An Entropy-View Secure Multi-Party Computation Protocol Based on Semi-honest Model

Yun Luo
Guizhou University
Yuling chen (ylchen3@gzu.edu.cn)
Guizhou University
Tao Li
Guizhou University
Yilei Wang
Qufu Normal University
Yixian Yang
Beijing University of Posts and Telecommnuications
Xiaomei Yu
Shandong Normal University

Research Article

Keywords: Secure Multi-Party Computation, Semi-Honest Model, Information Entropy, Mutual Information, Information Interaction

Posted Date: February 7th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1326438/v1

RESEARCH

An Entropy-View Secure Multi-Party Computation Protocol Based on Semi-honest Model

Yun Luo[1], Yuling chen[1*], Tao Li[1], Yilei Wang[2], Yixian Yang[3] and Xiaomei Yu[4]

*Correspondence:
ylchen3@gzu.edu.cn
[1]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China
Full list of author information is available at the end of the article

Abstract

Secure multi-party computation(SMPC) is an important research area in cryptography with many application scenarios, but there are still many problems to be solved. Aiming at security and fairness issues in SMPC, we consider that semi-honest participants are able to execute the protocol according to the specification, but there would be some additional malicious operations such as collusion and refuse to exchange information in the process of information interaction, which leads to deviations in the security and fairness of the protocol. To solve the above problems, we combine information entropy and mutual information to propose an n-round information exchange protocol, in which each participant broadcasts a relevant information value in each round without revealing additional information. The uncertainty of the correct result value is fuzzed by the interactive information in each round, and each participant cannot determine the correct result value until the end of the protocol, which effectively prevents malicious behavior and ensures the correct execution of the protocol. Security analysis and fairness analysis show that under the semi-honest model, our protocol guarantees the security and relative fairness of the output obtained by the participants after completing the protocol.

Keywords: Secure Multi-Party Computation; Semi-Honest Model; Information Entropy; Mutual Information; Information Interaction

Introduction

In the context of the rapid development of big data, cybersecurity information on the Internet and data privacy protection [1-3] have become inevitable issues in the security field, which data from different domains are cross-integrated, each participant forms an interactive scenario for distributed computing. This includes cloud computing, edge computing [4-7] for the internet of Things [8-11], and secure computing, among others. In the two-party computation due to insufficient computing power, their own data is encrypted and sent to the second party for computation and return the result value. Multi-party computation is formed when the number of participants increases, and disruption and advocacy actions [12-15]occur when multiple parties are involved in the computation. Secure multi-party computation can be expressed as multiple participants jointly calculating a common function, each participant has a private input. After the protocol is executed, a corresponding output is obtained. The security of SMPC is that each participant can only obtain the output corresponding to his own private input and cannot obtain other additional

information after the end of the protocol. The fairness of SMPC means that after the end of the protocol each participant can get its own output. Since SMPC does not need to rely on the existence of a trusted third party, all calculations are borne by each participant. By sending encrypted private data to other participants, after the other participants receive the data, through calculates and returns a corresponding the calculated value of is given to the sender. Security and fairness issues will arise during the implementation of the protocol. Integrity and trust [16]is an issue that exists between the parties involved, all participants include honest participants, semi-honest participants, and malicious participants [17]. The honest participants will only follow the rules of the protocol and will not perform malicious operations. The semi-honest parties will abide by the rules of the protocol, but there are some malicious operations have occurred, such as collusion, leaking intermediate data to adversaries, etc. Malicious participants will deviate from the implementation of the protocol and destroy the protocol in order to maximize their own interests. As in deep learning and machine learning [18,19], there are many security vulnerabilities and risks of malicious attacks. Among the three types of participants, the malicious participants have the strongest attack intensity and damage degree. For this type of participants, the current solution is mainly through a trusted third party, and the input is handed over to the trusted third party for calculation. The third parties distribute the corresponding output after calculating. But in many cases, there is no trusted third party, which is similar to the decentralized idea of blockchain [20,21]. Under the semi-honest model, it is usually not dependent on a trusted third party. The calculation and sending of messages are performed by the respective participants, it raises the issue of security and fairness. This problem is closely related to the subjective consciousness of the participants, and there will also be certain game situations between parties, which may cause the protocol to deviate. In order to eliminate these negative effects, this paper designs an n-round interactive protocol scheme based on information entropy under the semi-honest model to achieve the security and fairness of the SMPC protocol.

Related Work

In 1982, Yao [22] proposed two millionaire problems, forming a secure two-party computation protocol, using garbled circuit to ensure the security of computing under the semi-honest model. With the increase of participants, a secure multi-party computation protocol has been formed, and secure multi-party computation has unique advantages in processing private data. Zhao et al. [17] conducted theoretical and practical research on SMPC protocol, and explored cutting-edge methods on cloud SMPC protocol. With the in-depth research on SMPC, it has been widely used in many fields. Aiming at the problem of data sorting on insecure channels, Sun et al. [23] studied the efficient calculation and sorting of secure multi-party computation on insecure channels. Based on the privacy protection problem of symmetric homomorphic encryption, an effective secure multi-party computation protocol is proposed. Regarding data security and efficiency issues in the field of distributed data mining, Liu et al. [24] can protect data privacy based on the SPDZ protocol (SMPC's computing framework), and Bogdanov et al. [25] proposed a high-performance secure multi-party computation protocol for data mining. In order to

realize a secure multi-party protocol using anonymization, Shukla et al. [26] combined an asymmetric encryption scheme and it relies on the existence of a credible third party, but it is difficult to find a credible third party in practical. Secure multiparty computation protocol require higher safety at malicious model, in order to prevent the malicious adversary departing protocol breach security protocol, Mishra et al [27] extended the Encrytpo_Random protocol to introduce multiple trusted third parties, such that the security of the data is further guaranteed, and an attempt is made to further strengthen the existing protocol, thereby paving the way for a safer multi-party computation process. For the practical application of SMPC, Naidu et al. [28] combined cryptography and secure multi-party computation technology to create an electronic voting system, which has high research value and significance. In the case of rational participants (semi-honest parties), Groce et al. [29] explored the fairness of the participants in the implementation of the protocol, and considered the fairness of the two parties, that is, the two parties participating in the protocol after the end of the protocol both can get the correct output.

Since Shannon created information theory, information entropy [30,31] is often used as a tool to measure the amount of information change. During the execution of the calculation protocol between two parties, due to the different beliefs of the participants, the beliefs at a certain moment cause the participants to believe that their own benefits can be maximized, and they may act that deviates the fairness of the protocol. For example, if participant A receives a correct value sent by participant B, and A refuses to send B's correct value to B and terminates the protocol. At this time, A receives the correct value but B does not receive it, causing the unfairness of the protocol. In response to this unfairness, Wang [32] used belief and entropy to design a new utility function. Under the rational participants, by increasing the number of protocol rounds, the random number is sent before the i-th round, and the correct value is sent after the i-round, so that there are only two each participant compares the entropy of the value received before and after the rounds. If it is equal, the received result is the correct value, otherwise it is not the correct value. This makes the participants believe that they have not received the correct value and can only continue to execute the protocol, thereby ensuring the fairness of the protocol. Ah-Fat et al. [33] used entropy to quantify the amount of information leakage in the public output of the public function of secure multi-party computation, and considered the function replacement scheme, replacing the function that displays sensitive data with one an approximate function to enhance the confidentiality of the input and control the degree of distortion of the output value. In order to achieve a single-round distributed decryption of multi-key ciphertexts, Mukherjee et al. [34,35] performed multi-party calculations based on the MFHE structure of LWE, it makes the protocol more flexible. In practice, data is distributed among different parties, in response to the problem of malicious destruction of the integrity of data, Sundari et al. [36] expanded the field of secure computing, using secure multi-party computation technology for data integrity protection to prevent general or malicious destruction. Aiming at the strategy of using garbled circuit technology to replace functions only to solve the problem of two-party calculation, Riazi et al. [37] extended it on multi-party computation and made some improvements to

promote the implementation of scalable SMPC in practice. Due to the abusive use of a lot of data, in order to make the private data use pricing problem, Shen et al. [38] used information entropy to quantitatively analyze the private data, so that the use of private data can be effectively and reasonably distributed, and discussed issues such as price measurement of private data. In the field of smart cities and smart applications [39,40], intelligent computing is still needed for intelligence and cyber security to solve the problem of security vulnerabilities in products and to ensure security. Additionally, Wang et al. [32] explored the fairness of secure two-party computation, and we extended it to secure multi-party computation to study security and fairness issues.

Our Contributions

During the execution of the SMPC protocol, the presence of semi-honest parties causes multiple semi-honest parties to collude. As shown in Figure 1(a) below, by colluding with each other to exchange information and obtain information held by other semi-honest parties in order to increase the amount of information they hold, this poses a threat to the information security of other parties and undermines the security of the protocol. For this problem, the situation where it gets a little collusion advantage by weakening the advantage gained by collusion of multiple semi-honest parties is not enough to affect the information security of other participants.

Figure 1: Security and fairness issues under the SMPC semi-honest model

In secure multi-party computation, each participant P_i has a different utility belief. After the participant interacts with other participants, if P_i can determine that the information that has been received from a participant is his correct result value, he will measure his own benefit. After the participant P_i thinks that he has received the correct result value, if he refuses to send the correct result value to the Participants can maximize their own benefits, and P_i will terminate the information interaction with the participant and refuse to send the correct result value, as shown in Figure 1(b). At this time, the fairness of the secure multi-party computation protocol has shifted. To address this problem, information entropy and mutual information are introduced in secure multi-party computation to quantify the information of the interaction. Each participant divides his private data into n subproblems and assigns them to n participants, then compute the corresponding problem solution and use it as interaction information. Uncertainty [41] about the correct value through fuzziness prevents participants from obtaining the corresponding information in advance, it can be guaranteed that each participant will be relatively fair at the end of the protocol.

this paper conducts n rounds of protocol interaction under the semi-honest model, and quantitatively analyzes the information of each round of protocol interaction through entropy and mutual information, in order to seek the security and fairness of the protocol. The main works of this paper are as follows:

(1) This protocol uses mutual information and entropy to quantify each round of interaction information. Each participant has n interaction messages and performs n

rounds of the information exchange protocol. Each round randomly broadcasts one of the interaction messages to the other participants. At the end of the protocol, each participant integrates all relevant information to recover the corresponding correct values.

(2) In each round of information exchange between the parties in the protocol, the semi-honest party seeks to obtain additional information and threatens the information security of the other parties through malicious operations. In this paper, we consider collusion of (n-1)/2 semi-honest parties based on the semi-honest model to ensure the information security of other participants and make the protocol secure.

(3) To address the problem that participants obtain their own relevant information in advance during the execution of the protocol and thus terminate the information exchange with a certain participant, this paper investigates the change of association between the interactive information and the correct value in each round, and all participants cannot obtain their own relevant information in advance and can only continue to execute the protocol, thus ensuring the fairness of all parties to the protocol.

Preliminaries

Secure Multi-Party Computation

Secure multi-party computation can be expressed as n participants $P_1, P_2, ..., P_n$, and $X_1, X_2, ..., X_n$ correspond to the respective initial input carried by each participant, n participants agree on a common function f to be calculated. Participants implement a secure multi-party computation protocol so that there is $f(X_1, X_2, ..., X_n) = (Y_1, Y_2, ..., Y_n)$ after the calculation Where Y_j is the one-to-one corresponding output of X_i $(i, j = 1, 2, ..., n)$, and after the calculation, the n participants can only obtain the output corresponding to their own input, but cannot obtain other additional information.

Secure multi-party computation can be divided into honest/semi-honest model and malicious model according to the computing model, the solution in this paper is based on the semi-honest model for research. In secure multi-party computation, a semi-honest participant refers to a participant whose degree of damage is between the honest participant and the malicious participant [32]. Under the semi-honest model, there must be at most $t < [n/2]$ Semi-honest parties, otherwise the security of the protocol cannot be guaranteed. In the semi-honest model of secure multi-party computation, all participants will perform calculations in accordance with the rules of the protocol, but there may be situations in which multiple participants collude or are controlled by an adversary. In order to obtain additional information, these participants will exchange their calculation data or intermediate results and other information, the participants controlled by the adversary will send these data directly to the adversary to enhance the adversary's attack capability.

Information Entropy

The concept of entropy first appeared in physics, representing changes in energy [32,33]. Shannon [30] later used entropy to create information theory. Since then, Information entropy [31] has become the uncertainty of information indicators that indicate the occurrence of events.

Definition 1 (Self-information quantity $I(x_i)$): x_i represents a certain random variable, $p(x_i)$ represents the probability of occurrence of x_i, when $p(x_i)$ is smaller, that is, the probability of occurrence of x_i is smaller, then the amount of information that can be provided after the occurrence of x_i The bigger it is, it is defined as:

$$I(x_i) = -logp(x_i) \tag{1}$$

There are two explanations for this formula. (1) Before the event: it represents the uncertainty of the event. (2) After the event occurs: Indicates the amount of information that the event can provide.

Definition 2 (Mutual information $I(x_i; y_j)$): Mutual information measures the correlation between two events, denoted as: estimate the expected value as

$$I(x_i; y_j) = \sum_{i=1}^{n}\sum_{j=1}^{n} p(x_i, y_j) log\frac{p(x_i, y_j)}{p(x_i)p(x_j)} \tag{2}$$

The information sent by the source is x_i, the sink receives y_j, $p(x_i|y_j)$ represents the posterior probability, which refers to the probability when y_j is known, and $p(x_i)$ represents the prior probability, which refers to the probability when y_j is unknown.

Definition 3 (Information entropy $H(x_i)$): Let x_i be a discrete random variable, and its corresponding probability is $p(x_i)(i = 1, 2, ..., n)$, then:

$$H(x_i) = -\sum_{i=1}^{n} p(x_i) logp(x_i) \tag{3}$$

Secret sharing

Secret sharing [42] means that a secret information is divided into multiple parts in a distributed network and managed by different participants. A single participant cannot recover the complete information, only a few participants or all participants can Restore the original secret. It can be formally expressed as a (t, n) threshold scheme, which divides the secret into n shares to share with different users. When t $(t \leq n)$ shared secrets are known, the secret can be calculated. The secret cannot be obtained when there are t shared secrets. At the same time, secret sharing can also be used to protect multiple secrets, and different secrets are associated with different authorized subsets. In the secret sharing scheme involving n users, if one cannot be trusted, this person can be removed and become a secret sharing scheme involving n-1 users. Secret sharing can protect any type of data, and is mainly used for key management and information protection.

Our Proposed Protocol

Information exchange protocol

Through each round of randomly sending the interactive information of a certain participant, the participants carry out n rounds of information interaction, and the protocol is as follows:

Information exchange protocol

Step1: Each participant P_i divides its input into n sub-problems as the initial privacy input $privacy_{data_i}^{input}(1 \leq i \leq n)$, after being encrypted by the encryption algorithm $Enc_{privacy}$ Sent to other participants separately.

Step2: After the participants receive $Enc_{privacy_i}$ from Step 1, they use the public function f to calculate the encrypted data from all participants as follows : $f_i(Enc_{privacy_1}, Enc_{privacy_2}, ..., Enc_{privacy_n}) \rightarrow Output_i(x_1, x_2, ..., x_n)$, which means that the i-th participant P_i calculates the encrypted data of each participant as the parameter of function f, and obtains the corresponding output $x_1, x_2, ..., x_n$.

Step3: Each participant uses the output of Step2 as the information to be interacted, and the participant P_i randomly selects one from $x_1, x_2, ..., x_n$ as a round of interactive information, and broadcasts it to all other participants $\overline{P_i}$:

·Round 1:$P_i$randomly selects an interactive information $x_i \in x_1, x_2, ..., x_n$ to broadcast to $\overline{P_i}$, and x_i corresponds to the relevant information of a participant in $\overline{P_i}$.

·Round 2: Excluding the x_i selected in the first round, P_i uses the remaining interactive information $x_1, x_2, ...x_{i-1}, x_{i+1}, ..., x_n$ randomly select one of them to broadcast.

....

·Round n: Broadcast the last interactive message.

Step4: After n rounds of protocol interaction are completed, if no participant terminates the protocol during the execution of the protocol, the result of the protocol is that the participants $P_1P_2...P_n$ have all their own relevant information, and the corresponding correct value is restored by integrating all relevant information. The output value is also called the correct result value.

Step5: All participants withdrew from the protocol and the protocol ended.

In secure multi-party computation, there are many fairness issues [29] and security issues [43]. If a trusted third party exists, each participant can fully transfer their privacy input to a trusted third party for calculation, and distribute the output back to the corresponding participants. This type of protocol relies heavily on the existence of a trusted third party, but in many cases, it is difficult to find a trusted third party. Therefore, in the case of removing the trusted third party, each participant can only undertake the tasks of calculation and transmission. For security and fairness considerations, each participant has n pieces of interactive information, and each interactive information corresponds to one participant's relevant information. Only when the participants obtain all n relevant information, can they integrate their own correct values.

N-round SMPC protocol scheme based on information entropy

Under the semi-honest model, since the attack capability of each participant is between the honest party and the malicious honest party [44], and the semi-honest party will execute according to the rules of the protocol, without the malicious participants deviating from the protocol. If the situation exists, there will only be multiple semi-honest parties colluding to exchange information or sending their own

intermediate output and private input to the adversary to increase the adversary's attack capability. Therefore, this paper introduces information entropy for n rounds of multi-party calculations based on the semi-honest model.

Figure 2: Flow chart of n-round information exchange

The program interaction process is shown in Figure 2. The interactive information value sent by the participant P_i in each round with a certain probability is $x_i^t(i, t \in 1, 2, ..., n)$, x_i^t is the randomly selected interactive information. After receiving this value, the other n-1 participants will calculate the mutual information $I(x_{p_i}; x_i^t)$. Until the end of the protocol, the other participants compare all the interactive information received by P_i with the mutual information of the correct value, and the one with the largest mutual information value is its own correct value relevant information.

(1) The secure multi-party computation protocol performs n rounds of calculations, $(x_1^1 x_1^2 ... x_1^n), ..., (x_n^1 x_n^2 ... x_n^n)$ respectively correspond to the participants $P_1 P_2 ... P_n$ with n rounds of interactive information with a certain probability $p(x_i^t)$, x_i^t represents the relevant information interacted in the protocol, that is, the information to be transmitted by the participant P_i in the $t(1 \leq t \leq n)$ round, andx_i^t is related information about a random participant from P_i, each participant has its own correct result value x_{p_i} and has an entropy value $H(x_{p_i}) = -p(x_{p_i}) log p(x_{p_i})$ with a very small prior probability $p(x_{p_i})$. Through the implementation of the protocol to obtain information from other participants to form a new posterior probability.

(2) N rounds of secure multi-party calculation. Each round of the participants will randomly select one from the interactive information they have and broadcast it to all other participants. This interactive information only corresponds to the relevant information of one of the participants. For example, in the first round choose one randomly from n interactive information, and choose from the remaining n-1 in the second round...until the end of the n-th round.

(3) During the execution of the protocol, each time the participant receives a interactive information value, and calculate its mutual information relative to the correct information. The interactive information received by each participant has the largest amount of mutual information relative to the correct value is its own relevant information. Because in the current round, the participants do not know whether they have received their own relevant information, so they can only continue to interact with other participants in order to expect to obtain the interactive information corresponding to the maximum mutual information value in the next rounds, that is, you have received your own relevant information value. In the multi-symbol channel, when the source and the sink are exchanging information, the information rate of the channel can be maximized by adjusting the distribution of the information, that is, $I(x_{p_i}; x_k^c)$ can reach the maximum, expressed as $:\underbrace{max}_{p(x_k^c)} I(x_{p_i}; x_k^c) = \underbrace{max}_{p(x_k^c)} H(x_{p_i}) - H(x_{p_i}|x_k^c)$.

(4) After the end of the n-th round of the protocol, each participant will integrate all relevant information screened out by (3)$x_1^{c_1} \oplus x_2^{c_2} \oplus ... \oplus x_n^{c_n} = x_{p_i}, j = 1, 23..., n$,

where c_1,c_2, ..., $c_n \in 1, 2, 3...n$ represents the number of rounds , $x_i^c(c = c1, c2, ..., cn)$ represents the information sent by P_i in round c, x_{p_i} represents the correct result value of a participant, and $\oplus$ represents a certain algebraic operation that can integrate all The relevant information is restored to the correct value.

(5) The protocol is completed and terminated. Each participant has n-1 participants' relevant information. Each time a round of information exchange is conducted, the participants will randomly select one relevant information to broadcast. When the protocol is completed, each participant will receive all of its own relevant information.

Security and fairness analysis

Security analysis

Participants carry out n rounds of secure multi-party calculations. Starting from the first round, they will interact with other participants for the correct value of information. Since it is a secure multi-party calculation under the semi-honest model, each participant will execute it in accordance with the protocol. Considering the semi-honest model, the number of semi-honest parties does not exceed $n/2$, that is, not more than half of the number of all participants, we consider P_i to exchange information with other $(n/2) - 2$ parties Collusion.

(1) Assuming that $P_k, P_{k+1}, ..., P_m(1 \leq k, m \leq n)$ total $(n/2) - 1$ participants are semi-honest participants, each semi-honest participant has corresponding $(x_k^1 x_k^2 ... x_k^n), ..., (x_m^1 x_m^2 ... x_m^n)$ interactive information. From the beginning of the protocol, these semi-honest parties colluded to exchange all the information of each other, then the maximum amount of information that the semi-honest party $P_r(k \leq r \leq m)$can have in the t $(1 \leq t \leq n)$ round is:

$$\left(x_k^1 x_k^2 ... x_k^n, ..., x_m^1 x_m^2 ... x_m^n\right) \cup \left\{x_b^t \middle| b \neq k, ..., m, t \in [1, n]\right\} \tag{4}$$

Because $x_1^{c_1} \oplus x_2^{c_2} \oplus ... \oplus \underbrace{x_k^{c_k} \oplus ... \oplus x_m^{c_m}}_{\frac{n}{2}-1} \oplus ... \oplus x_n^{c_n} = x_{p_i}$, and the participants randomly send interactive information. In the first round, the probability that each participant receives relevant information about itself from another participant is $\frac{1}{n}$. If the semi-honest party wants to exchange information through collusion to achieve the purpose of inferring or predicting the information of other parties, then the semi-honest party gets information from the other $(n/2) - 2$ semi-honest parties. They need to obtain relevant information from $(n/2) + 1$ honest participants. Then the probability about the semi-honest party can learn the information of other participants in the $t >= 2$ round is $(\frac{1}{n} * ... * \frac{1}{n-t+1})^{[\frac{n}{2}]+1}$, when n is large enough, $(\frac{1}{n} * ... * \frac{1}{n-t+1})^{[\frac{n}{2}]+1} \leq negl$ is negligible. Therefore, the semi-honest party cannot calculate the correct results of the other parties and its own in advance. We uses a mutual information function to simulate the amount of information that each round of interactive information can bring, and obtain a change map of the difference in each round of mutual information. Assuming n=64, 64 rounds of information interaction between each participant, the change of the mutual information from the same participant to the correct value is shown in Figure 3:

Figure 3: Information from all rounds of the same participant reduces the uncertainty of the correct value

Figure 3 shows the change in the uncertainty reduction of the correct value caused by the change in the interactive information received from the same participant, which means that when receiving a message that can reduce the uncertainty of the correct value, each participant cannot determine in advance that this information is their own relevant information, and always expect to seek information with a greater amount of mutual information in subsequent rounds.

(2) After the semi-honest party colludes and receives all the information about itself from other semi-honest parties, the semi-honest party will use the relevant information to try to determine whether the information from the honest party is related to itself. When the semi-honest party colludes and interacts with the honest party:

$$I\left(x_{p_i}; x_b^t | x_k^c ... x_m^c\right) = \sum_{b \neq k,\ldots,m} \sum_{t=1}^{n} p\left(x_{p_i} x_b^t x_k^c \ldots x_m^c\right) log \frac{p\left(x_{p_i} | x_b^t x_k^c \ldots x_m^c\right)}{p\left(x_{p_i} | x_k^c \ldots x_m^c\right)} \quad (5)$$

$I(x_{p_i}; x_b^t | x_k^c ... x_m^c)$ denote that when the relevant information from $(n/2) - 2$ semi-honest participants is known, other honest participants are received After sending the information, the reduction in uncertainty of the correct result value. This value is used to judge whether the information from the honest party is related to a specific correct value. After receiving the information of the honest party, there are $0 \leq I(x_{p_i}; x_b^t | x_k^c ... x_m^c)$ and it will be too small, otherwise it will be too large, so in this case, the semi-honest party can only determine the information that can form the largest reduction in uncertainty in the before t round, but it does not certain whether this information is the largest reduction in uncertainty in all n rounds, and so far it is still impossible to determine the correct information. Participants can neither determine their own correct information before the end of the protocol, nor can they determine in advance whether a certain round of information from a participant is their own relevant information, and the honest party's information will be disclosed during the protocol process so the protocol is safe.

Fairness analysis

Wang et al. [32] redefines the utility function by entropy, the random number is send before the i round, and the correct result value is send after the i round, compare whether the entropy value of the front and back rounds is the same to judge whether the participants have obtained the correct result value. In contrast, this paper pays more attention to the amount of mutual information in the exchange of information in the protocol process. There are n participants $P_1, P_2, ...P_n$, each participant has interactive information x_i^c with a certain probability before proceeding with the protocol. For example, P_1 has the interactive information $x_1, x_2, ...x_n$, which the information exchanged from the first round is associated with the correct value of any one of the other $n-1$ participants.

(1) Each participant has relevant information of other $n-1$ participants, so there is a channel probability transition matrix in the process of channel transmission of rel evant information:

$$\begin{bmatrix} p(x_1|x_1) & p(x_2|x_1) & \ldots & p(x_n|x_1) \\ p(x_1|x_2) & p(x_2|x_2) & \ldots & p(x_n|x_2) \\ \ldots & \ldots & \ldots & \ldots \\ p(x_1|x_n) & p(x_2|x_n) & \ldots & p(x_n|x_n) \end{bmatrix} \tag{6}$$

Where x_i represents the relevant information required by the participant P_i, which means that the relevant information sent by each participant in any round is different from the relevant information sent in other rounds and corresponds to different recipients, and the interactive information is randomly selected send it.

(2) When the participant receives its own relevant information, the participant cannot confirm that it is his own relevant information, because he can only determine the information that has the largest amount of mutual information up to the current round. It is not necessarily the one with the largest amount of mutual information among all the information from the same participant. He can only continue to execute the protocol and send relevant information of other participants in order to expect other participants to send their relevant information. Each round of information from other participants has a mutual information to the correct value, which is expressed as follows:

$$\begin{aligned} I(x_{p_i}; x_k^c) &= p(x_{p_i}, x_k^c) log \frac{p(x_{p_i}|x_k^c)}{x_{p_i}} \\ &= -p(x_{p_i}) \, logp(x_{p_i}) + p(x_{p_i}, x_k^c) \, logp(x_{p_i}|x_k^c) \\ &= H(x_{p_i}) - H(x_{p_i}|x_k^c)(1 \leq i, k, c \leq n) \end{aligned} \tag{7}$$

Where x_{p_i} represents the correct value of the participant P_i after the end of the protocol and integrates its own relevant information to recover its correct value, x_k^c represents the information is sent by the participant P_k in the c round, this information is related to other $n-1$ participants. When the $n-1$ participants receive the interactive information x_k^c, they will judge based on this information, and the criterion for judging is whether this information is the one that reduces the uncertainty of their correct information the most. Each participant needs to consider the degree of correlation between the information he wants to interact and the true correct result value in each round of information exchange.

(3) If P_i receives interactive information from the same participant in a certain round, the relative correct value of the mutual information value is greater than the mutual information value of other rounds, but P_i does not know that he has received the correct value for related information, only after the last round, that is, the n-th round of interactive information, compare the mutual information value of each round, then the participant P_i knows that the round of information with the largest mutual information is its relevant information can be integrated to restore the correct value. If the participants have a certain probability to predict their correct value in the later round of the protocol, since each participant randomly

selects the interactive information to send, then the other participants will have a correspondingly similar probability to predict their correct value, thus ensuring the relative fairness of the protocol.

During the execution of the protocol, the information value is calculated and recorded in each round, and the change in the uncertainty of the correct value of the interactive information is used to prevent the semi-honest participants from terminating the protocol, which makes the fairness deviate. In this way, the fairness of the protocol is guaranteed. At the end of the protocol, each participant can receive its own relevant information at the end, and the correct value can be restored by integrating it. The comparison between this paper and Wang et al. [32] and Ah-Fat et al. [33] is shown in Table 1:

Table 1: Security and fairness comparison between this article and Wang et al. [32] and Ah-Fat et al. [33]

scheme	Trusted third party	Security	Fairness
Wang et al. [32]	×	Yes	Fairness based on beliefs
Ah-Fat et al. [33]	✓	Rely on TTP and f	Rely on the fairness of TTP
Our protocol	×	Yes	Relatively fair

Wang et al. [32] combined the concepts of entropy and belief to redefine utility, assuming that the correct values of the two participants are the same, and ensure the fairness of the two participants in the secure two-party computation. Ah-Fat et al. [33] proposed to use an approximate function to replace the defective public function in SMPC, made a trade-off between input privacy and output accuracy, and used trusted hardware or a trusted third party to ensure the security and fairness of the protocol. Compared with this paper, entropy and mutual information are used to quantify interactive information in secure multi-party computation to ensure the relative fairness of each participant. The final correct information for each participant is different, and relatively fairness can be obtained at the end of the protocol.

Conclusion

In secure multi-party computation, there are rational participants and malicious participants. The rational participants will execute the protocol according to the steps of the protocol. The malicious participants can execute or deviate from the protocol according to their own wishes. The purpose is to destroy the interests of others or to pursue do whatever it takes in their best interest. This paper studies the security and fairness issues that exist in the process of protocol and interaction information between multiple parties under the semi-honest model, and combines the relevant knowledge of information theory to formulate a reasonable information interaction protocol. By sending the interactive information randomly, use entropy and mutual information to quantify the amount of interactive information, aiming at the correlation between interactive information and correct value information, in order to pursue all participants participating in the protocol, at the end there is a corresponding probability to determine the correct value, eliminating the game when the protocol is completed. After the protocol is completed, security and a relative fairness can be guaranteed. Under the malicious model, there are many

uncontrollable factors for the participants, and higher security and fairness requirements are required. For this reason, it is important to rely on a trusted third party to solve this problem, but it is difficult to find a trusted third party. How to eliminate the existence of a third party to ensure the security and fairness of the protocol is a question worth discussing.

In addition, secure multi-party computation involves various domains, but the efficiency of secure multi-party computation has been widely criticized. For future prospects, the next step will be to focus more on the efficiency of secure multi-party computing. Both blockchain and secure multi-party computation require a third party, and smart contracts are very helpful for the proper execution of the protocol. By combining with blockchain, the security of the protocol can be enhanced. As well as the extended application of secure multi-party computation in the quantum domain, combined with federated learning, homomorphic cryptography, etc., these can greatly improve the efficiency. If more optimizations of SMPC can be successfully implemented, it will be a great research progress in the field of SMPC.

Acknowledgements
This research was supported by both State Key Laboratory of Public Big Data, College of Computer Science and Technology that of Guizhou University.

Funding
This study is supported by Foundation of National Natural Science Foundation of China(Grant Number:61962009), Major Scientific and Technological Special Project of Guizhou Province (20183001), Science and Technology Support Plan of Guizhou Province ([2020] 2Y011), Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No.2018BDKFJJ003).

Abbreviations
SMPC:Secure Multi-party Computation;TTP:Trusted Third Party.

Availability of data and material
Data sharing is not applicable to this paper as no datasets were generated or analyzed during the current study.

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

Authors' contributions
YL was a major contributor in writing the manuscript as a 1st Author and others were Co-Corresponding Authors. YC and TL proposed some ideas. YW,YY and XY gave some important suggestions for this paper. All authors read and approved the final manuscript.

Author details
[1]State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China. [2]School of Computer Science, Qufu Normal University, Rizhao, China. [3]School of Cyberspace Security, Beijing University of Posts and Telecommnuications, Beijing, China. [4]School of Information Science and Engineering, Shandong Normal University, Jinan, China.

References

1. Ma, P., Jiang, B., Lu, Z., Li, N., Jiang, Z.: Cybersecurity named entity recognition using bidirectional long short-term memory with conditional random fields. Tsinghua Science and Technology **26**(3), 259–265 (2021). doi:10.26599/TST.2019.9010033 (document)
2. Kou, H., Liu, H., Duan, Y., Gong, W., Xu, Y., Xu, X., Qi, L.: Building trust/distrust relationships on signed social service network through privacy-aware link prediction process. Applied Soft Computing **100**, 106942 (2021). doi:10.1016/j.asoc.2020.106942 (document)
3. Li, Y.C.S.Y.Y.T., Zhou, X.N.H.: Pssp: A source location privacy protection scheme based on sector phantom routing in wsns. International Journal of Intelligent Systems. (2021). Doi:10.1002/int.22666 (document)
4. Huang, J., Lv, B., Wu, Y., Chen, Y., Shen, X.: Dynamic admission control and resource allocation for mobile edge computing enabled small cell network. IEEE Transactions on Vehicular Technology, 1–1 (2021). doi:10.1109/TVT.2021.3133696 (document)
5. Chen, Y., Zhang, N., Zhang, Y., Chen, X., Wu, W., Shen, X.S.: Toffee: Task offloading and frequency scaling for energy efficiency of mobile devices in mobile edge computing. IEEE Transactions on Cloud Computing **9**(4), 1634–1644 (2021). doi:10.1109/TCC.2019.2923692 (document)
6. Y. Chen, Y.L.X.C. F. Zhao: Dynamic task offloading for mobile edge computing with hybrid energy supply. Tsinghua Science and Technology (2021). doi:0.26599/TST.2021.9010050 (document)

7. Huang, J., Lan, Y., Xu, M.: A simulation-based approach of qos-aware service selection in mobile edge computing. Wireless Communications and Mobile Computing **2018**, 1–10 (2018). doi:10.1155/2018/5485461 (document)
8. Li, F., Wang, D., Wang, Y., Yu, X., Wu, N., Yu, J., Zhou, H.: Wireless communications and mobile computing blockchain-based trust management in distributed internet of things. Wireless Communications and Mobile Computing **2020**, 1–12 (2020). doi:10.1155/2020/8864533 (document)
9. Wei, D., Ning, H., Shi, F., Wan, Y., Xu, J., Yang, S., Zhu, L.: Dataflow management in the internet of things: Sensing, control, and security. Tsinghua Science and Technology **26**(6), 918–930 (2021). doi:10.26599/TST.2021.9010029 (document)
10. Azrour, M., Mabrouki, J., Guezzaz, A., Farhaoui, Y.: New enhanced authentication protocol for internet of things. Big Data Mining and Analytics **4**(1), 1–9 (2021). doi:10.26599/BDMA.2020.9020010 (document)
11. Jiwei Huang, J.Z. Chenxiang Zhang: A multi-queue approach of energy efficient task scheduling for sensor hubs. Chinese Journal of Electronics **29**(2), 242–247 (2020) (document)
12. Li, T., Wang, Z., Yang, G., Cui, Y., Chen, Y., Yu, X.: Semi-selfish mining based on hidden markov decision process. International Journal of Intelligent Systems **36** (2021). doi:10.1002/int.22428 (document)
13. Wang, Y., Yang, G., Bracciali, A., Leung, H.-f., Tian, H., Ke, L., Yu, X.: Incentive compatible and anti-compounding of wealth in proof-of-stake. Information Sciences **530** (2020). doi:10.1016/j.ins.2020.03.098 (document)
14. Li, T., Chen, Y., Wang, Y., Wang, Y., Zhao, M., Zhu, H., Tian, Y., Yu, X., Yang, Y.: Rational protocols and attacks in blockchain system. Security and Communication Networks **2020**, 1–11 (2020). doi:10.1155/2020/8839047 (document)
15. Li, T., Wang, Z., Chen, Y., Li, C., Jia, Y., Yang, Y.: Is semi-selfish mining available without being detected? International Journal of Intelligent Systems. (2021). Doi:10.1002/int.22656 (document)
16. Wang, F., Zhu, H., Srivastava, G., Li, S., Khosravi, M., Qi, L.: Robust collaborative filtering recommendation with user-item-trust records. IEEE Transactions on Computational Social Systems **PP**, 1–11 (2021). doi:10.1109/TCSS.2021.3064213 (document)
17. Zhao, C., Zhao, S., Zhao, M., Chen, Z., Gao, C.-Z., Li, H., yu-an, T.: Secure multi-party computation: Theory, practice and applications. Information Sciences **476** (2018). doi:10.1016/j.ins.2018.10.024 (document)
18. Chen, H., Zhang, Y., Cao, Y., Xie, J.: Security issues and defensive approaches in deep learning frameworks. Tsinghua Science and Technology **26**(6), 894–905 (2021). doi:10.26599/TST.2020.9010050 (document)
19. Guezzaz, A., Asimi, Y., Azrour, M., Asimi, A.: Mathematical validation of proposed machine learning classifier for heterogeneous traffic and anomaly detection. Big Data Mining and Analytics **4**(1), 18–24 (2021). doi:10.26599/BDMA.2020.9020019 (document)
20. Wang, Y., Wang, Y., Wang, Z., Yang, G., Yu, X.: Research cooperations of blockchain: toward the view of complexity network. Journal of Ambient Intelligence and Humanized Computing, 1–14 (2020). doi:10.1007/s12652-020-02596-6 (document)
21. Li, P., Li, K., Wang, Y., Zheng, Y., Wang, D., Yang, G., Yu, X.: A systematic mapping study for blockchain based on complex network. Concurrency and Computation: Practice and Experience (2020). doi:10.1002/cpe.5712 (document)
22. Yao, A.C.: Protocols for secure computations. In: 23rd Annual Symposium on Foundations of Computer Science (sfcs 1982), pp. 160–164 (1982). doi:10.1109/SFCS.1982.38 (document)
23. Sun, Y., Wen, Q., Zhang, Y.-D., Huan, Z., Jin, Z.: Efficient secure multiparty computation protocol for sequencing problem over insecure channel. Mathematical Problems in Engineering **2013** (2013). doi:10.1155/2013/172718 (document)
24. Liu, J., Tian, Y., Zhou, Y., Xiao, Y., Ansari, N.: Privacy preserving distributed data mining based on secure multi-party computation. Computer Communications **153**, 208–216 (2020). doi:10.1016/j.comcom.2020.02.014 (document)
25. Bogdanov, D., Niitsoo, M., Toft, T., Willemson, J.: High-performance secure multi-party computation for data mining applications. International Journal of Information Security **11** (2012). doi:10.1007/s10207-012-0177-2 (document)
26. Shukla, S., Sadashivappa, G.: Secure multi-party computation protocol using asymmetric encryption. In: 2014 International Conference on Computing for Sustainable Global Development (INDIACom), pp. 780–785 (2014). doi:10.1109/IndiaCom.2014.6828069 (document)
27. Mishra, D., Koria, N., Kapoor, N., Bahety, R.: Malicious computation prevention protocol for secure multi-party computation. TENCON 2009 - 2009 IEEE Region 10 Conference, 1–6 (2009) (document)
28. Naidu, P., Kharat, R., Tekade, R., Mendhe, P., Magade, V.: E-voting system using visual cryptography & secure multi-party computation, pp. 1–4 (2016). doi:10.1109/ICCUBEA.2016.7860062 (document)
29. Groce, A., Katz, J.: Fair computation with rational players, vol. 2011, p. 396 (2011). doi:10.1007/978-3-642-29011-4_7 (document)
30. Shannon, C.E.: A mathematical theory of communication. Acm Sigmobile Mobile Computing & Communications Review **5**, 3–55 (2001). doi:10.1145/584091.584093 (document)
31. Yang, Y.X., Niu, X.X.: The General Theory of Information Security. Publishing House of Electronics Industry, New Haven (2018) (document)
32. Wang, Y., Yang, G., Li, T., Li, F., Tian, Y., Yu, X.: Belief and fairness: A secure two-party protocol toward the view of entropy for iot devices. Journal of Network and Computer Applications **161**, 102641 (2020). doi:10.1016/j.jnca.2020.102641 (document), 1
33. Ah-Fat, P., Huth, M.: Optimal accuracy-privacy trade-off for secure multi-party computations. IEEE Transactions on Information Theory **PP** (2018). doi:10.1109/TIT.2018.2886458 (document), 1
34. Mukherjee, P., Wichs, D.: Two round multiparty computation via multi-key fhe, pp. 735–763 (2016). doi:10.1007/978-3-662-49896-5_26 (document)
35. Chen, Y., Dong, S., Li, T., Wang, Y., Zhou, H.: Dynamic multi-key fhe in asymmetric key setting from lwe. IEEE Transactions on Information Forensics and Security **16**, 5239–5249 (2021).

doi:10.1109/TIFS.2021.3127023 (document)
36. S, S., Manikandan, A.: Secure multi-party computation in differential private data with data integrity protection, pp. 180–184 (2015). doi:10.1109/ICCCT2.2015.7292742 (document)
37. Riazi, S., Javaheripi, M., Hussain, S.U., Koushanfar, F.: Mpcircuits: Optimized circuit generation for secure multi-party computation, pp. 198–207 (2019). doi:10.1109/HST.2019.8740831 (document)
38. Shen, Y., Guo, B., Shen, Y., Duan, X., Dong, X., Zhang, H.: Pricing personal data based on information entropy. Association for Computing Machinery, New York, NY, USA (2019). doi:10.1145/3305160.3305204. https://doi.org/10.1145/3305160.3305204 (document)
39. Tong, Z., Ye, F., Yan, M., Liu, H., Basodi, S.: A survey on algorithms for intelligent computing and smart city applications. Big Data Mining and Analytics **4**(3), 155–172 (2021). doi:10.26599/BDMA.2020.9020029 (document)
40. Tang, J., Li, R., Wang, K., Gu, X., Xu, Z.: A novel hybrid method to analyze security vulnerabilities in android applications. Tsinghua Science and Technology **25**(5), 589–603 (2020). doi:10.26599/TST.2019.9010067 (document)
41. Bhardwaj, N., Sharma, P.: An advanced uncertainty measure using fuzzy soft sets: Application to decision-making problems. Big Data Mining and Analytics **4**(2), 94–103 (2021). doi:10.26599/BDMA.2020.9020020 (document)
42. Schillinger, F., Schindelhauer, C.: Crucial and redundant shares and compartments in secret sharing, pp. 1–7 (2020). doi:10.1109/AICCSA50499.2020.9316460 (document)
43. Mishra, D., Pathak, R., Joshi, S., Ludhiyani, A.: Secure multi-party computation for statistical computations using virtual parties on a token ring network, pp. 1–6 (2010). doi:10.1109/WOCN.2010.5587326 (document)
44. Akbari Nodehi, H., Maddah-Ali, M.: Secure coded multi-party computation for massive matrix operations. IEEE Transactions on Information Theory **PP**, 1–1 (2021). doi:10.1109/TIT.2021.3050853 (document)

Figures

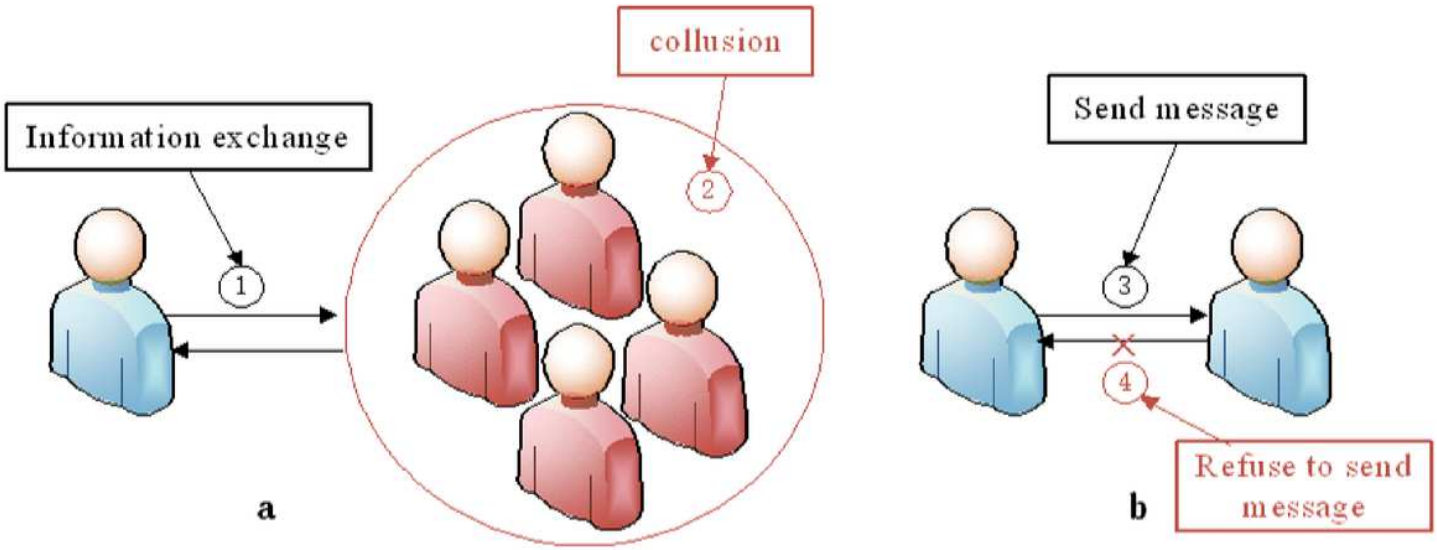

Figure 1

Security and fairness issues under the SMPC semi-honest model

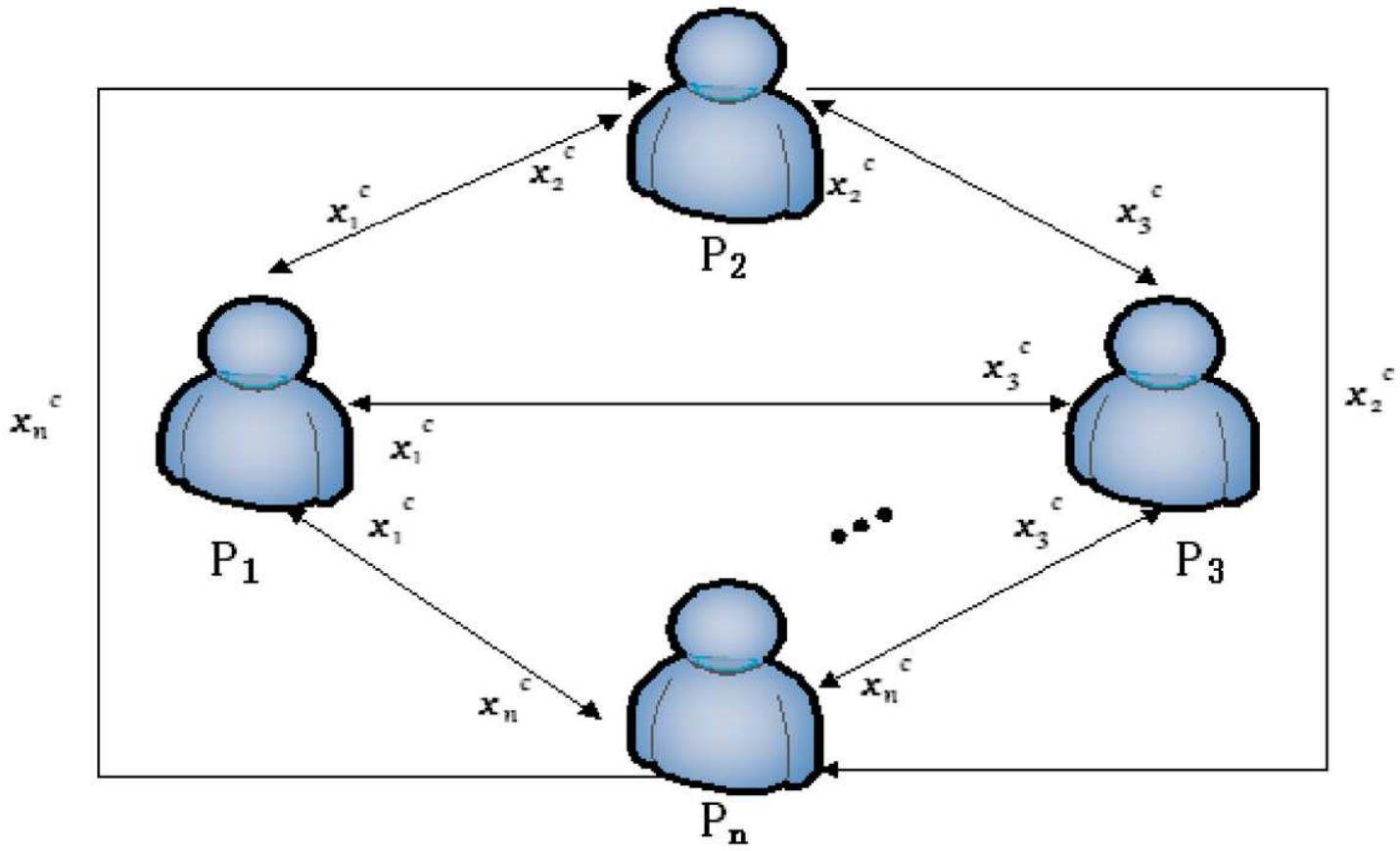

Figure 2

Flow chart of n-round information exchange

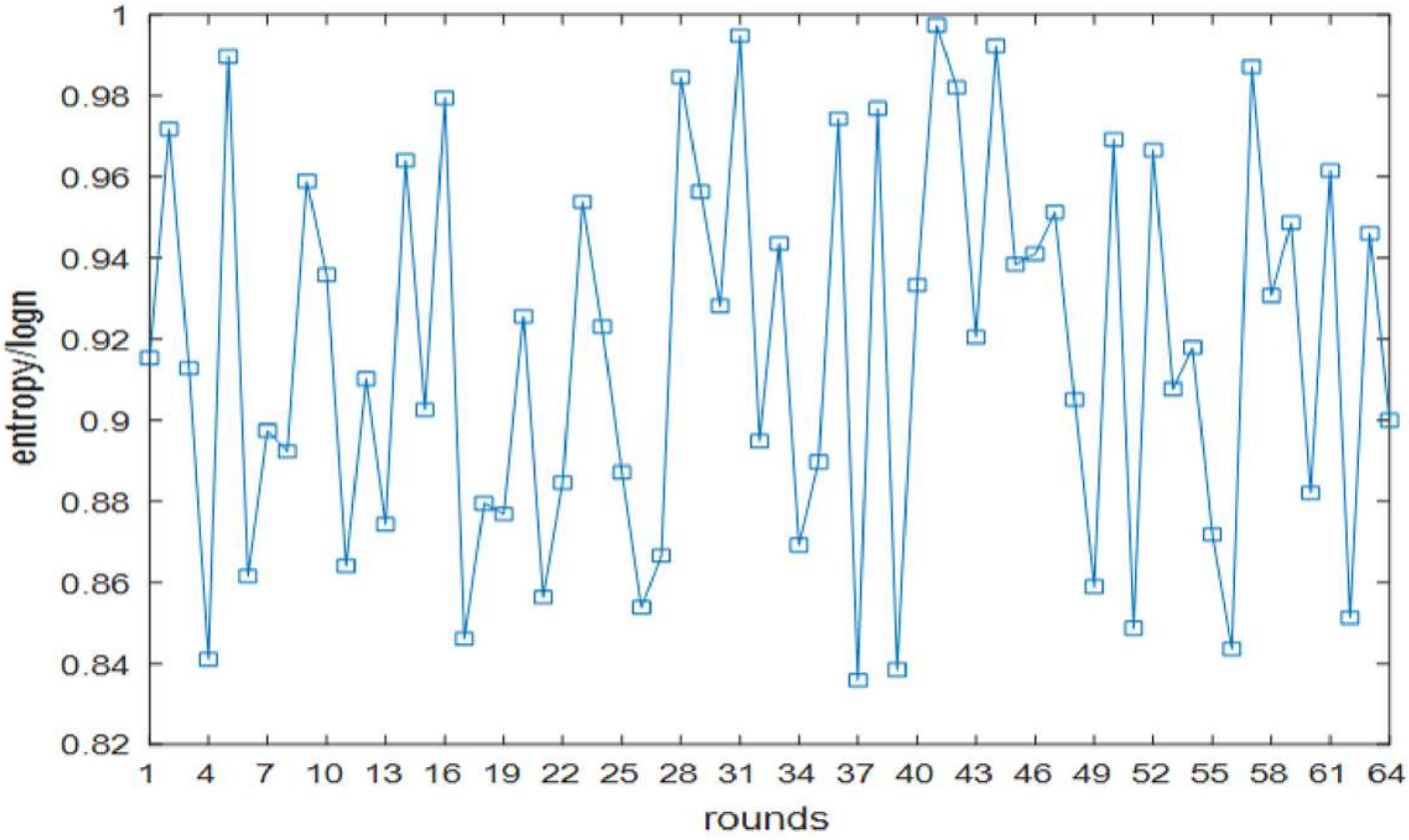

Figure 3

Information from all rounds of the same participant reduces the uncertainty of the correct value