1)$ to help P_1 before that. However, in classical stage, all the players' roles are same. They may send their random number R_{ij} or not. Here strategies, corresponding outcomes, explanations and utilities of all the cases are described in Table 1. They will be employed in the following analyses.

Table 1 The detailed strategies, outcomes, explanations and utilities

Stage	Role	Strategy	Outcome	Explanation	Utility
Quantum	$P_i(i \neq 1)$	*Cooperating*	*Successful code*	$P_i(i \neq 1)$ encodes his MR_{ij} to help P_1. P_1 obtains all the MR_{ij} successfully	U_c
Quantum	$P_i(i \neq 1)$	*Cooperating*	*Unsuccessful code*	$P_i(i \neq 1)$ encodes his MR_{ij} to help P_1, but someone else does not	U_{uc}
Quantum	$P_i(i \neq 1)$	*Stopping1*	*Abandoned code*	$P_i(i \neq 1)$ does not encode his MR_{ij} to help P_1	U_a
Quantum	P_1	*Publishing*	*Public code*	P_1 computes and publishes S_{1j}	U_p
Quantum	P_1	*Stopping2*	*Private code*	P_1 does not compute or publish S_{1j}	U_{ud}
Quantum	P_1	*Null*	*Failed code*	Not all the players encode their MR_{ij}, so P_1 has nothing to compute or publish	U_f
Classical	Any player P_i	*Sending*	*Successful computation*	P_i sends his random number R_{ij}, all the $\text{info}_k(\boldsymbol{a}) = 1$ for $1 \leq k \leq n$	U_s
Classical	Any player P_i	*Sending*	*Someone else computation*	P_i sends R_{ij}, $\text{info}_i(\boldsymbol{a}) = 0$, but $info_k(\boldsymbol{a}) = 1$ for another P_k	U_{us}
Classical	Any player P_i	*Sending*	*Unsuccessful computation*	P_i sends R_{ij}, all the $\text{info}_k(\boldsymbol{a}) = 0$ for $1 \leq k \leq n$	U_{sn}
Classical	Any player P_i	*Stopping3*	*No one computation*	When $c_{ij} = 1$, P_i does not send R_{ij}, all the $\text{info}_k(\boldsymbol{a}) = 0$ for $1 \leq k \leq n$	U_{nn}
Classical	Any player P_i	*Stopping3*	*Punished computation*	When $c_{ij} = 0$, P_i does not send R_{ij}, all the $\text{info}_k(\boldsymbol{a}) = 0$ for $1 \leq k \leq n$	U_{pn}
Classical	Any player P_i	*Stopping3*	*Only him computation*	P_i does not send R_{ij}, $\text{info}_i(\boldsymbol{a}) = 1$, but all the $\text{info}_k(\boldsymbol{a}) = 0$ for $k \neq i$	U_o
Classical	Any player P_i	*Sending/Stopping3*	*Wrong computation*	P_i obtains a wrong result	U_w

Some illustrations about utilities are given. (1) The classical stage will be performed if and only if all the players cooperate in the quantum stage. (2) If all the players choose to cooperate and publish, their utilities will be U_c and U_p, respectively. However, they will go to classical stage next, and their utilities can also be denoted as U_s, U_{us}, U_{sn}, U_{nn}, U_{pn}, U_w or U_o. Then, the latter seven symbols will be used to describe players' utilities, instead of the former two. (3) From notes (N1)–(N3), we can know that $U_o > U_s > U_{nn} > U_{us}$, $U_o > U_s > U_{pn} > U_{us}$ and $U_o > U_s > U_{sn} > U_{us}$. (4) Comparing the outcome "*Unsuccessful computation*" with "*Punished computation*," we find that no player can obtain S_{2j} or S_j in both cases. The difference is P_i sends his random number in the former case. Since the player who did not fulfill his obligations may be discovered at the end of round, we say that $U_{sn} > U_{pn}$. (5) Comparing the outcome "*Unsuccessful computation*" with "*No one computation*," we find that player fulfills his obligation, but no one can obtain the result in both cases. The only difference is the player sends R_{ij} in the former case. It means that he does some extra work, so it is easy to get $U_{sn} < U_{nn}$. Now, we can get $U_o > U_s > U_{nn} > U_{sn} > U_{pn} > U_{us}$ further.

In quantum stage, P_1 chooses to publish or stop after all the others encoded their MR_{ij}. This stage could be considered as a dynamic game. Game tree is a visual description to show this kind of game. Here the quantum stage is analyzed in four-party version. The game tree of this game Γ_1 is illustrated in Fig. 1. Dotted lines mean that P_2, P_3 and P_4 know nothing about each other's choice. In other words, they make choices at the same time.

If any player chooses the strategy *Stopping1* or *Stopping2*, none of players will obtain useful result. They would restart the game. Otherwise, all the players will obtain S_{1j} and go to the classical stage. From the view of type of game, if any agent is punished to send the random number before the others, it will be a dynamic game. Otherwise, all the players choose their strategies at the same time and are equivalent. It is a static game. Consider the type of game and the value of c_{kj}, four cases may occur: (1) Not all the $c_{kj} = 0$ in a static game; (2) all the $c_{kj} = 0$ in a static game; (3)

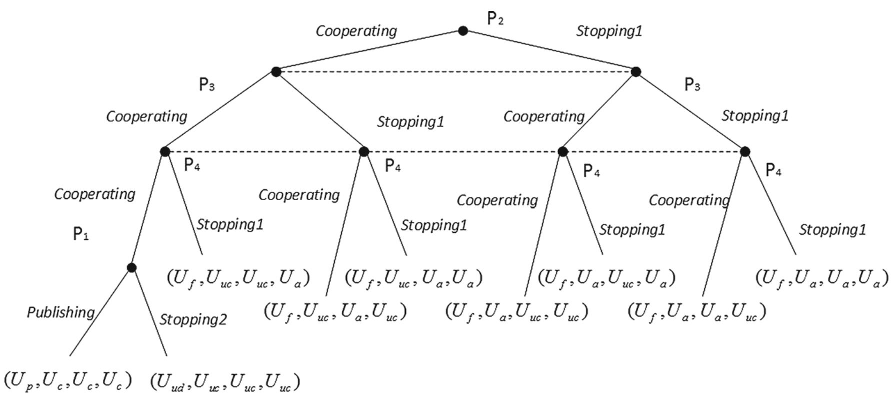

Fig. 1 Game tree of the quantum stage with four players

not all the other $c_{kj} = 0$ in a dynamic game; (4) all the other $c_{kj} = 0$ in a dynamic game. Four cases are analyzed with examples as follows:

(1) Since all the players are equivalent, we suppose $c_{1j} = c_{3j} = 1$ and $c_{2j} = c_{4j} = 0$, and denote this game as Γ_2. In this case, utilities of players in different strategy vectors are shown in Table 2.
(2) Here $c_{1j} = c_{2j} = c_{3j} = c_{4j} = 0$. Likewise, we denote this game as Γ_3. Utilities are also given in Table 3.
(3) Suppose P_1 is punished, and $c_{2j} = c_{3j} = c_{4j} = 0$. Game tree is also utilized to describe this game Γ_4(Fig. 2).
P_1 needs to make a decision at first. If he stopped, the others need not send, the utility vector is $(U_{pn}, U_{nn}, U_{nn}, U_{nn})$. Otherwise, they choose strategies at the same time. Similarly, dotted lines in Fig. 2 imply that they make choices at the same time.
(4) Likewise, suppose P_1 is punished, $c_{2j} = c_{3j} = 1$, and $c_{4j} = 0$ (Fig. 3).
The game tree of Γ_5 is similar with the tree of Γ_4. The differences are P_2's and P_3's utilities are changed from U_{pn} to U_{nn} if they choose *Stopping3*.

4.2 Correctness

Definition 4 (*Correctness* [17]) A rational multi-party protocol is *correct* if the following holds:

$$\Pr[o_{-i}(\Gamma, (a_i, a_{-i})) = \mathit{Wrong\ computation}] = 0 \tag{7}$$

for each player P_i's arbitrary strategy a_i.

Theorem 1 *The correctness is ensured if all the players are in fail-stop setting.*

Proof In our protocol, players are supposed to be in fail-stop, and they can only choose to send the number or not, instead of sending a false number. Because players' private inputs cannot be revealed to any other in MC protocol, authenticity of inputs also cannot be confirmed. The fail-stop setting is the best of a bad bunch. In this case, no player will get a wrong result, and correctness of protocol holds further. □

4.3 Nash equilibrium

Equilibrium is the situation in which all the players are balanced. Nash equilibrium of our protocol will be discussed below. The existence of Nash equilibrium is given.

Theorem 2 *There exist some values of x and α that make the protocol achieve mixed strategy Nash equilibrium.*

Proof As we have shown, in our protocol, quantum stage could be regarded as a dynamic game. If there is no punishment, classical stage is a static game. Otherwise, it is also dynamic.

Table 2 Utility matrix of four-party static game Γ_2

P_3		*Sending*		*Stopping*	
P_4		*Sending*	*Stopping*	*Sending*	*Stopping*
P_1	P_2				
Sending	*Sending*	(U_s, U_s, U_s, U_s)	$(U_{us}, U_{us}, U_{us}, U_o)$	$(U_{us}, U_{us}, U_o, U_{us})$	$(U_{sn}, U_{sn}, U_{nn}, U_{pn})$
	Stopping	$(U_{us}, U_o, U_{us}, U_{us})$	$(U_{sn}, U_{pn}, U_{sn}, U_{pn})$	$(U_{sn}, U_{pn}, U_{nn}, U_{sn})$	$(U_{sn}, U_{pn}, U_{nn}, U_{pn})$
Stopping	*Sending*	$(U_o, U_{us}, U_{us}, U_{us})$	$(U_{nn}, U_{sn}, U_{sn}, U_{pn})$	$(U_{nn}, U_{sn}, U_{nn}, U_{sn})$	$(U_{nn}, U_{sn}, U_{nn}, U_{pn})$
	Stopping	$(U_{nn}, U_{pn}, U_{sn}, U_{sn})$	$(U_{nn}, U_{pn}, U_{sn}, U_{pn})$	$(U_{nn}, U_{pn}, U_{nn}, U_{sn})$	$(U_{nn}, U_{pn}, U_{nn}, U_{pn})$

Table 3 Utility matrix of four-party static game Γ_3

P_3		*Sending*		*Stopping*	
P_4		*Sending*	*Stopping*	*Sending*	*Stopping*
P_1	P_2				
Sending	*Sending*	(U_s, U_s, U_s, U_s)	$(U_{us}, U_{us}, U_{us}, U_o)$	$(U_{us}, U_{us}, U_o, U_{us})$	$(U_{sn}, U_{sn}, U_{pn}, U_{pn})$
	Stopping	$(U_{us}, U_o, U_{us}, U_{us})$	$(U_{sn}, U_{pn}, U_{sn}, U_{pn})$	$(U_{sn}, U_{pn}, U_{pn}, U_{sn})$	$(U_{sn}, U_{pn}, U_{pn}, U_{pn})$
Stopping	*Sending*	$(U_o, U_{us}, U_{us}, U_{us})$	$(U_{pn}, U_{sn}, U_{sn}, U_{pn})$	$(U_{pn}, U_{sn}, U_{pn}, U_{sn})$	$(U_{pn}, U_{sn}, U_{pn}, U_{pn})$
	Stopping	$(U_{pn}, U_{pn}, U_{sn}, U_{sn})$	$(U_{pn}, U_{pn}, U_{sn}, U_{pn})$	$(U_{pn}, U_{pn}, U_{pn}, U_{sn})$	$(U_{pn}, U_{pn}, U_{pn}, U_{pn})$

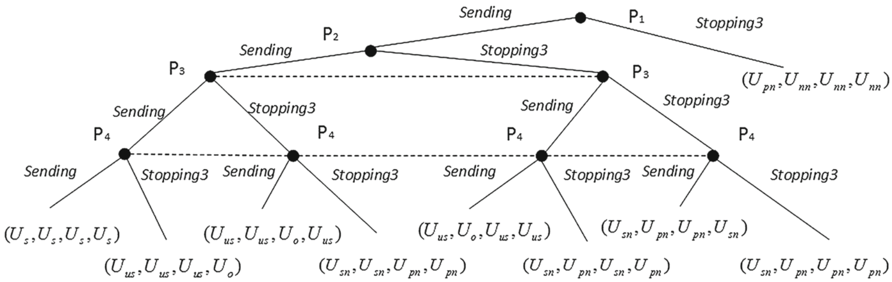

Fig. 2 Game tree of four-party dynamic game Γ_4

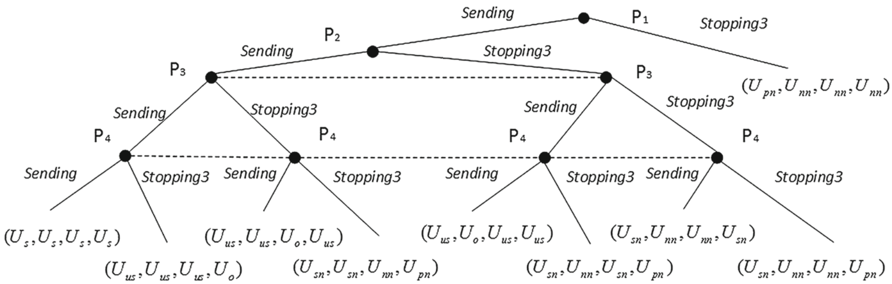

Fig. 3 Game tree of four-party dynamic game Γ_5

For static game, pure strategy or mixed strategy Nash equilibrium could be obtained easily. However, for dynamic game, backward induction is one of the most important methods. Specifically, the player who selects strategy earlier will consider which strategy the latter one may choose. Consequently, if we deduce which strategy the last player will choose in each case and which strategies the other players will choose backward one by one, the equilibrium of this game and the path to this equilibrium will be obtained. For the sake of describing our analysis more clearly, we take the four-party game as an example and then generalize the analysis to the n-party game.

(1) Four-party game

Firstly, the game Γ_5 will be analyzed. The game among players P_2, P_3 and P_4 can be denoted as a static sub-game Γ_6 which can be described by utility matrix (Table 4).

Since $U_o > U_s > U_{nn} > U_{sn} > U_{pn} > U_{us}$, it is easy to find that there only exists one Nash equilibrium: (*Sending*, *Stopping3*, *Stopping3*, *Sending*). Utilities of players are $(U_{sn}, U_{nn}, U_{nn}, U_{sn})$. In other words, a player will choose *Sending* if he has $c_{ij} = 0$, choose *Stopping3* if $c_{ij} = 1$. This conclusion could be generalized to n-party version when $q_j = 0$ but not all the $c_{kj} = 0$.

Secondly, we analyze the game Γ_4. The game among players P_2, P_3 and P_4 can be denoted as a sub-game Γ_7, which can also be described by utility matrix (Table 5).

From Table 5, we could find three pure strategy Nash equilibriums. However, since players do not know each other's strategy, they only have to choose a mixed strategy. The mixed strategy Nash equilibrium will be sought later. Here, we suppose that P_2, P_3 and P_4 choose the strategy *Sending* with probability p'_2, p'_3 and p'_4, respectively.

Table 4 Utility matrix of sub-game Γ_6

P_3		*Sending*		*Stopping*	
P_4		*Sending*	*Stopping*	*Sending*	*Stopping*
P_1	P_2				
Sending	*Sending*	(U_s, U_s, U_s, U_s)	$(U_{us}, U_{us}, U_{us}, U_o)$	$(U_{us}, U_{us}, U_o, U_{us})$	$(U_{sn}, U_{sn}, U_{nn}, U_{pn})$
	Stopping	$(U_{us}, U_o, U_{us}, U_{us})$	$(U_{sn}, U_{nn}, U_{sn}, U_{pn})$	$(U_{sn}, U_{nn}, U_{nn}, U_{sn})$	$(U_{sn}, U_{nn}, U_{nn}, U_{pn})$

Table 5 Utility matrix of sub-game Γ_7

P_3		*Sending*		*Stopping*	
P_4		*Sending*	*Stopping*	*Sending*	*Stopping*
P_1	P_2				
Sending	*Sending*	(U_s, U_s, U_s, U_s)	$(U_{us}, U_{us}, U_{us}, U_o)$	$(U_{us}, U_{us}, U_o, U_{us})$	$(U_{sn}, U_{sn}, U_{pn}, U_{pn})$
	Stopping	$(U_{us}, U_o, U_{us}, U_{us})$	$(U_{sn}, U_{pn}, U_{sn}, U_{pn})$	$(U_{sn}, U_{pn}, U_{pn}, U_{sn})$	$(U_{sn}, U_{pn}, U_{pn}, U_{pn})$

Each player chooses suitable p_i' to makes the others' utilities completely equal when choosing different strategies. The following three equations can be deduced.

$$\begin{aligned} & p_3'p_4'U_s + p_3'(1-p_4')U_{us} + (1-p_3')p_4'U_{us} + (1-p_3')(1-p_4')U_{sn} \\ & \quad = p_3'p_4'U_o + p_3'(1-p_4')U_{pn} + (1-p_3')p_4'U_{pn} + (1-p_3')(1-p_4')U_{pn}. \end{aligned} \tag{8}$$

$$\begin{aligned} & p_2'p_4'U_s + p_2'(1-p_4')U_{us} + (1-p_2')p_4'U_{us} + (1-p_2')(1-p_4')U_{sn} \\ & \quad = p_2'p_4'U_o + p_2'(1-p_4')U_{pn} + (1-p_2')p_4'U_{pn} + (1-p_2')(1-p_4')U_{pn}. \end{aligned} \tag{9}$$

$$\begin{aligned} & p_2'p_3'U_s + p_2'(1-p_3')U_{us} + (1-p_2')p_3'U_{us} + (1-p_2')(1-p_3')U_{sn} \\ & \quad = p_2'p_3'U_o + p_2'(1-p_3')U_{pn} + (1-p_2')p_3'U_{pn} + (1-p_2')(1-p_3')U_{pn}. \end{aligned} \tag{10}$$

In order to simplify the calculation, let $a = U_s - U_o < 0$, $d = U_{sn} - U_{us} > 0$, $x = U_{sn} - U_{pn} > 0$. After computation, we find that the solution of Eqs. (8)–(10) is

$$p' = \begin{cases} \frac{d-\sqrt{(d-x)^2-ax}}{a+2d-x}, & \text{if } a+2d-x \neq 0 \\ 1+\frac{a}{2d}, & \text{if } a+2d-x = 0 \end{cases}. \tag{11}$$

Here $0 < p' = p_2' = p_3' = p_4' < 1$. Utility expectation of players P_2, P_3 and P_4 is $U_{ex} = 2d(e-a+x)\frac{d-\sqrt{(d-x)^2-ax}}{(a+2d-x)^2} - \frac{(2d+e)x}{a+2d-x} + U_{sn}$ if $a+2d-x \neq 0$. $U_{ex} = e - a + \frac{a(2d+e)}{d} + \frac{a^2(2d+e)}{4d^2} + U_{sn}$ if $a+2d-x = 0$. Here $e = U_s - U_{sn}$.

For the sake of simplicity, we further suppose that utilities approximatively constitute an arithmetic progression, i.e., $a = -1$, $d = 2$ and $e = 1$, then $0 < x < 2$. Utility expectation of player P_1 if he chooses to send is

$$U_{1se} = \frac{(24\sqrt{x^2-3x+4}+24)x - 6x^2 - 6x^3 + 12\sqrt{x^2-3x+4} + 7\sqrt{(x^2-3x+4)^3} - 80}{(x-3)^3} + U_{sn}. \tag{12}$$

If and only if $U_{1se} > U_{pn}$, P_1 will send his random number. Fortunately, this inequality holds true for any $0 < x < 2$. The image of $U_{1se} - U_{pn}$ is drawn in Fig. 4 to show it.

From this figure, we can know that $U_{1se} - U_{pn}$ is always bigger than 0, and positively related to x. In a word, P_1 will send even if he is punished.

Thirdly, Γ_3 could be analyzed. Similarly, although there exist six pure strategy equilibriums, players will choose mixed strategies actually. We also suppose $a = -1$, $d = 2$ and $e = 1$, then $0 < x < 2$. The probability of sending is p_i'' for player P_i. Just similar as the first case, the following equations can also be deduced.

$$\begin{aligned} & p_2''p_3''p_4''U_s + p_2''p_3''(1-p_4'')U_{us} + p_2''(1-p_3'')p_4''U_{us} + p_2''(1-p_3'')(1-p_4'')U_{sn} \\ & + (1-p_2'')p_3''p_4''U_{us} + (1-p_2'')p_3''(1-p_4'')U_{sn} + (1-p_2'')(1-p_3'')p_4''U_{sn} \\ & + (1-p_2'')(1-p_3'')(1-p_4'')U_{sn} = p_2''p_3''p_4''U_o + p_2''p_3''(1-p_4'')U_{pn} + p_2''(1-p_3'')p_4''U_{pn} \\ & + p_2''(1-p_3'')(1-p_4'')U_{pn} + (1-p_2'')p_3''p_4''U_{pn} + (1-p_2'')p_3''(1-p_4'')U_{pn} \\ & + (1-p_2'')(1-p_3'')p_4''U_{pn} + (1-p_2'')(1-p_3'')(1-p_4'')U_{pn}. \end{aligned} \tag{13}$$

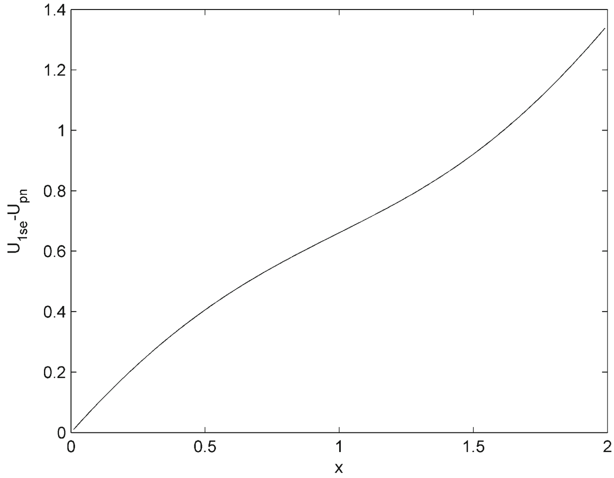

Fig. 4 The relationship between $U_{1se} - U_{pn}$ and x

$$
\begin{aligned}
& p_1'' p_3'' p_4'' U_s + p_1'' p_3'' (1 - p_4'') U_{us} + p_1'' (1 - p_3'') p_4'' U_{us} + p_1'' (1 - p_3'') (1 - p_4'') U_{sn} \\
& \quad + (1 - p_1'') p_3'' p_4'' U_{us} + (1 - p_1'') p_3'' (1 - p_4'') U_{sn} + (1 - p_1'') (1 - p_3'') p_4'' U_{sn} \\
& \quad + (1 - p_1'') (1 - p_3'') (1 - p_4'') U_{sn} = p_1'' p_3'' p_4'' U_o + p_1'' p_3'' (1 - p_4'') U_{pn} + p_1'' (1 - p_3'') p_4'' U_{pn} \\
& \quad + p_1'' (1 - p_3'') (1 - p_4'') U_{pn} + (1 - p_1'') p_3'' p_4'' U_{pn} + (1 - p_1'') p_3'' (1 - p_4'') U_{pn} \\
& \quad + (1 - p_1'') (1 - p_3'') p_4'' U_{pn} + (1 - p_1'') (1 - p_3'') (1 - p_4'') U_{pn}. \qquad (14)
\end{aligned}
$$

$$
\begin{aligned}
& p_1'' p_2'' p_4'' U_s + p_1'' p_2'' (1 - p_4'') U_{us} + p_1'' (1 - p_2'') p_4'' U_{us} + p_1'' (1 - p_2'') (1 - p_4'') U_{sn} \\
& \quad + (1 - p_1'') p_2'' p_4'' U_{us} + (1 - p_1'') p_2'' (1 - p_4'') U_{sn} + (1 - p_1'') (1 - p_2'') p_4'' U_{sn} \\
& \quad + (1 - p_1'') (1 - p_2'') (1 - p_4'') U_{sn} = p_1'' p_2'' p_4'' U_o + p_1'' p_2'' (1 - p_4'') U_{pn} + p_1'' (1 - p_2'') p_4'' U_{pn} \\
& \quad + p_1'' (1 - p_2'') (1 - p_4'') U_{pn} + (1 - p_1'') p_2'' p_4'' U_{pn} + (1 - p_1'') p_2'' (1 - p_4'') U_{pn} \\
& \quad + (1 - p_1'') (1 - p_2'') p_4'' U_{pn} + (1 - p_1'') (1 - p_2'') (1 - p_4'') U_{pn}. \qquad (15)
\end{aligned}
$$

$$
\begin{aligned}
& p_1'' p_2'' p_3'' U_s + p_1'' p_2'' (1 - p_3'') U_{us} + p_1'' (1 - p_2'') p_3'' U_{us} + p_1'' (1 - p_2'') (1 - p_3'') U_{sn} \\
& \quad + (1 - p_1'') p_2'' p_3'' U_{us} + (1 - p_1'') p_2'' (1 - p_3'') U_{sn} + (1 - p_1'') (1 - p_2'') p_3'' U_{sn} \\
& \quad + (1 - p_1'') (1 - p_2'') (1 - p_3'') U_{sn} = p_1'' p_2'' p_3'' U_o + p_1'' p_2'' (1 - p_3'') U_{pn} + p_1'' (1 - p_2'') p_3'' U_{pn} \\
& \quad + p_1'' (1 - p_2'') (1 - p_3'') U_{pn} + (1 - p_1'') p_2'' p_3'' U_{pn} + (1 - p_1'') p_2'' (1 - p_3'') U_{pn} \\
& \quad + (1 - p_1'') (1 - p_2'') p_3'' U_{pn} + (1 - p_1'') (1 - p_2'') (1 - p_3'') U_{pn}. \qquad (16)
\end{aligned}
$$

The solution is:

$$p'' = \frac{2 + 2\left(\cos\frac{\theta}{3} - \sqrt{3}\sin\frac{\theta}{3}\right)}{5 - x}. \qquad (17)$$

Here $\theta = \arccos\left(\frac{x(x-5)^2}{16} - 1\right)$, $0 < p'' = p_1'' = p_2'' = p_3'' = p_4'' < 1$. The utility expectation of each player is $U_{ex2} = (p'')^2(7p'' - 6) + U_{sn}$.

Fourthly, Γ_2 could be analyzed. This game is very similar to Γ_6. Likewise, there only exists one Nash equilibrium: (*Stopping3*, *Sending*, *Stopping3*, *Sending*). Utilities of players are $(U_{nn}, U_{sn}, U_{nn}, U_{sn})$.

Fifthly, consider the game Γ_1. We analyze this game simply. If players do not go to the classical stage, they will get nothing. Otherwise, they may get the result of computation. That is to say, they will all cooperate to go to classical stage.

In conclusion, player P_i will choose *Stopping3* without doubt if $q_j = 1$ or $c_{ij} = 1$, he will consider whether sending or not only if $q_j = c_{ij} = 0$. There are two cases when $q_j = c_{ij} = 0$: (1) Two of three other players hold $c_{kj} = 1$ with probability $3\alpha(1-\alpha)^2$. P_i will choose *Sending* without doubt. (2) All the other c_{kj} are equal to 0 with probability α^3. In this case, P_i will choose *Sending* with probability p''. Hence, the conditional probability of case (1) is $3(1-\alpha)^2/(4\alpha^2 - 6\alpha + 3)$, case (2) is $\alpha^2/(4\alpha^2 - 6\alpha + 3)$. On the whole, if $q_j = c_{ij} = 0$, the probability of P_i sending is:

$$p_{wh} = \frac{\alpha^2}{4\alpha^2 - 6\alpha + 3} p'' + \frac{3(1-\alpha)^2}{4\alpha^2 - 6\alpha + 3}. \tag{18}$$

(2) n-party game

Similarly, in a n-party protocol, if all the $c_{kj} = 0\,(1 \le k \le n)$, mixed strategy Nash equilibrium could also be deduced. For the player P_i, the probability of sending is p_i. The other players will choose their probabilities to make:

$$p_{Ai} U_s + p_{Bi} U_{us} + p_{Ci} U_{sn} = p_{Ai} U_o + p_{Bi} U_{pn} + p_{Ci} U_{pn}. \tag{19}$$

Here $p_{Ai} = \prod_{j \ne i}^{n} p_j$, $p_{Bi} = \sum_{\substack{k=1 \\ k \ne i}}^{n} \prod_{\substack{j \ne i \\ j \ne k}}^{n} p_j(1-p_k)$, and $p_{Ci} = 1 - p_{Ai} - p_{Bi}$. If we put all P_i's equations together and simplify it, the following equation can be obtained.

$$\begin{aligned} &p^{n-1}a + (n-1)p^{n-2}(1-p)(x-d) + [1 + (n-2)p^{n-1} - (n-1)p^{n-2}]x = 0 \\ &\Rightarrow p^{n-1}[a + (n-1)d - x] - (n-1)p^{n-2}d + x = 0. \end{aligned} \tag{20}$$

Where $0 < p = p_1 = p_2 = \cdots = p_n < 1$. Let $g(p) = p^{n-1}[a + (n-1)d - x] - (n-1)p^{n-2}d + x$, it is easy to get $g(0) = x > 0$ and $g(1) = a < 0$. Thus, $g(p) = 0$ has a solution for $0 < p < 1$. In other words, each player can find a suitable p to make the other players' utilities the same when they choose different strategies. The mixed strategy Nash equilibrium is achieved.

In addition, as we mentioned in the four-party case, if $q_j = 0$ but not all the $c_{kj} = 0$ in an n-party protocol, a player will choose *Sending* if he has $c_{ij} = 0$, choose *Stopping3* if $c_{ij} = 1$.

Furthermore, we could also compute the probability of each player sending his random number if $q_j = c_{ij} = 0$. Just as we discussed before, there also are two cases: (1) even but not zero numbers of c_{kj} are equal to 1 with probability $\beta_{1n} =$

$\sum_{k=1}^{\lceil n/2 \rceil -1} C_{n-1}^{2k} \alpha^{n-2k-1}(1-\alpha)^{2k}$; (2) all the c_{kj} are equal to 0 with probability $\beta_{2n} = \alpha^{n-1}$. In general, if $q_j = c_{ij} = 0$, the probability of P_i sending is:

$$p_{nwh} = \frac{\beta_{2n}}{\beta_{1n} + \beta_{2n}} p + \frac{\beta_{1n}}{\beta_{1n} + \beta_{2n}}. \tag{21}$$

Here p is the solution of Eq. (20).

In summary, there exist some suitable coefficients x and α to make the protocol achieve mixed strategy Nash equilibrium. □

4.4 Fairness

Definition 5 (*Fairness* [17]) A rational multi-party protocol is *fair* if the following holds:

$$\begin{aligned} &\Pr[o_i(\Gamma, (a_i, a_{-i})) = Successful\ \ computation] \\ &\quad + \Pr[o_i(\Gamma, (a_i, a_{-i})) = Only\ \ him\ \ computation] \\ &\leq \Pr[o_{-i}(\Gamma, (a_i, a_{-i})) = Successful\ \ computation] \\ &\quad + \Pr[o_{-i}(\Gamma, (a_i, a_{-i})) = Only\ \ him\ \ computation] \end{aligned} \tag{22}$$

for each player P_i's arbitrary strategy a_i.

Theorem 3 *There exist some values of coefficients x and α that make the protocol achieve fairness.*

Proof Just like Ref. [17], for each player, if the probability of sending is very close to 1, he will not have incentive to deviate the protocol. Fairness of our protocol will be ensured further. As we analyzed in Sect. 4.3, in classical stage, player P_i will choose a mixed strategy if $q_j = c_{ij} = 0$. Next, we will discuss how to select coefficients to make the probability close to 1, i.e., $p_{nwh} = 99.95\%$.

We also suppose that $a = -1$, $d = 2$ and $e = 1$. Since $0 < x < 2$ and we hope that all the players send their R_{ij}, we give $x = 1.9 + \varepsilon$ (ε is a small number), then we can compute p and α to satisfy $p_{nwh} = 99.95\%$. When one of p and α is fixed, the other is determined. A possible pair of values of p and α is given in Table 6 for n=5, 10, 20, 50, 100, 200, 500, 1000. For the other value of n, it is also easy to find suitable x and α to make p_{nwh} close to 1. In other words, there exist some coefficients to ensure the fairness of protocol. □

4.5 Security

Firstly, in quantum stage, any secure quantum multi-party homomorphic computation protocol could be utilized as a black box, for example, Refs. [22, 23]. Since that, as long as the original protocol is secure, this stage is also secure.

Secondly, let us take our rational quantum summation protocol as an example. All the R_{ij} which are sent among different players are random in classical stage. Player P_1 cannot deduce any useful information about other players' inputs M_k from R_{kj}.

Table 6 Values of coefficients to make p_{nwh}= 99.95%

n	x	p	α	p_{nwh}
5	1.9004	0.7783	0.1878	0.9995
10	1.9007	0.9002	0.5129	0.9995
20	1.9034	0.9525	0.7584	0.9995
50	1.9022	0.9815	0.9159	0.9995
100	1.9146	0.9909	0.9643	0.9995
200	1.9257	0.9955	0.9856	0.9995
500	1.9213	0.9982	0.9961	0.9995
1000	1.9198	0.9991	0.9988	0.9995

Thirdly, since R_{ij} are random, MR_{ij} and S_{1j} are also random. It means that even if MR_{ij} and S_{1j} are revealed, the protocol is secure as long as the eavesdropping is found before all the players publish their R_{ij}. From this point of view, our protocol is something like quantum key distribution protocol [24, 25] or quantum key agreement protocol [26].

In other words, our protocol is more secure than general MC protocols. The security of our protocol holds easily.

4.6 Probability and efficiency

Let us look over all the outcomes of our protocol. The outcome *Successful computation* means that the protocol is performed successfully, which is desired for us. The probability of this outcome is p^n_{nwh} if all the $c_{ij} = 0$. What we last expect is the outcome *Only him/Someone else computation*, which happens if and only if only one player chooses *Stopping3* in classical stage. The probability of this outcome is $np^{n-1}_{nwh}(1 - p_{nwh})$ if all the $c_{kj} = 0$.

Just as we discussed before, p_{nwh} is related to coefficients α, p and n. At the same time, p is related to n and x. Here, we also give $x = 1.9 + \varepsilon$, then compute p when n=5, 10, 20, 50, 100, 200, 500, 1000. After that, we compute p_{nwh} which makes p^n_{nwh} two, ten, hundred times as big as $np^{n-1}_{nwh}(1 - p_{nwh})$, respectively. Next, α can be determined. We list all the coefficients in following tables.

From Tables 7, 8, 9, we can know that it is easy to make the probability of outcome *Successful computation* much bigger than *Only him/Someone else computation*. Therefore, the latter outcome would almost never happen. At the same time, the probability of outcome *Successful computation* could be very close to 1. This also shows that our protocol is efficient.

In addition, we can also find some relationships among coefficients. Firstly, if x is approximatively fixed, p increases with increasing n. Secondly, if x, p and n are all fixed, α decreases with increasing p_{nwh}. Thirdly, if x, p and $p^n_{nwh}/np^{n-1}_{nwh}(1 - p_{nwh})$ are all fixed, α decreases with increasing n. These relationships could help us to choose coefficients for protocol under different circumstances.

Table 7 Values of coefficients to make $p_{nwh}^{n}/np_{nwh}^{n-1}(1-p_{nwh})=2$

n	x	p	α	p_{nwh}	p_{nwh}^{n}	$np_{nwh}^{n-1}(1-p_{nwh})$
5	1.9004	0.7783	0.6754	0.9091	0.6209	0.3105
10	1.9007	0.9002	0.8571	0.9524	0.6139	0.3070
20	1.9034	0.9525	0.9341	0.9756	0.6103	0.3051
50	1.9022	0.9815	0.9750	0.9901	0.6080	0.3040
100	1.9146	0.9909	0.9879	0.9950	0.6073	0.3036
200	1.9257	0.9955	0.9940	0.9975	0.6069	0.3035
500	1.9213	0.9982	0.9976	0.9990	0.6067	0.3033
1000	1.9198	0.9991	0.9988	0.9995	0.6066	0.3033

Table 8 Values of coefficients to make $p_{nwh}^{n}/np_{nwh}^{n-1}(1-p_{nwh})=10$

n	x	p	α	p_{nwh}	p_{nwh}^{n}	$np_{nwh}^{n-1}(1-p_{nwh})$
5	1.9004	0.7783	0.4573	0.9804	0.9057	0.0906
10	1.9007	0.9002	0.7155	0.9901	0.9053	0.0905
20	1.9034	0.9525	0.8561	0.9950	0.9051	0.0905
50	1.9022	0.9815	0.9421	0.9980	0.9049	0.0905
100	1.9146	0.9909	0.9711	0.9990	0.9049	0.0905
200	1.9257	0.9955	0.9856	0.9995	0.9049	0.0905
500	1.9213	0.9982	0.9942	0.9998	0.9048	0.0905
1000	1.9198	0.9991	0.9971	0.9999	0.9048	0.0905

Table 9 Values of coefficients to make $p_{nwh}^{n}/np_{nwh}^{n-1}(1-p_{nwh})=100$

n	x	p	α	p_{nwh}	p_{nwh}^{n}	$np_{nwh}^{n-1}(1-p_{nwh})$
5	1.9004	0.7783	0.2616	0.9980	0.9901	0.0099
10	1.9007	0.9002	0.5545	0.9990	0.9901	0.0099
20	1.9034	0.9525	0.7583	0.9995	0.9901	0.0099
50	1.9022	0.9815	0.8988	0.9998	0.9901	0.0099
100	1.9146	0.9909	0.9488	0.9999	0.9901	0.0099
200	1.9257	0.9955	0.9742	1.0000	0.9901	0.0099
500	1.9213	0.9982	0.9896	1.0000	0.9900	0.0099
1000	1.9198	0.9991	0.9948	1.0000	0.9900	0.0099

4.7 Comparison

In this subsection, we compare our protocol with two valuable rational protocols, Halpern et al.'s classical protocol [13] and Maitra et al.'s quantum protocol [17], from the following aspects.

Firstly, we consider the application of the protocol. Halpern et al.'s protocol [13] is used to resolve secret sharing. Maitra et al.'s protocol [17] is utilized to settle sharing known quantum state. However, our protocol can be employed to solve various multi-party problems. This characteristic is a kind of universality of protocol [27]. As we all know, shares in players' hands are random in classical secret sharing, QSS and QSTS protocols. Therefore, they could be transmitted among players. However, in MC protocols, inputs of players are deterministic and private, so they could not be conveyed among players directly. In our protocol, we introduce random number to solve this problem. Only random numbers are transmitted, so true input of one player cannot be obtained by any others. Security of players' inputs is ensured in our protocol further.

Secondly, think about the assumption of the protocol. When Halpern et al. [13] and Maitra et al. [17] analyze P_1's strategy, they suppose that P_2 and P_3 will obey the protocol. In this situation, cooperation is better than deviation for the third party. This assumption is not practical because the others' strategies cannot be known beforehand for any player. In this paper, we analyze each case of players' strategies without presupposition.

Last but not least, consider the number of participants of the protocol. In Ref. [17], a (k, n) threshold protocol was investigated via quantum error correcting code. As for Ref. [13], Halpern et al. also generalized their three-party protocol to n-party version. Nevertheless, all the players are divided into three sets. In each set, players elect a leader and send shares to their leader. In the end, leaders perform the rational three-party protocol. This generalization is trivial. Compared with Ref. [13], in our n-party protocol, each player performs the protocol equally. Ours is more like a rational n-party protocol than Halpern et al.'s [13].

In summary, our protocol is better than Halpern et al.'s [13] and Maitra et al.'s [17] in these aspects.

5 Conclusion

In this paper, rational quantum MC protocol was investigated. Processes of our protocol are learned and improved from Ref. [13]. This is the first rational quantum multifunctional computation protocol. For any problem, if the key of a quantum solution is a computation which is homomorphic, this problem could be resolved by our protocol. Besides that, our rational protocol was analyzed in detail. It is secure, multifunctional and efficient. No extra assumption about players' strategies holds in our protocol.

Acknowledgements Project supported by NSFC (Grant Nos. 61671087, 61272514, 61170272, 61003287), the Fok Ying Tong Education Foundation (Grant No. 131067), Open Foundation of Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ007) and BUPT Excellent Ph.D. Students Foundation (Grant No. CX2018310).

References

1. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on IEEE SFCS'08, pp. 160–164. IEEE, Chicago (1982)

2. Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., Zhu, M.Y.: Tools for privacy preserving distributed data mining. ACM SIGKDD Explor. Newsl. **4**, 28–34 (2002)
3. Sanil, A.P., Karr, A.F., Lin, X., Reiter, J.P.: Privacy preserving regression modelling via distributed computation. In: Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 677–682. ACM, Seattle (2004)
4. Atallah, M., Bykova, M., Li, J., Frikken, K., Tophara, M.: Private collaborative forecasting and benchmarking. In: Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society, pp. 103–114. ACM, Washington (2004)
5. Li, P., Li, J., Huang, Z., Li, T., Gao, C.Z., Yiu, S.M., Chen, K.: Multi-key privacy-preserving deep learning in cloud computing. Future Gener. Comput. Syst. **74**, 76–85 (2017)
6. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**, 2050–2056 (1999)
7. Mayers, D.: Unconditional security in quantum cryptography. ACM **48**, 351–406 (2001)
8. Zhang, W.W., Li, D., Zhang, K.J., Zuo, H.J.: A quantum protocol for millionaire problem with Bell states. Quantum Inf. Process. **12**, 2241–2249 (2013)
9. Luo, Q., Yang, G., She, K., Niu, W.N., Wang, Y.Q.: Multi-party quantum private comparison protocol based on d-dimensional entangled states. Quantum Inf. Process. **13**, 2343–2352 (2014)
10. Du, J.Z., Chen, X.B., Wen, Q.Y., Zhu, F.C.: Secure multiparty quantum summation. Acta. Phys. **56**, 6214–6219 (2007)
11. Chen, X.B., Xu, G., Yang, Y.X., Wen, Q.Y.: An efficient protocol for the secure multi-party quantum summation. Int. J. Theor. Phys. **49**, 2793–2804 (2010)
12. Shi, R., Mu, Y., Zhong, H., Cui, J., Zhang, S.: Secure multiparty quantum computation for summation and multiplication. Sci. Rep-UK **6**, 19655 (2016)
13. Halpern, J., Teague, V.: Rational secret sharing and multiparty computation. In: Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing, pp. 623–632 ACM, New York (2004)
14. Zhang, E., Yuan, P., Du, J.: Verifiable rational secret sharing scheme in mobile networks. Mob. Inf. Syst. **2015**, 462345 (2015)
15. Wang, Y., Li, T., Qin, H., Li, J., Gao, W., Liu, Z., Xu, Q.: A brief survey on secure multi-party computing in the presence of rational parties. J. Ambent Intell. Humaniz. Comput. **6**, 807–824 (2015)
16. Wang, Y.L., Li, T., Chen, L.F., Li, P., Leung, H.F., Liu, Z., Xu, Q.L.: Rational computing protocol based on fuzzy theory. Soft. Comput. **20**, 429–438 (2016)
17. Maitra, A., De, S.J., Paul, G., Pal, A.K.: Proposal for quantum rational secret sharing. Phys. Rev. A **92**, 022305 (2015)
18. Dou, Z., Xu, G., Chen, X.B., Liu, X., Yang, Y.X.: A secure rational quantum state sharing protocol. Sci. China. Inform. Sci. **61**, 022501 (2018)
19. Li, X.H., Zhou, P., Li, C.Y., Zhou, H.Y., Deng, F.G.: Efficient symmetric multiparty quantum state sharing of an arbitrary m-qubit state. J. Phys. B-At. Mol. Opt. **39**, 1975 (2006)
20. Xu, J., Wei, L., Zhang, Y., Wang, A., Zhou, F., Gao, C.Z.: Dynamic fully homomorphic encryption-based merkle tree for lightweight streaming authenticated data structures. J Netw. Comput. Appl. **107**, 113–124 (2018)
21. Fudenberg D., Tirole J.: Game theory. The MIT press (1991)
22. Huang, W., Wen, Q.Y., Liu, B., Su, Q., Qin, S.J., Gao, F.: Quantum anonymous ranking. Phys. Rev. A **89**, 032325 (2014)
23. Lin, S., Guo, G.D., Huang, F., Liu, X.F.: Quantum anonymous ranking based on the Chinese remainder theorem. Phys. Rev. A **93**, 012318 (2016)
24. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE, Bangalore (1984)
25. Gong, L.H., Song, H.C., He, C.S., Liu, Y., Zhou, N.R.: A continuous variable quantum deterministic key distribution based on two-mode squeezed states. Phys. Scr. **89**, 035101 (2014)
26. Min, S.Q., Chen, H.Y., Gong, L.H.: Novel multi-party quantum key agreement protocol with G-like States and Bell States. Int. J. Theor. Phys. (2018). https://doi.org/10.1007/s10773-018-3706-6
27. Chen, X.B., Dou, Z., Xu, G., He, X.Y., Yang, Y.X.: A kind of universal quantum secret sharing protocol. Sci. Rep-UK **7**, 39845 (2017)