IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON ADVANCED COMMUNICATIONS AND NETWORKING TECHNIQUES FOR WIRELESS CONNECTED INTELLIGENT ROBOT SWARMS

Received December 4, 2019, accepted January 3, 2020, date of publication February 4, 2020, date of current version February 14, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2971544

Cooperate Delegation of Computation for Rational Party Using Zero-Determinant Strategy Approach

DUO ZHANG[1,2], YOULIANG TIAN[1], (Member, IEEE), CHAOYUE YUE[2], AND MEIMEI FAN[2]

[1]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang 550025, China
[2]School of Mathematics and Statistics, Guizhou University, Guiyang 550025, China

Corresponding author: Youliang Tian (youliangtian@163.com)

This work was supported in part by the Key Projects of the Joint Fund of the National Natural Science Foundation of China under Grant U1836205, in part by the National Natural Science Foundation of China under Grant 61662009 and Grant 61772008, in part by the Science and Technology Top-Notch Talent Support Project in Guizhou Province Department of Education under Grant Qian Education Combined KY word [2016]060, in part by the Guizhou Province Science and Technology Major Special Plan under Grant 20183001, in part by the Guizhou Provincial Science and Technology Plan Project under Grant [2017]5788, in part by the Ministry of Education-China Mobile Research Fund Project under Grant MCM20170401, in part by the Guizhou University Fostering Project under Grant [2017]5788, in part by the Research on Key Technologies of Blockchain for Big Data Applications under Grant [2019]1098, and in part by the Foundation of Postgraduate of Guizhou Province under Grant YJSCXJH2019015.

ABSTRACT Delegating calculation is an important approach to solve the correctness and reliability of task subcontracting and delegating calculation results in cloud computing environment. However, the dynamic, complexity and openness of cloud computing bring unprecedented risks to the security and reliability of computing tasks. To solve the problem the new approach is presented. Firstly, the game theory is introduced into the delegating calculation, and the single-client and multi-server rational delegating calculation game model is given. Secondly, the Zero-determinant Strategy scheme based on delegating calculation is constructed through implementing the single-client and single-server rational delegating calculation protocol and Zero-determinant Strategy, and the conditions of the existence of Nash equilibrium of Zero-determinant Strategy is analyzed. Then, through the iterative implementation of the Zero-determinant Strategy, the participants will cooperate with each other actively. Finally, the performance analysis results show that the entrusting party can regulate the betrayers in the computing party through Zero-determinant Strategy to ensure the interests of honest people in cloud computing.

INDEX TERMS Cloud computing, delegating calculation, single-client multi-server, zero-determinant strategy, Nash equilibrium.

I. INTRODUCTION

In the era of big data, whether there is a large amount of data, such as governments, enterprises and individuals, needs to be calculated and stored, which is likely to cause serious shortage of local resources. The availability of a large collection of personal information and the growing popularity of data storage devices that support data-intensive servers and the belief those server providers will increasingly be responsible for storage, efficiency, and reliable dissemination of information, these will enable *Data outsourcing* [1] architecture. However, the emergence of cloud computing technology makes good use of data outsourcing architecture to solve the burden of data owners to manage data, but at the same time introduce new privacy and security concerns for data outsourcing.

Under the cloud-computing model, resource-constrained users outsource their own computing and data to the platform provided by cloud service providers for processing and storage [2], [3]. For the user, ensuring the appropriate security and privacy of the data is paramount. Since servers that provide data storage and access are honest but curious servers that manage data honestly, the data owner for reading their content may trust them. In order to ensure adequate privacy protection, prevent external attacks and intrusion from the server itself, it is necessary to introduce new models and methods for the definition and implementation of outsourced data access control, while ensuring the necessity and effectiveness of effective query execution.

The associate editor coordinating the review of this manuscript and approving it for publication was Jinming Wen.

Delegating computation [4] is an important measure to deal with the correctness and reliability of delegating computation result and to solve subcontract in the cloud-computing environment, so it is also known as verifiable computation. Traditional delegating computation is to entrusting party complete a certain calculation task and gain a calculation results that is verifiable, focusing on the construction of computational complexity and of cryptography techniques. Generally assume that participants (including the entrusting party and calculation party) are either honest where protocol is enforced or malicious where protocol is arbitrarily enforced, pay little attention to the research of delegating calculation model. In particular, insufficient attention is paid to the security risk of the delegating computing task due to the different behaviors and preferences of the participants.

The rational delegating computation [5] combines the ideas of game theory and delegating computation, and from the perspective of the self-interested party, the utility function is used to guarantee the reliability of the calculation results. However, rational delegating computation schemes will lead to the prisoner's dilemma. Few schemes achieve global optimum, not to mention the designed schemes that forces the other party to cooperate to achieve optimal calculation. According to the model of Press and Dyson [6], this paper studies reasonable delegation calculation in the big data environment to ensure the correctness and reliability of the calculation results. Based on the challenge of maximizing the benefits of the computing party and the cooperating party in rational delegating calculation and perspective of the entrusting party, this paper uses the Zero-determinant Strategy method to regulate the computing parties benefits according to its own preferences and benefits. From the perspective of the calculation party, cooperation is the best way to obtain the maximum benefit. The specific contributions are:

1) Based on the game theory and the single-client and single-server delegating computation model, we construct single-client and multi-server rational delegating computation model.
2) Within certain range, By using the Zero-determinant Strategy, we construct a linear relationship between single-client and multi-server interests. By using this relationship, client can control each other's profits.
3) We construct the Zero-determinant Strategy in single-client and multi-server rational delegating computation, and analyze the existence condition of Nash equilibrium to ensure the profit of honest calculators.

The remainder of this paper is organized as follows. We introduce the related work in Section 2 and the necessary preliminaries in Section 3. Then we formulate the problem and give the system model and security model in Section 4. The building blocks that support rational delegation computation protocol based on Zero-determinant Strategy are given in Section 5. On the basis of that, We give the experimental results in Sections 6. Finally, we conclude our work in Section 7.

II. RELATED WORK

The security outsourcing technology under the cloud platform is a challenging and very meaningful research topic; it has developed a lot in the past few decades. In addition, with the widespread use of cloud computing technology, researchers' interest in research on security outsourcing computing continues to ferment. Gentry [7] proposed a full homomorphic encryption algorithm (FHE) and designed a general security outsourcing computing framework to implement security-outsourcing calculations for all problems. Gennaro et al. [8] first proposed a general outsourcing computing scheme based on FHE and encrypted Boolean circuit [9], which not only can effectively protect user privacy, but also the verifiability of the computing party's calculation results. Subsequently, Chung et al. [10] proposed an improved solution, which reduced the implementation complexity of the general outsourcing computing solution to a certain extent. However, these traditional hand-crafted features have their inherent defects, since they often rely on expert knowledge and require expensive human labor.

Other work strived to address the problems in certain rational system. In 2014, Rational proofs, introduced by Azar and Micali [11], are an interactive proof model in which the prover is rational rather than untrustworthy he may lie, but only to increase his payment. In 2014, Chritian and Bin [12] constructed a Zero-determinant Strategy of multi-player cooperative game. They results highlight the importance of individual control and coordination to succeed in large groups. In 2015, Hao and Rong [13] applied them to public goods game and repeated noise game. In 2016, Chen [14] studied rational proof problem which include multiple provers from the perspective of complexity. In model, a verifier can cross-check the answers received by asking several provers. The verifier can pay the provers according to the quality of their work, incentivizing them to provide correct information. In 2017, Yin and Tian [15] designed a new rational delegating computation protocol based on the random vector representation technology of Micali-Rabin and bitcoin. However, All of these delegate computing models cause in collusion with the computing parties.

In this paper, we use the Zero-determinant Strategy to adjust the expected payoff of the worker to motivate his everlasting cooperation. The Zero-determinant Strategy were proposed by Press and Dyson [6] in 2012. A ZD player can unilaterally set the opponent's expected payoff on a fixed value by enforcing a linear relationship between the two expected payoffs. Although some studies [16], [17], challenged the stability of ZD, it is still widely investigated and discussed. However, it is a consensus that current delegate computing always introduce expensive verification costs into the system. Recently, In [14], an extension of the Zero-determinant Strategy from two-player games to multi-player games was studied. While in [18], Rong et al. investigated the influence of the strategy-selection timescale, and found that cooperation can be promoted if one permits an individual

with a high payoff to hold onto his/her successful strategy for longer,which was also originally mentioned in [6].

III. PRELIMINARIES

In this section, we briefly review the concept of game theory.

Definition 1 [19]: Refers to that the user sends the function $f(x)$ and input data a to the service provide, the service provider returns the calculation result y and proves of result $Proof_f^a(y)$. Users can verify the correctness of the calculation results, and the cost verification is much less than calculating by themselves.

Definition 2 [19] (Nash Equilibrium): Let n participants of strategic expressive game $G = \{P_1, \ldots, P_n; S_1, \ldots, S_n; u_1, \ldots, u_n\}$, Composition strategy $s^* = \{s_1^*, \ldots, s_i^*, \ldots, s_n^*\}$ is a Nash equilibrium. If for each i, s_i^* is the optimal strategy for the ith participant given the choice of other participants $s_{-i}^* = \{s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_n^*\}$, $u_i(s_i^*, s_{-i}^*) \geq u_i(s^*, s_{-i}^*)$, s.t. $\forall i, s_i^* \in S_i$.

Definition 3 [20] (Cooperative Game): In n players independent non-cooperative game, it is not allowed for any two or more players to agree in advance to combine their strategies and to redistribute the sum of payments they receive. In n players cooperative game, any two or more players can agree in advance to combine their strategies and redistribute the sum of their payoffs after the end of the game. Let $P = \{P_1, \ldots, P_n\}$ be a set of players, $v(S)$ defined on all of itself of P, a real-valued function on all subsets of P, It represents the maximum benefit that a coalition S can obtain by coordinating the strategies of its members, and satisfies the conditions: $v(\Phi) = 0$, $v(P) \geq \sum_{i=1}^{n} v(\{P_i\})$. $\Gamma = (P, v)$ is called n players cooperative game, $v(S)$ is the characteristic function of the game.

IV. SYSTEM ARCHITECTURE

Rational delegating calculation belongs to the category of rational cryptography [21], [22]. At present, rational cryptography mainly focuses on two aspects [23]: one is the application of cryptographic protocols to solve problems in game theory [24], the other is the application of game theory to analyze cryptographic protocol. Rational delegating calculation designs utility functions that satisfy two or more parties of delegating calculation, by combining game theory and delegating calculation, and analyzing the utility of participants in delegating calculation from the perspective of calculator's self-interest, which studies the influence of participants on the delegating calculation model under rational circumstances, so as to ensure the reliability of the calculation.

Rational delegating calculation can be divided into a single client single-server delegating calculation and a single-client multi-server delegated delegating calculation according to different scenarios. This paper proposes a single-client multi-server delegated computing model by taking example of the prisoner's dilemma game theory, that is to say, 1 to n rational delegating calculation game model, 1 represents the client which is the entrusting party of computing service, n represents multiple servers which are the calculator of computing service, the relationship between them is not exactly opposite and consistent.

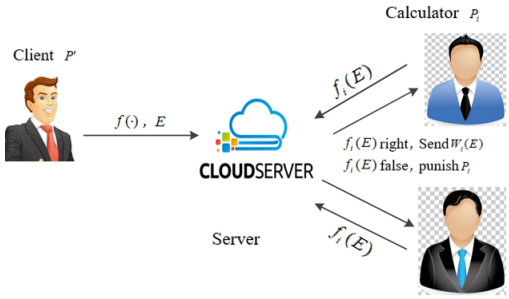

FIGURE 1. Rational delegating calculation.

A. SYSTEM MODEL

Assume that the client is the entrusting party P', the server is the calculator P_i, and all of them are rational participants. Many computing parties constitute a computing group, but each computing party is a single independent individual when accepting computing tasks. In the process of calculation, the entrusting party and n calculators repeatedly appear the prisoner's dilemma. They can choose to cooperate with each other C to complete the entrusted calculation task or conspire to betray the D calculator among the members of the calculator [25]. The payoff of the calculating party depends on its own decision and the decision of all other members of the calculating party. As shown in Figure. 1:

The client P' computing tasks E and a function f stores on the server side. Then, any calculators P_i can request a calculation task E and a calculation function f from the server and uses their own resources to accomplish calculation task E. Once P_i accomplish a calculation task, will send a calculation result $f_i(E)$ to the client. The client returns a calculation result $f_i(E)$, meanwhile provide a correct proof of the calculation result. The client P' decides whether to accept or deny the results to P' by verifying the correctness of the calculation results and pay the calculator $W_i(E)$ if accept the result. Because participants are rational, the calculator P_i may send a wrong result, the client P' can punish the calculator P_i.

Given the n participants, each participant has the same computational ability, and separately calculates the benefits c. If choosing to cooperate, the benefits will increase by r ($r > 1$) times and the increased benefits will be assigned equally to all participants. If all participants choose to cooperate, benefit is $(r-1)c$ for each participant. But every rational participant faces the temptation that sitting and sharing dividends not effort. Then the betrayal strategy will be used as a highly adaptable and successful strategy in the future evolution process, and will be imitated by more and more participants. When the partners don't participate, the ultimate owner's benefits is 0; If the number of participant is m, $0 \leq m \leq n$ and $m \in Z$. f_C represents benefits of cooperation, f_D represents benefits of betrayal. Then $f_C(m) = \frac{mr}{n-1}$; $f_D(m) = \frac{mrc}{n}$.

Each participant makes decisions independently in the game model, Nash equilibrium of the game model can be studied by the changing trends of the benefits under the participants' different of strategies.

Let $f_C(m) - f_D(m-1) = \frac{r}{n-1}c$,

- When $r > n, f_C(m) > f_D(m-1)$;

All participants choose cooperation as Nash equilibrium, and no participant will gain higher profits by changing their strategies in this state.

- When $r < n, f_C(m) < f_D(m-1)$;

All participants choose betrayal as Nash equilibrium, and no participant will gain higher returns by changing their strategies in this state.

- When $r = n, f_C(m) = f_D(m-1)$;

Any state is Nash equilibrium, but the collective benefits are different in each state.

In general, $r > n$ can't be happened. As a result, the system state tends to benefit the least in most cases, all participants do not choose to cooperate [26]. However, there is often a great difference between theoretical analysis and experimental results. In order to reveal the internal causes of the differences or conflicts between theory and practice, researchers have proposed many mechanisms and strategies to encourage cooperation or punish betrayal.

In 2012, the Zero-determinant Strategy proposed by Press and Dyson can unilaterally control the interests of participants and force the profit of client and service providers to meet the linear relationship, which is especially suitable for forcing rivals to choose strategies according to their own wishes. In the delegating calculation, the client uses Zero-determinant Strategy to control the profit of the calculator and force it to calculate honestly. In rational delegation calculation, rational participants will choose self-interested behaviors in order to obtain the maximum benefits, which is likely to create a prisoner's dilemma between the client and the calculators, so that they will not choose to cooperate with each other. Based on the rational entrustment calculation scheme, we construct the Zero-determinant Strategy scheme of rational delegating calculation. Under this scheme, the client can control the benefits of the calculator, ensure the benefits of the honest person and prevent the occurrence of collusion among the participants.

B. SECURITY MODEL

As for the security model, we adopt the standard rational security model [6], which is also called honest-but-curious model. According to the model, the participants execute the protocol as required by the protocol. That means the calculator can only passively learn the information about the protocols. However, driven by economic interests, neither side can afford to miss any opportunity to exploit loopholes in the agreement.

Furthermore, we assume that at most one calculator can be malicious in our model and no participant tries to collude with each other. In addition, even though calculators have infinite computing power, they can learn nothing but the messages received from other participants in accordance with our proposed protocols. Naturally, it is rational to hypothesize that there are secure communication channels between any two participants. In addition, Zero-determinant Strategy can control the profit of the calculator. Thus, as we suppose, any participants cannot be corrupted or dishonest.

V. RATIONAL DELEGATION COMPUTATION PROTOCOL BASED ON ZERO-DETERMINANT STRATEGY

A. ZERO-DETERMINANT STRATEGY

In the prisoner's dilemma model, let's say the participants are X and Y, the strategy adopted is cooperation C or betray D. The results of the game are as follows: $xy \in (cc, cd, dc, dd)$, $yx \in (cc, dc, cd, dd)$. The probability of cooperation between X and Y in the next round is respectively: $p = (p_1, p_2, p_3, p_4)$, $q = (q_1, q_2, q_3, q_4)$. Then every pair of strategies (p, q) generate a Markov chain which construct a state transition matrix [27]:

$$M(p,q) = \begin{bmatrix} p_1q_1 & p_1(1-q_1) & (1-p_1)q_1 & (1-p_1)(1-q_1) \\ p_2q_3 & p_2(1-q_3) & (1-p_2)q_3 & (1-p_2)(1-q_3) \\ p_3q_2 & p_3(1-q_2) & (1-p_3)q_2 & (1-p_3)(1-q_2) \\ p_4q_4 & p_4(1-q_4) & (1-p_4)q_4 & (1-p_4)(1-q_4) \end{bmatrix}$$

Let $S_X(p,q)$, $S_Y(p,q)$ are profit functions of participants X and Y respectively, when Markov Chain is a steady state distribution $v(p,q)$, and $S_X(p,q) = \frac{D(p,q,S_X)}{D(p,q,I)}$, $S_Y(p,q) = \frac{D(p,q,S_Y)}{D(p,q,I)}$, s.t. $S_X = (R,S,T,P)$, $S_Y = (R,T,S,P)$, $I = (1,1,1,1), f = (f_1, f_2, f_3, f_4)$,

$$D(p,q,f) = det \begin{bmatrix} -1+p_1q_1 & -1+p_1 & -1+q_1 & f_1 \\ p_2q_3 & -1+p_2 & q_3 & f_2 \\ p_3q_2 & p_3 & -1+q_2 & f_3 \\ p_4q_4 & p_4 & q_4 & f_4 \end{bmatrix}.$$

By determinant $D(p,q,f)$, the second column of the determinant relates only to participant X, the third column only concerns participant Y. Therefore, there is a linear relationship between the returns of participants X and Y, namely,

$$\alpha s_X + \beta s_Y + \gamma = \frac{D(p,q,\alpha S_X + \beta S_Y + \gamma I)}{D(p,q,I)}, \quad (\alpha, \beta, \gamma \in R).$$

According to the properties of determinant, the participant X can adjust the benefit of setting Y unilaterally, namely, $\alpha s_X + \beta s_Y + \gamma = 0$. By this time, the strategy adopted by participant X is

$$\begin{aligned} p_1 &= p_{CC} = 1 + \phi(\alpha R + \beta R + \gamma) \\ p_2 &= p_{CD} = 1 + \phi(\alpha S + \beta T + \gamma) \\ p_3 &= p_{DC} = \phi(\alpha T + \beta S + \gamma) \\ p_4 &= p_{DD} = \phi(\alpha P + \beta P + \gamma), \end{aligned}$$

and the parameter ϕ is not zero.

B. RATIONAL DELEGATION COMPUTATION MODEL BASED ON ZERO-DETERMINANT STRATEGY

In the delegating calculation game model, $r > n$ can't be happened. All participants choose to cooperate, which results

in minimal benefit of the system. To encourage calculators to choose not to cooperate, the client needs to adopt strategies to punish the betrayer. Since the relationship between the client and calculators are multiple cooperation, which is a process of continuous game, participants will try their best to infer their opponents' strategies from previous rounds and then make their own decisions. But Haunt and Schuller [28], [29] have proved that the ability of historical memory is of no help to the decision-making of participants, so we study the case of historical memory-1. Following is a Zero-determinant Strategy proposed by Press and Dyson to design Zero-determinant Strategy suitable for delegating calculation game.

Assume that the result of each round of the game is $\sigma \in \{C, D\}^n$. $|\sigma|$ is the total number of people who choose to cooperate in each round of the game, the payoff vector is $g^i = (g^i_\sigma)_{\sigma\in\{C,D\}^n}$, g^i_σ is benefit of participant i,

$$g^i_{(S_1,\ldots,S_n)} = \begin{cases} a_{|\sigma\|-1}, & S_i = C \\ b_{|\sigma\|}, & S_i = D. \end{cases}$$

Then the participant i gains benefit of in round t of the game is $\pi^i(t) = g^i \cdot v(t)$, $v(t) = [v_\sigma(t)]_{\sigma\in\{C,D\}^n}$. The participant i's expected benefit is $\pi^i = g^i \cdot v$. Limit distribution v, when $t \to \infty$, the limit is $I = (1)_{\sigma\in\{C,D\}^n}$ of sequence $[v(1) + \cdots + v(t)]/t$, and $I \cdot v = 1$.

Definition 4 [13] Let α, β_j, γ are parameters, s.t. $\sum_{j\neq i} \beta_j \neq 0$. In the repetition game of historical memory-1, according to the $p = p^{rep} + \alpha g^i + \sum_{j\neq i}^n \beta_j g^j + \gamma I$, $p = p^{rep}$ represents a strategy of the last round of choices

$$p^{rep}_{(S_1,\ldots,S_n)} = \begin{cases} 1, & S_i = C \\ 0, & S_i = D \end{cases}$$

is Zero-determinant Strategy.

Lemma 1 [30]: In the repetition game, the historical memory ability is 1. If the client policy p is any limit distribution v (without considering the results of the first round), s.t. $(p - p^{rep}) \cdot v = 0$, and $p \cdot v = \Sigma_{\sigma\in\{C,D\}^n} p_\sigma v_\sigma$.

Theorem 1: If the client adopts the Zero-determinant Strategy in the repeated game with the historical memory-1, then benefits of $n-1$ calculators satisfy $\alpha\pi^i + \sum_{j\neq i} \beta_j \pi^j + \gamma = 0$.

Proof: From the definition of Zero-determinant Strategy, we can know that,

$$p - p^{rep} = \alpha g^i + \sum_{j\neq i}^n \beta_j g^j + \gamma I.$$

According to Akin's lemma, we can know that,

$$\begin{aligned}(p - p^{rep}) \cdot v &= (\alpha g^i + \sum_{j\neq i}^n \beta_j g^j + \gamma I) \cdot v \\ &= \alpha g^i \cdot v + \sum_{j\neq i}^n \beta_j g^j \cdot v + \gamma I \cdot v \\ &= \alpha\pi^i + \sum_{j\neq i}^n \beta_j \pi^j + \gamma = 0.\end{aligned}$$

C. EVOLUTION OF PARTICIPANTS UNDER ZERO-DETERMINANT STRATEGY

1) THE RELATIONSHIP BETWEEN ARITHMETIC AND BENEFIT

According to the nature of the Zero-determinant Strategy, if the client adopts the Zero-determinant Strategy, it can establish a linear relationship with the calculating party's benefit, and can directly control the form of the revenue relationship by properly selecting the value of the parameters α, β, γ. Combined with the selection of parameters in Press and Dyson literature, we may set up $s = \frac{-\alpha}{\sum_{k\neq i}\beta_k}$, $w_{j\neq i} = \frac{\beta_j}{\sum_{k\neq i}\beta_k}$, $l = \frac{-\gamma}{\alpha+\sum_{k\neq i}\beta_k}$, $w_i = 0$, $\phi = -\sum_{k\neq i}\beta_k$. therefore, the Zero-determinant Strategy can be transformed into, $p = p^{rep} + \phi[sg^i - \sum_{j\neq i}^n w_j g^j + (1-s)lI]$ s.t. $\phi \neq 0$, $w_i = 0$, $\sum_{j\neq i}^n w_j = 1$. According to Akin's lemma, we can know that,

$$\begin{aligned}(p - p^{rep}) \cdot v &= \phi[sg^i - \sum_{j\neq i}^n w_j g^j + (1-s)lI] \cdot v \\ &= \phi[s\pi^i - \sum_{j\neq i}^n w_j \pi^j + (1-s)l] = 0.\end{aligned}$$

Thus, $s\pi^i - \sum_{j\neq i}^n w_j\pi^j + (1-s)l = 0$, i.e. $\pi^{-i} =: \sum_{j\neq i}^n w_j\pi^j = s\pi^i + (1-s)l$. $\pi^{-i} =: \sum_{j\neq i}^n w_j\pi^j$ is called the weighted average benefit of the calculating party. l is basic benefit; s is the slope of the linear income relationship; $w = (w_j)$ is the weight of strategy; ϕ is that the client adjusts the intensity of the revenue relationship in the process of game.

a: THE CASE OF THE SAME ARITHMETIC

Assuming that each member of the calculating party has the same computational power and the weight of the strategy $w_j = \frac{1}{n-1}$, the probability that the calculators chooses to cooperate is

$$p_\sigma = \begin{cases} 1 + \phi[(1-s)(l - a_{|\sigma|-1}) \\ \quad -\frac{n-|\sigma|}{n-1}(b_{|\sigma|} - a_{|\sigma|-1})]; & S_i = C \\ \phi[(1-s)(l - b_{|\sigma|}) + \frac{|\sigma|}{n-1}(b_{|\sigma|} - a_{|\sigma|-1})]; & S_i = D. \end{cases}$$

According to the formula, the probability of the calculator choosing cooperation only depends on the strategy selected in the last outsourcing task and the number of partners $|\sigma|$. In other words, the game model discussed in this paper is exactly the case of the same computing power in Zero-determinant Strategy, and the weighted average revenue $\pi^{-i} = s\pi^i + (1-s)l$ is the arithmetic average of all the cooperative calculators' revenue at this time i.e. $\pi^{-i} = \sum_{j\neq i}\pi^j/(n-1)$.

b: THE CASE OF DIFFERENT ARITHMETIC

Assuming that each member of the computing party has different computing power, this situation is the closest to the reality, but different computing power leads to the complexity of the delegating calculation model and the analysis

is quite difficult. In order to carry out the research work smoothly, we first consider the most basic situation, only one person in the calculating party undertakes the calculation task, the strategy weight $w_j = 1$; the other people sit and enjoy the achievement, the strategy weight $w_{k\neq j} = 0$. Then the probability of the calculator choosing cooperation is

$$p_\sigma = \begin{cases} 1+\phi(1-s)(l-a_{|\sigma|-1}), & S_i = S_j = C; \\ 1+\phi[sa_{|\sigma|-1}+b_{|\sigma|}+(1-s)l], & S_i = C, S_j = D; \\ \phi[sb_{|\sigma|}-a_{|\sigma|-1}+(1-s)l], & S_i = D, S_j = C; \\ \phi(1-s)(l-b_{|\sigma|}), & S_i = S_j = D. \end{cases}$$

The formula shows that the probability of cooperation depends on the sincerity of the calculating party, the number of cooperators $|\sigma|$ and the sincerity of the entrusting party. At this time, the entrusting party's fee is $\pi^j = s\pi^i + (1-s)l$.

2) NASH EQUILIBRIUM IN ZERO-DETERMINANT STRATEGY

- Existence conditions of Nash equilibrium.

Proposition 1 ([13] Necessary Condition): Any forcible earnings relationship (l, s, w) should be satisfied $-\frac{1}{n-1} \leq s \leq 1$, and $s > 1$, $b_0 \leq l \leq a_{n-1}$, $\phi > 0$.

Proof: According to the definition of Zero-determinant Strategy, the probability of cooperation and betrayal are respectively

$$P_{(C,\ldots,C)} = 1+\phi(1-s)(l-a_{n-1}),$$
$$P_{(D,\ldots,D)} = \phi(1-s)(l-b_0),$$

so $\phi(1-s)(l-a_{n-1}) \leq 0$ and $\phi(1-s)(l-b_0) \geq 0$. The two formula is summed up $\phi(1-s)(b_0-a_{n-1}) \leq 0$; and because $b_0 < a_{n-1}$, so $\phi(1-s) \geq 0$.

Similarly: Consider the result σ (all participants have only one choice to cooperate), σ is the replacement of $(C, C, \ldots, C, D)$. i.e.,

$$P_\sigma = \begin{cases} 1+\phi[sa_{n-2}-(1-w_j)a_{n-2}-w_jb_{n-1} \\ \quad +(1-s)l], & i \neq j; \\ \phi[sb_{n-1}-a_{n-2}+(1-s)l], & i = j; \end{cases}$$

so $\phi[sa_{n-2}-(1-w_j)a_{n-2}-w_jb_{n-1}+(1-s)l] \leq 0$, $\phi[sb_{n-1}-a_{n-2}+(1-s)l] \geq 0$. The two formula is summed up:$\forall j \neq i$, $\phi(s+w_j)(b_{n-1}-a_{n-2}) \geq 0$ and $\forall j$, $0 \leq j < n-1$, s.t. $b_{j+1} > a_j$, so $\forall j \neq i$, $\phi(s+w_j) \geq 0$.

Since there is at least one w_j non-negative ($\sum w_j = 1$), therefore $\phi \geq 0$. Because of $min_{j\neq i}w_i \leq \frac{1}{n-1}$, $\sum w_j = 1$ inequality $\phi(1-s) \geq 0$; $\forall j \neq i$, $\phi(s+w_j) \geq 0$; then $-min_{j\neq i}w_i \leq s \leq 1$, thus $-\frac{1}{n-1} \leq s \leq 1$.

If $s \neq 1$, since $\phi(1-s)(l-a_{n-1}) \leq 0$, $\phi(1-s)(l-b_0) \geq 0$, so $b_0 \leq l \leq a_{n-1}$.

Proposition 2 (Sufficient Condition): Benefit relationship of all of the participants (l, s, w) should satisfy $\forall j$, $w_j \geq 0$, if $\hat{w}_j$ is the sum of the smallest inputs of j under $(w_j)_{j\neq i}$, and $\hat{w}_0 = 0$, then (l, s, w) feasible sufficient conditions as follows, $s = 1$ or $\max_{0\leq j\leq n-1}\{b_j - \frac{\hat{w}_j(b_j-a_{j-1})}{1-s}\} \leq l \leq \min_{0\leq j\leq n-1}\{a_j + \frac{\hat{w}_{n-j-1}(b_{j+1}-a_j)}{1-s}\}$.

- The case of same arithmetic $w_j = \frac{1}{n-1}$, $\hat{w}_j = \frac{j}{n-1}$.

Let (l, s, w) the necessary and sufficient conditions is $s = 1$ or $\max_{0\leq j\leq n-1}\{b_j - \frac{j}{n-1} \cdot \frac{b_j-a_{j-1}}{1-s}\} \leq l \leq \min_{0\leq j\leq n-1}\{a_j + \frac{n-j-1}{n-1} \cdot \frac{b_{j+1}-a_j}{1-s}\}$.

- The case of different arithmetic $\forall k \neq i$, $w_k = 0$, the components in other w are all 0 and

$$\begin{cases} w_j = 0, & j < n-1, \\ \hat{w}_j = 1, & j = n-1. \end{cases} \qquad b_{j+1} > b_j, a_{j+1} > a_j.$$

- Then, the executable conditions of the benefit relationship are as follows: $s = 1$ or $\max_{0\leq j\leq n-1}\{b_{n-2}, \frac{a_{n-2}-sb_{n-1}}{1-s}\} \leq l \leq \min_{0\leq j\leq n-1}\{\frac{b_1-sa_0}{1-s}, a_1\}$.

Proof: Let $\sigma = (S_1, \ldots, S_n)$, the Zero-determinant Strategy of P_σ: $p = p^{rep} + \phi[sg^i - \sum_{j\neq i}^n w_jg^j + (1-s)ll]$, i.e. $P_\sigma = P_\sigma^{rep} + \phi[(1-s)(l-g_\sigma^i) + \sum_{j\neq i} w_j(g_\sigma^i - g_\sigma^j)]$, s.t.

$$P^{Rep}_{\sigma(S_1,\ldots,S_n)} = \begin{cases} 1, & S_i = C \\ 0, & S_i = D, \end{cases}$$
$$g^i_{(S_1,\ldots,S_n)} = \begin{cases} a_{|\sigma|-1}, & S_i = C \\ b_{|\sigma|}, & S_i = D \end{cases}$$

Let σ^C the first non-cooperator to choose cooperation in the next state, σ^D non-cooperators still choose not to cooperate in the next state, then

$$P_\sigma = \begin{cases} 1+\phi[(1-s)(l-a_{|\sigma|-1})- \\ \quad \Sigma_{j\in\sigma^D}w_j(b_{|\sigma|}-a_{|\sigma|-1})], & S_i = C; \\ \phi[(1-s)(l-b_{|\sigma|})+\Sigma_{j\in\sigma^C}w_j(b_{|\sigma|}-a_{|\sigma|-1})], & S_i = D. \end{cases}$$

Since $\phi > 0$, for any σ satisfy $P_\sigma \in [0, 1]$, so

$(1-s)(l-a_{|\sigma|-1}) - \sigma_{j\in\sigma^D}w_j(b_{|\sigma|}-a_{|\sigma|-1}) \leq 0$, $S_i = C$;
$(1-s)(l-b_{|\sigma|}) + \sigma_{j\in\sigma^C}w_j(b_{|\sigma|}-a_{|\sigma|-1}) \geq 0$, $S_i = D$.

If $s = 1$, he above formula is unconstrained to the parameters l and the inequalities are all valid.

If $s < 1$, then $1-s > 0$, so

$$a_{|\sigma|-1} + \frac{\Sigma_{j\in\sigma^D}w_j(b_{|\sigma|}-a_{|\sigma|-1})}{1-s} \geq l, \quad S_i = C;$$
$$b_{|\sigma|} - \frac{\Sigma_{j\in\sigma^C}w_j(b_{|\sigma|}-a_{|\sigma|-1})}{1-s} \leq l, \quad S_i = D.$$

Thus, $\max_{\sigma|_{S_i=D}}\{b_{|\sigma|} - \frac{\Sigma_{j\in\sigma^C}w_j(b_{|\sigma|}-a_{|\sigma|-1})}{1-s}\} \leq l \leq \min_{\sigma|_{S_i=C}}\{a_j + \frac{\Sigma_{j\in\sigma^D}w_j(b_{|\sigma|}-a_{|\sigma|-1})}{1-s}\}$.

Since $\frac{b_{|\sigma|}-a_{|\sigma|-1}}{1-s} > 0$, the maximum and minimum values of l can be obtained by adjusting the weighting coefficients w_j. i.e. for a given number $|\sigma|$ of partner, the extremal of $\Sigma_{j\in\sigma^C}w_j$ and $\Sigma_{j\in\sigma^D}w_j$ can be obtained under the state $|\sigma|$.

Hence, $\max_{0\leq j\leq n-1}\{b_j - \frac{\hat{w}_j(b_j-a_{j-1})}{1-s}\} \leq l \leq \min_{0\leq j\leq n-1}\{a_j + \frac{\hat{w}_{n-j-1}(b_{j+1}-a_j)}{1-s}\}$, $\hat{w}_j$ is the sum of the minimum inputs under conditions j.

- Nash equilibrium theorem.

Consider all participants using the Zero-determinant Strategy p, parameter l, s, ϕ, $w_j = \frac{1}{n-1}(j \neq i)$.

Let's say the first n calculators choose to betray and not cooperate, we think the first $n-1$ calculator as an invariant, the first n calculator is a mutant. The benefits of mutants are defined under invariant conditions. The mutant's benefit $\hat{\pi}$ is defined under the benefit of the invariant. Since the invariant applies the Zero-determinant Strategy, according to the benefit function $\pi^{-i} = s\pi^i + (1-s)l$, each participant in the calculator performs this relationship $\frac{n-2}{n-1}\pi + \frac{1}{n-1}\hat{\pi} = s\pi + (1-s)l$, that is $\hat{\pi} = s^R\pi + (1-s^R)l$ and $s^R = s(n-1) - (n-2)$.

In other words, $n-1$ the invariant set enforces a linear relationship between their own benefits π and the mutant's benefits $\hat{\pi}$, and the corresponding benefits limits respectively are l and s^R. If the variant uses the same strategy, the mutant's benefits are $\hat{\pi} = \pi$.

$s^R < 1, \hat{\pi} = s^R\pi + (1-s^R)l$, means $\hat{\pi} = \pi = l$;

$s^R = 1$, l is a free parameter, that is to say l has no effect on the ZD strategy.

Consistent with $s^R < 1$, the benefit of l is defined as: if all participants adopt this strategy (the first round chooses cooperative strategy), then using the invariant strategy, the benefit of the mutant is l, which is Nash equilibrium for P. Thus, mutants are required not to change the Zero-determinant Strategy p, $\hat{l}$, $-\frac{1}{n-1} < \hat{s} < 1$. From this we can know that the mutant's profit relationship is as follows $\pi = \hat{s}\hat{\pi} + (1-\hat{s})\hat{l}$.

Therefore,

$$\begin{cases} \hat{\pi} = s^R\pi + (1-s^R)l \\ \pi = \hat{s}\hat{\pi} + (1-\hat{s})l \end{cases}$$

and $\hat{\pi} = \frac{l(1-s^R)+\hat{l}s^R(1-\hat{s})}{1-\hat{s}s^R} \leq 0$.

When $\hat{\pi} \leq l$ mutants have no inducement i.e.$\hat{\pi} - l = \frac{(\hat{l}-l)s^R(1-\hat{s})}{1-\hat{s}s^R} \leq 0(*)$. Since $-\frac{1}{n-1} \leq s \leq 1$ (proposition 1), $-\frac{1}{n-1} \leq \hat{s} \leq 1$ (hypothetical condition), then$(*)$ is positive number, there are three situations:

- $s^R = 0, \hat{\pi} - l = 0$, mutants can't improve their benefits by changing their strategies.
- $s^R > 0, \hat{\pi} - l \leq 0 \Leftrightarrow \hat{l} \leq l$. In order to prevent mutant from changing strategies, invariants require a strategy to maximize possible baseline gains.
- $s^R < 0, \hat{\pi} - l \geq 0 \Leftrightarrow \hat{l} \geq l$. In order to prevent mutant replacement strategy, the Zero-determinant Strategy of the invariant needs to take the minimum $l_{min} = b_0$ of l.

Therefore, the Nash equilibrium theorem of Zero-determinant Strategy can be obtained.

Theorem 2 (Nash Equilibrium of Zero-Determinant Strategy): In rational delegating calculation, the friendly cooperation is the best result for the system, and betrayal is the worst thing. When $b_0 \leq \min_{0\leq j\leq n}\{\frac{ja_{j-1}-(n-j)b_j}{n}\} \leq \max_{0\leq j\leq n}\{\frac{ja_{j-1}+(n-j)b_j}{n}\} \leq a_{n-1}$, the p enforce Zero-determinant Strategy, and l, s, ϕ, $s^R = (n-1)s - (n-2)$ are all parameters. The sufficient and necessary conditions for the Nash equilibrium is shown as follows.

$$\begin{aligned} s^R = 0, &\quad b_0 \leq l \leq a_{n-1}; \\ s^R > 0, &\quad l = a_{n-1}; \\ s^R < 0, &\quad l = a_0. \end{aligned}$$

D. RATIONAL DELEGATION COMPUTATION PROTOCOL DESIGN

According to the game analysis of delegation calculation and the Nash equilibrium theorem of Zero-determinant Strategy in the previous section, and $b_0 \leq \min_{0\leq j\leq n}\{\frac{ja_{j-1}-(n-j)b_j}{n}\} \leq \max_{0\leq j\leq n}\{\frac{ja_{j-1}+(n-j)b_j}{n}\} \leq a_{n-1}$, it is shown that rational participants can control opponents to execute the game according to their best results. Based on this, we construct a general protocol algorithm, which is divided into three sub-protocols [31]:

Algorithm 1 Fair Protocol Algorithm

Input: Input p^{rep}: the client's strategy whose initial value is set to be the one used in the last round of the preparatory stage;
$p_\sigma = (p_{cc}, p_{cd}, p_{dc}, p_{dd})$: the state transition probability of the calculator, its initial value is statistically calculated by the client based on the collected data in the preparatory stage;
n: the total round number;
S^R: the benefit limit of nonvariant;
l: the basic benefit;
π: the benefit of nonvariant;
$\hat{\pi}$: the benefit of variant.

Output: the output benefits of the i participant, π^{-i}.

```
Initialize π_0^i;
for i = 1 to n do
    if the client's previous move is c then
        if P_cc > P_cd, s^R = 0, π̂ = 1 then
            the calculate p_σ^i = j/(n−1) which makes
            π^{−i} ← sπ^i + (1 − s)l
        end if
    end if
    if this round terminates then
        update p_σ
    end if
end for
```

Remarkably, it is worth noting that our proposed algorithms can prevent both malicious attacks by a single client and collusive attacks by multiple outsourcers. In fact, we considers collusion is a game between the client and any calculating party, and finally drives the calculating party to calculate honestly. Therefore, When more than one calculator participates in the computation, each computing party will be forced to cooperate by algorithm 1-3, resulting in global cooperation.

Algorithm 2 Extortion Protocol Algorithm

Input: Input p^{rep}: the client's strategy whose initial value is set to be the one used in the last round of the preparatory stage;
$p_\sigma = (p_{cc}, p_{cd}, p_{dc}, p_{dd})$: the state transition probability of the calculator, its initial value is statistically calculated by the client based on the collected data in the preparatory stage;
n: the total round number;
S^R: the benefit limit of nonvariant;
l: the basic benefit;
π: the benefit of nonvariant;
$\widehat{\pi}$: the benefit of variant.
Output: the output benefits of the i participant, π^{-i}.

Initialize π_0^i;
for $i = 1$ to n **do**
  if the client's previous move is c **then**
    if $P_{cc} > P_{cd}, s^R = 0, \hat{\pi} = 1$ **then**
      the calculate $p_\sigma^i = \frac{j}{n-1}$ which makes
      $\pi^{-i} \leftarrow s\pi^i + (1-s)l$
    end if
  end if
  if this round terminates **then**
    update p_σ
  end if
end for

Algorithm 3 Generous Protocol Algorithm

Input: Input p^{rep}: the client's strategy whose initial value is set to be the one used in the last round of the preparatory stage;
$p_\sigma = (p_{cc}, p_{cd}, p_{dc}, p_{dd})$: the state transition probability of the calculator, its initial value is statistically calculated by the client based on the collected data in the preparatory stage;
n: the total round number;
S^R: the benefit limit of nonvariant;
l: the basic benefit;
π: the benefit of nonvariant;
$\widehat{\pi}$: the benefit of variant.
Output: the output benefits of the i participant, π^{-i};

Initialize π_0^i;
for $i = 1$ to n **do**
  if the client's previous move is c **then**
    if $P_{dc} > P_{dd}, s^R < 0, \hat{\pi} \leq 1$ **then**
      the calculate $p = \frac{j}{n-1} + (1-s)\frac{n-j-1}{n-1} \cdot \frac{n(r-1)}{r+(n-r)s}$ which makes
      $\pi^{-i} \leftarrow s\pi^i + (1-s)l$
    end if
  end if
  if this round terminates **then**
    update p_σ
  end if
end for

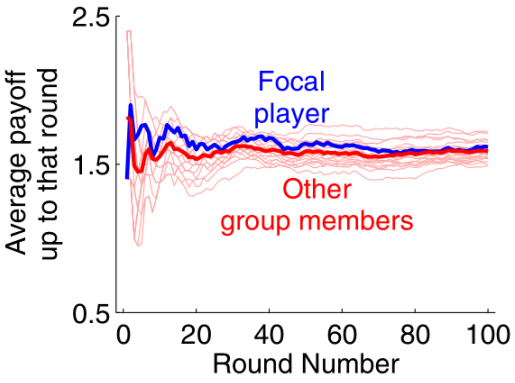

FIGURE 2. Rational delegating calculation.

VI. EXPERIMENTAL SIMULATION

Based on the rational delegating calculation model, the Zero-determinant Strategy under different characteristics can be simulated through experiments to maintain the linear relationship between the average return of the client and the calculator, and to maintain the stability of the system benefits, so as to illustrate the effectiveness of the Zero-determinant Strategy in rational delegating calculation ($r = 4$, $c = 1$, $n = 20$).

1) Let $s = 1$, $\phi = 1/c$, and c is the cost of honest calculate. From the benefit function $\pi^{-i} = s\pi^i + (1-s)l$, we know $\pi^{-i} = \pi^i$. When the entrusting party adopts the Zero-determinant Strategy to a certain calculator, the average benefit of all members of the calculator is equal. We call the fairness of the Zero-determinant Strategy.

As shown in Figure. 2, a fair strategy does not guarantee that all members of the calculator will get the same benefits, but it is positively correlated. This is because no matter whether there are honest and fair participants in the calculation group, the profits of a betrayed calculator must be more than honest calculator', in which the honest calculator can only ensure that they do not take advantage of any unilateral advantages.

2) Let $s = 0.8$, $l = b_0 = 0$, $\phi = \dfrac{n}{(n-r)sc + rc}$, and c is cost of honest calculation. Then the Zero-determinant Strategy $p = p^{rep} + \phi[sg^i - \sum_{j \neq i}^{n} w_j g^j + (1-s)lI]$ translates into $p = \dfrac{j}{n-1}[1-(1-s)\dfrac{n(r-1)}{r+(n-r)s}]$. From the benefit function $\pi^{-i} = s\pi^i + (1-s)l$, we know $\pi^{-i} = s\pi^i + (1-s)b_0$. The client imposes compulsory constraints on multiple betrayers of the calculating party by adopting the Zero-determinant strategy. For all members of the calculators, only through each round of cooperation can we get the greatest benefit. We call it the extortion of Zero-determinant Strategy.

As shown in Figure. 3, the blackmail strategy enables honest calculation of participants' average benefits to exceed that of betrayal calculation participants. This is because the entrusting party can impose compulsory constraints on the betrayed calculator (adding blackmail factor) to prevent mutual betrayal leading to the lowest system benefits, in order to prevent system collapse.

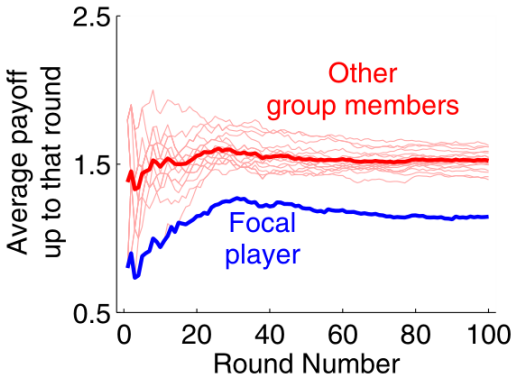

FIGURE 3. Rational delegating calculation.

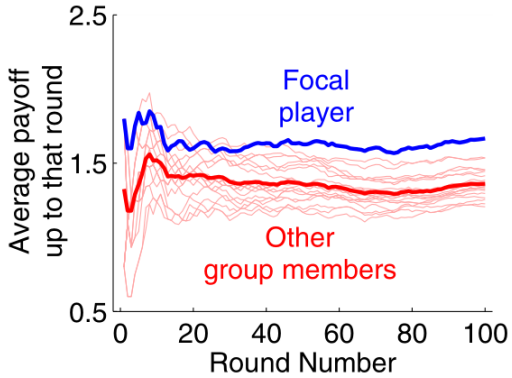

FIGURE 4. Rational delegating calculation.

3) Let $s = 0.8, l = a_{n-1} = rc - c, \phi = \dfrac{n}{(n-r)sc + rc}$, and c is the cost of honest calculate. Then the Zero-determinant Strategy $p = p^{rep} + \phi[sg^i - \sum_{j \neq i}^{n} w_j g^j + (1-s)ll]$ translates into $p = \dfrac{j}{n-1} + (1-s)\dfrac{n-j-1}{n-1} \cdot \dfrac{n(r-1)}{r+(n-r)s}$. From the benefit function $\pi^{-i} = s\pi^i + (1-s)l$, we know $\pi^{-i} = s\pi^i + (1-s)a_{n-1}$. The client also imposes compulsory constraints on multiple betrayers, but unlike 2) the client should treat the betrayer be friendly, the Zero-determinant generosity strategy [32], [33] described by Stewart and Plakin which we call the generosity of the Zero-determinant strategy.

As shown in Figure. 4, the generous strategy of blackmail makes the average benefits of honest participants slightly lower than that of betrayed participants. This is because the principle of good faith persuasion is adopted when the client restrains the rebel, hoping to achieve the optimal average return of the system by cooperating with the betrayer. This situation is uaually applicable to some computational individuals with special properties.

Experiments show that not all strategies in rational delegating calculation are good strategies, the client needs to choose the appropriate Zero-determinant strategies based on different outsourcing tasks and computing power. More specifically. Even if the requestor has a strong Zero-determinant Strategy, she cannot defect to obtain a higher payoff when the participant cooperates. The final state CC of the algorithm can not only increase both players' payoffs but also be fair to both of them, making the proposed algorithm acceptable by both players in a long run. So the system is continuous and the transactions between participants are fair.

TABLE 1. Protocol comparison.

	Computational	Communication	Anti-Collusion	Extortion
Dong [34]	$O(n)$	≥ 2	$\surd$	$\times$
Ours	$O(n)$	2	$\surd$	$\surd$

Our work is closely related to [34], which is to solve the problem of a rational delegation calculation resisting collusion. *Table* 1 shows the comparison between the protocol in this paper and other schemes in terms of anti-collusion, extortion and complexity. All the protocols are to realize the calculation task through continuous rounds, but they cannot simultaneously resist collusion and force to control the calculation side benefits and promote the reasonable evolution of game results. However, in the process of information interaction, the protocol in this paper guarantees the linear relationship between the benefit of the client and the calculators through the Zero-determinant Strategy, forcing the calculator to implement a reasonable strategy and ensuring the reliability of the calculation results.

VII. CONCLUSION

Based on the prisoner's dilemma in the delegating calculation model, we designs a 1-to-n rational delegating calculation model. Combined the idea of 1-to-1 rational delegating calculation protocol with the Zero-determinant strategy in game theory, we analyses the Nash equilibrium conditions of Zero-determinant strategy in rational delegating calculation. The simulation experiment verifies the effectiveness of the Zero-determinant strategy in rational delegation. Through this strategy, the client can control the betrayer in the calculator to ensure a fair deal between the participants. However, in the calculation process, there is often collusion between participants, which will be the future research direction.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This article was presented in part at the Proceeding of IEEE Global Communications Conference on Revolutionizing Communications (GLOBECOM) 2019.

REFERENCES

[1] M. J. Atallah and J. Li, "Secure outsourcing of sequence comparisons," *Int. J. Inf. Secur.*, vol. 4, no. 4, pp. 277–287, Oct. 2005.
[2] A. C. Durgun, C. A. Balanis, C. R. Birtcher, H. Huang, and H. Yu, "High-impedance surfaces with periodically perforated ground planes," *IEEE Trans. Antennas Propag.*, vol. 62, no. 9, pp. 4510–4517, Sep. 2014.
[3] L. Zhang, "Editorial: Big services era: Global trends of cloud computing and big data," *IEEE Trans. Services Comput.*, vol. 5, no. 4, pp. 467–468, Oct. 2012.
[4] S. Goldwasser, T. Y. Kalai, and N. G. Rothblum, "Delegating computation: Interactive proofs for muggles," *J. ACM*, vol. 62, no. 4, pp. 1–63, Aug. 2015.

[5] J. Halpern and V. S. Teague, "Rational secret sharing and multiparty computation: Extended abstract," in *Proc. 36th Annu. ACM Symp. Theory Comput.*, New York, NY, USA, May 2004, pp. 623–632.

[6] W. H. Press and F. J. Dyson, "Iterated Prisoner's Dilemma contains strategies that dominate any evolutionary opponent," *Proc. Nat. Acad. Sci. USA*, vol. 109, no. 26, pp. 10409–10413, 2012.

[7] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, Bethesda, MD, USA, Jun. 2009, pp. 169–178.

[8] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Proc. CRYPTO*, vol. 6223. Berlin, Germany: International Association for Cryptologic Research, May 2010, pp. 465–482.

[9] A. C. Yao, "Protocols for secure computations," in *Proc. 23rd Annu. Symp. Found. Comput. Sci.*, Chicago, IL, USA, Nov. 1982, pp. 60–65.

[10] K. Chung, Y. Kalai, and S. Vadhan, "Improved delegation of computation using fully homomorphic encryption," in *Proc. CRYPTO*, vol. 6223. Berlin, Germany: International Association for Cryptologic Research, May 2010, pp. 483–501.

[11] P. D. Azar and S. Micali, "Super-efficient rational proofs," in *Proc. 14th ACM Conf. Electron. Commerce*, Philadelphia, PA, USA, Jun. 2013, pp. 29–30.

[12] C. Hilbe, B. Wu, A. Traulsen, and M. A. Nowak, "Cooperation and control in multiplayer social dilemmas," *Proc. Nat. Acad. Sci. USA*, vol. 111, no. 46, pp. 16425–16430, Nov. 2014.

[13] G. Leonardo, S. Gary, M. G. Karina, and B. Gianmarco, "Connectivity and security in a D2D communication protocol for public safety applications," in *Proc. ISWCS*, Barcelona, Spain, Aug. 2014, pp. 548–552.

[14] J. Chen, S. Mccauley, and S. Singh, "Rational proofs with multiple provers," in *Proc. ITCS*, Cambridge, MA, USA, Jan. 2016, pp. 237–248.

[15] X. Yin, Y. L. Tian, and H. L. Wang, "Fair and rational delegation computation protocol," *J. Softw.*, vol. 29, no. 7, pp. 1953–1962, 2018.

[16] J. Chen and A. Zinger, "The robustness of zero-determinant strategies in Iterated Prisoner's Dilemma games," *J. Theor. Biol.*, vol. 357, pp. 46–54, Sep. 2014.

[17] C. Adami and A. Hintze, "Evolutionary instability of zero-determinant strategies demonstrates that winning is not everything," *Nature Commun.*, vol. 4, p. 2193, Aug. 2013.

[18] Z. Rong, Z. X. Wu, D. Hao, M. Z. Chen, and T. Zhou, "Diversity of timescale promotes the maintenance of extortioners in a spatial Prisoner's Dilemma game," *New J. Phys.*, vol. 17, no. 3, Mar. 2015, Art. no. 033032.

[19] A. H. Sodhro, Z. Luo, A. K. Sangaiah, and S. W. Baik, "Mobile edge computing based QoS optimization in medical healthcare applications," *Int. J. Inf. Manage.*, vol. 45, pp. 308–318, Apr. 2019.

[20] A. H. Sodhro, S. Pirbhulal, G. H. Sodhro, A. Gurtov, M. Muzammal, and Z. Luo, "A joint transmission power control and duty-cycle approach for smart healthcare system," *IEEE Sensors J.*, vol. 19, no. 19, pp. 8479–8486, Oct. 2019.

[21] J. Liu, Y. Li, C. Xu, and P. M. Hui, "Evolutionary behavior of generalized zero-determinant strategies in Iterated Prisoner's Dilemma," *Phys. A, Stat. Mech. Appl.*, vol. 430, pp. 81–92, Jul. 2015.

[22] A. Joel, C. Christian, P. Olivier, S. Ahmad-Reza, S. Berry, S. Abhi, and V. Ivan, "Summary report on rational cryptographic protocols," *Eur. Netw. Excellence Cryptol.*, vol. 30, pp. 510–525, Apr. 2007.

[23] L. Pan, D. Hao, Z. H. Rong, and T. Zhou, "Zero-determinant strategies in iterated public goods game," *Sci. Rep.*, vol. 5, p. 13096, Aug. 2015.

[24] I. Abraham, D. Dolev, R. Gonen, and J. Halpern, "Distributed computing meets game theory: Robust mechanisms for rational secret sharing and multiparty computation," in *Proc. PODC*, Denver, CL, USA, Jul. 2006, pp. 53–62.

[25] W. Ting, Z. Qin, and L. Zhao, "Publicly verifiable delegation of set intersection," in *Proc. Int. Conf. Cloud Comput. Internet Things*, Changchun, China, Dec. 2014, pp. 26–30.

[26] M. G. Yu and D. W. Guo, "Evolutionary dynamics of public goods game based on set structured populations," *J. Inf. Comput. Sci.*, vol. 9, no. 2, pp. 413–424, Nov. 2012.

[27] G. Ichinose and N. Masuda, "Zero-determinant strategies in finitely repeated games," *J. Theor. Biol.*, vol. 438, pp. 61–77, Feb. 2018.

[28] A. A. Chandio, D. J. Zhu, and A. H. Sodhro, "Integration of interconnectivity of information system (i3) using Web services," *Eng. Comput. Sci.*, vol. 2195, no. 1, pp. 651–655, May 2015.

[29] H. Magsi, A. H. Sodhro, F. A. Chachar, and S. A. Abro, "Evolution of 5G in Internet of medical things," in *Proc. iCoMET*, Sukkur, Pakistan, Mar. 2018, pp. 1–7, doi: 10.1109/ICOMET.2018.8346428.

[30] E. Akin, "Stable cooperative solutions for the Iterated Prisoner's Dilemma," 2013, *arXiv:1211.0969*. [Online]. Available: https://archive.org/details/arxiv-1211.0969/

[31] Q. Hu, S. L. Wang, L. Ma, R. F. Bie, and X. Z. Cheng, "Anti-malicious crowdsourcing using the zero-determinant strategy," in *Proc. ICDCS*, Atlanta, GA, USA, Jul. 2017, pp. 1137–1146.

[32] A. J. Stewart and J. B. Plotkin, "Extortion and cooperation in the Prisoner's Dilemma," *Proc. Nat. Acad. Sci. USA*, vol. 109, no. 26, pp. 10134–10135, Jun. 2012.

[33] A. J. Stewart and J. B. Plotkin, "From extortion to generosity, evolution in the Iterated Prisoner's Dilemma," *Proc. Nat. Acad. Sci. USA*, vol. 110, no. 38, pp. 15348–15353, Sep. 2013.

[34] C. Y. Dong, Y. L. Wang, and A. Aldweesh, "Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing," in *Proc. CCS*, Dallas, TX, USA, Oct. 2017, pp. 211–227.

DUO ZHANG received the B.Sc. degree in mathematics and applied mathematics from the Xi'an University of Science and Technology, China, in 2012, and the M.Sc. degree in applied mathematics from Guizhou University, China, in 2015, where he is currently pursuing the Ph.D. degree. His research interests include game theory and rational delegation computation.

YOULIANG TIAN received the B.Sc. degree in mathematics and applied mathematics and the M.Sc. degree in applied mathematics from Guizhou University, in 2004 and 2009, respectively, and the Ph.D. degree in cryptography from Xidian University, in 2012. From 2012 to 2015, he was a Postdoctoral Associate with the State Key Laboratory for Chinese Academy of Sciences. He is currently a Professor and a Ph.D. Supervisor with the College of Computer Science and Technology, Guizhou University. His research interests include algorithm game theory, cryptography, and security protocol.

CHAOYUE YUE was born in 1992. She is currently pursuing the master's degree with the College of Mathematics and Statistics, Guizhou University, Guiyang, China. Her main research interests include rational outsourcing computing and cryptography theory.

MEIMEI FAN received the B.Sc. degree in information management and information system from the Jiangxi University of Finance and Economics, in 2003, and the M.Sc. degree in computer software and theory from Guizhou University, in 2009. Her research interests include cryptography, information security, and security protocol.