# CPU Resource Double Auction System with an Anonymous Protocol

Takashi Matsumoto Hidenori Kawamura Azuma Ohuchi

Graduate School of Information Science and Technology, Hokkaido University
Nishi 9, Kita 14, Kita-ku, Sapporo, Hokkaido, 060-0814, Japan
{matumo, kawamura, ohuchi}@complex.eng.hokudai.ac.jp

## Abstract

CPU resource of a computer has a case of using all the power and a slight amount of the power, according to time and circumstances. A company wants to buy CPU resource when large-scale processing or processing of emergency is performed, and wants to sell CPU resource when it uses a slight amount of the power. The way of marketing an electronic auction is performed actively. In a general way of auction, it has problem that the auctioneer finds out identity of bids. In case an auction is performed among companies, it can not make use of the auction with a sense of security unless such problem is solved. Since, if a company bids, a trend of the company leaks out as a company secret from the bid price whether it goes through or not. Moreover, if a company finds out that the trading partner is rival company, there is possibility of adverse effect to the auction. In this paper, we describe a set of protocols of CPU resource electronic double auction system among companies for protect identity of bid from other companies and the auctioneer by using Secret Sharing Scheme, public key encryption, and particular method for sending data.
*keywords:resource, auction, Secret Sharing Scheme*

## 1 Introduction

CPU resource of a computer has a case of using all the power and a slight amount of the power, according to time and circumstances. Thus research on utilization of idle CPU resource is increasing in recent years, suchlike grid computing [1].

As a general trend, company has large-scale CPU resource and there are often two distinguishing situations. One is a case of using all the power when large-scale processing or processing of emergency is performed, in this instance the company wants to buy CPU resource from other companies at a low price to speed up processing. The other is a case of using a slight amount of the power, in this instance the company wants to sell idle CPU resource for profit.

In the way of marketing, an auction is the best mechanism for price setting since a product of the auction can be sold at a price determined by interactions in the auction. Moreover, the Internet is the most suitable for carrying out a real time auction since participants can bid anytime regardless of a particular place. Therefore, at present an electronic auction spread. However, an auction has problem of leaking of personal information from bid history or a corrupt auctioneer.

Especially in case trading among companies, it is necessary to conceal identity of a bid for protecting an intellectual property. Since a company must not know worth of CPU resource needlessly. Moreover, it is necessary to conceal trading partner too. Since if it turns out that a trading partner is a rival company, there is possibility of adverse effect to the auction. On the other hand, buying and selling prices are published to all participants since trading are made easy to do.

Kikuchi et al. [2], propose anonymous protocols based on a multiparty secret computation protocol [3]. This auction protocol is based on that identity of seller is known by the auctioneer, and bid price distribution is concealed to the auctioneer and all participants. In double auction, both seller's identity and buyer's identity should be concealed, and bid price distribution is published to all participants. Therefore, this protocol is not able to use double auction system.

In this paper, we describe a set of protocols of CPU resource electronic double auction system among companies for performing protected identity of bid. An identity means the thing of what can be specified a participant, such as IP address, account which was assigned by the auctioneer and so on, in paper.

In our system, there are four features.
First, the system conceals an identity of bid from the auctioneer and all participants of the auction. Second, the system publishes selling and buying price distribution to all participants. Third, the system makes known an identity of participant whose trading was decided to only the auctioneer. Fourth, the system conceals trading partner from a participant whose trading was decided.

For realizing these terms, the following things are required.
· A bid data, which is sent when a participant bid,

has the feature that the bid-price is found out and the identity can not be found out. Moreover when trading goes, only the auctioneer finds out the identity.
· It is necessary to change a method of sending bid data, since by using a usual auction method an identity of the bidder founds out from IP address.
· It is necessary to work out the way of processing using the bought CPU resource.

These tasks are realized by using Secret Sharing Scheme (SSS), public key encryption, and particular method for sending data. At the following section, we describe details of the auction-protocol.

## 2 Proposed Protocol

### 2.1 Auction Style

We consider an electronic double auction formed by the auctioneer and participants registered by the auctioneer.

A participant can bid a selling and buying price and cancel a previous bid any time one likes. A participant sends these orders to the auctioneer as a bid. The auctioneer publishes selling and buying price distribution obtained from these bids to all participants, and selects pair of bid to trade.

In case a trading goes through, only the auctioneer can know identity of the pair of bids, and a participant can know his bid were decided except identity of his trading partner.

In order to conceal a trading partner, the following procedure is done. A participant which bought CPU resource from other participant hands over a process to the auctioneer, and a seller participant receive the process from the auctioneer and return the result to the buyer participant through the auctioneer.

In this auction, volume of CPU resource is defined as $B_i$ which is possible number of processing which was decided beforehand in a unit of time. $B_i$ is assigned interger value.

### 2.2 Bid data

A selling or buying bid data is sent to the auctioneer. If the bid data includes identity of the bidder, the auctioneer finds out it. Therefore, it is necessary to divide the bid data into a price-data, denoted by $p\text{-}data_i$, including selling or buying price from an identity-data, denoted by $i\text{-}data_i$ including account, denoted by $ac_i$, which was assigned by the auctioneer. A $p\text{-}data_i$ is sent to the auctioneer ($i \in N$:$N$ is a set of participants). The auctioneer selects trading partners from $p\text{-}data_i$. But an $i\text{-}data_i$ can not afford to be sent to the auctioneer, since auctioneer finds out identity of bid. Therefore, an $i\text{-}data_i$ is kept by participant.

If a bidder own self $i\text{-}data_i$, there is fear, such as a participant who is not bidding the selected bid insists on his bid, and a participant who bided the selected bid erase the $i\text{-}data_i$ for misbehave. Therefore, an $i\text{-}data_i$ is kept by all participants. But in this way, they can see $i\text{-}data_i$ of other participant. Though a bidder encrypts a $i\text{-}data_i$ with a public key of the auctioneer, a participant can see $i\text{-}data_i$ of others by at most one participant cooperates with the auctioneer. Therefore, a bidder encodes the $ac_i$ into multiple distributed codes by SSS.

### 2.3 $(k, n)$ threshold SSS

$(k, n)$threshold SSS make the number of $n$ distributed data, denoted by $w_j (1 \leq j \leq n)$, from secret-data [4]. It has a feature that if the number of $k$ or more of $w_j$ are collected the secret-data can restore, but in case less than the number of $k$ it can not restore even partial information of the secret-data.

A bidder makes the number of $n$ $i\text{-}data_i$s, denoted by $W_{ij}$, including one of $w_{ij}$ which is distributed from $ac_i$, and one of them own himself and remainder sends to other participants.

Figure 1A shows destination of $p\text{-}data_i$ and $W_{ij}$.

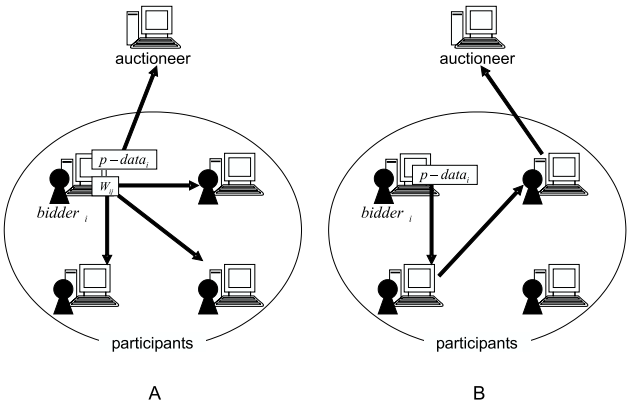


Figure 1: A:Destination of $p\text{-}data_i$ and $W_{ij}$. B:Method for sending data

It is impossible that restore variable $ac_i$ of other participant unless the number of $k$ or more participants cooperate and misbehave by using this method.

Figure 2 shows image of this method.

This algorithm is shown below. A bidder obtains the $j$-th distributed data ($w_{ij}$), by evaluating a $k-1$ polynomials of the form

$$f(x) = a + r_1 x + r_2 x + ... + r_{k-1} x^{k-1} \ (mod\, p)$$

at $x = j$ :

$$w_{ij} = f(j)$$

where $p$ is a large prime number greater than any of the coefficients and is made available to all participants

| sign | type | explanation |
|---|---|---|
| $ac_i$ | integer value of optional digit | identity of a participant which was assigned by the auctioneer |
| $B_i$ | integer value | possible number of processing which was decided beforehand |
| $price_i$ | integer value | selling or buying bid price |
| $M1_i$ | string | result from SHA algorithm of a bid time and $ac_i$ |
| $M2_i$ | string | result from SHA algorithm of $M1_i$ |
| $p\text{-}data_i$ | $\{M1_i, B_i, price_i\}$ | be sent to the auctioneer |
| $w_{ij}$ | integer value of | destributed data of $ac_i$ by using SSS |
| $W_{ij}$ | $\{M2_i, w_{ij}\}$ | be sent to other participants |

Table 1: Contents of data

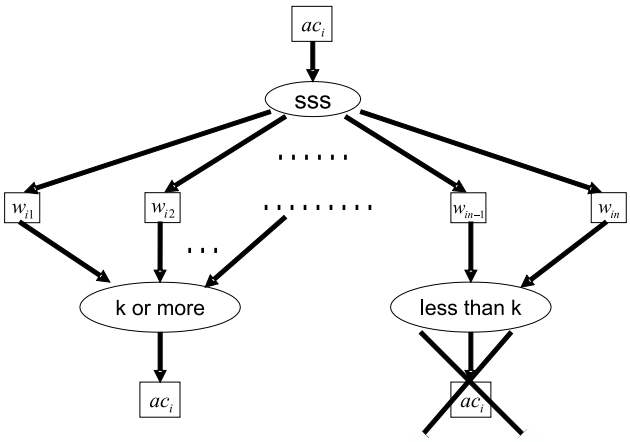


Figure 2: image of using SSS

and the auctioneer, and the coefficient $a$ is account of the bidder while other coefficients $r_1, r_2, ..., r_{k-1}$ are all randomly chosen. $W_{ij}$ includes one of these $w_{ij}$.

When a trading goes through and the auctioneer collects the number of $k$ or more of $W_{ij}$s, it can reconstruct the original polynomial by solving a set of linear equations over a finite field $GF(p)$. Assume that the auctioneer collects the number of $k$ $w_{ij}$s, which is $w_{i1}, w_{i2}, \cdots, w_{ik}$, from the number of $k$ $W_{ij}$s. The original polynomial $f(x)$ can be restored by Lagrange interpolation.

$$f(x) = \sum_{i=1}^{k} (w_i \cdot \prod_{j=1, j\neq i}^{k} \frac{x-j}{i-j}) \, (mod\, p)$$

The variable $ac_i$ can be restored by calculating $f(0)$.

## 2.4 Marks

When the auctioneer collects $W_{ij}$, a mark which associates a $p\text{-}data_i$ with $W_{ij}$ is necessary. The auctioneer selects trading partners from $p\text{-}data_i$ and when pair of bids are selected, and collect the $W_{ij}$ based on this mark.

On the other hand a participant cancels a bid, a mark which associates a cancel order with bid is necessary too.

If these marks are equal, a participant can cancel a bid of other participant since participant has a mark of others $W_{ij}$. Therefore, these two makes have to different things. Moreover, it is necessary to be connected with two marks.

These two marks must not overlap with it of other participants. Since, if same marks exist in database of the auctioneer, the marks can not be recognized. Therefore, these two marks are assigned a value of one-way function.

This algorithm is shown below. First, a bidder calculates the value, denoted by $M1_i$, from SHA algorithm, which is one-way function, of a present time and his account. Next, bidder calculates the value, denoted by $M2_i$, from SHA algorithm of the $M1_i$. $M1_i$ and $M2_i$ are assigned by string. $M1_i$ is attached to $p\text{-}data_i$ and $M2_i$ is attached to $W_{ij}$. In case cancel a bid, it is necessary to $M1_i$. A participant can not cancel bid of other participant by using this method, since it is very difficult to calculate $M2_i$ from $M1_i$. When a trading goes through, the auctioneer collects $W_{ij}$ based on a value ($M2_i$) from SHA algorithm of the $M1_i$ which is attached $p\text{-}data_i$.

Table 1 shows compilation of these data.

## 2.5 Method for sending data

When a participant sends $p\text{-}data_i$ to the auctioneer, the data is sent to the auctioneer not directly but through several participants selected at random. Since, if the data is sent to the auctioneer directly like Figure 1A, the auctioneer finds out the identity of the sender.

If a number of roam participants is decided, the original sender is found out from the number. Therefore, the number is decided from probable. Moreover time limit of roam participants is set, since it has possibility that the $p\text{-}data_i$ is hard to be sent to the auctioneer.

The algorithm is shown below. First, a bidder

chooses integer number, denoted by $NUM_i$, from 1 to 10, and set a limit time. Next, a bidder sends $p\text{-}data_i$ to a participant selected at random. Participants who receive the $p\text{-}data_i$ check the limit time and $NUM_i$. In case run past the limit time or $NUM_i$ equal to 0, the participant sends the $p\text{-}data_i$ to the auctioneer; the other case, the participant subtracts 1 or adds 1 from $NUM_i$, leaves it, or is set to 0 by restrictive probability, and sends the price-data to other participant selected at random. This operation is repeated until the $p\text{-}data_i$ is sent to the auctioneer.

But using this method, a participant can see $p\text{-}data_i$ of others. Therefore, bidder encrypts a $p\text{-}data_i$ with a public key of the auctioneer.

Figure 1B shows an example of $p\text{-}data_i$'s path.

In case of sending $W_{ij}$, it is in the same way that sending $p\text{-}data_i$, since it has same problem. Therefore, $W_{ij}$ includes a destination of sending. Moreover, a bidder encrypts a $W_{ij}$ with a public key of a participant of destination of sending, since a participant who receives $k$ or more of $W_{ij}$ can restore the account.

# 3 Procedure

## 3.1 Selling or Buying Bid

When a participant bids selling or buying bid, the same procedure is performed. Here is a procedure of the algorithm.

Step 1: A participant makes $M1_i$ and $M2_i$, to use method of described at preceding section.

Step 2: A participant makes $p\text{-}data_i$ include $M1_i$, $B_i$, and $price_i$.

Step 3: A participant encrypts the $p\text{-}data_i$ with a public key of the auctioneer, and attach $NUM_i$ and time limit.

Step 4: A participant sends the encrypted data to the auctioneer, to use method of described at preceding section.

Step 5: A participant make $w_{ij}$ from $ac_i$, to use method of described at preceding section.

Step 6: A participant makes $W_{ij}$ include $M2_i$ and one of $w_{ij}$.

Step 7: A participant encrypts $W_{ij}$ with a public key of a participant of destination of sending, and attach $NUM_i$ and time limit.

Step 8: A participant sends the encrypted data to a participant of destination, to use method of described at preceding section.

## 3.2 Cancel a previous Bid

When a participant bids cancel bid, the procedure is equal to Step 1 to Step 4 of selling or buying bid. In case a participant cancels bid, he uses $M1_i$ and $M2_i$ which restored at bid the selling or buying bid and the value of $B_i$ and $price_i$ is set to 0.

## 3.3 Auctioneer

Role of the auctioneer in auction is publishes price distribution which be sent as a $p\text{-}data_i$, selects trading partners, collects pair of $W_{ij}$ and restores a variable $ac_i$ of participant whom dealings determined, and relays process between participants. Here is a procedure of collect pair of $W_{ij}$ and restore a variable $ac_i$.

Step 1: The auctioneer selects trading partners from $p\text{-}data_i$, and calculates $M2_i$ from SHA algorithm of $M1_i$ of the $p\text{-}data_i$.

Step 2: The auctioneer collects $W_{ij}$ of the $M2_i$ from all participants, and order them to delete the $W_{ij}$.

Step 3: The auctioneer restores a variable $ac_i$ from the $W_{ij}$, to use method of described at preceding section.

# 4 Conclusion

We presented protocol of CPU resource electronic double auction system among companies. Using this proposed protocol, identity of bid will not become clear to the auctioneer and all participants unless $k$, that is threshold, or more participants cooperate and misbehave. Moreover, only selling and buying price distribution is published to all participants and the auctioneer.

If the auctioneer collects $W_{ij}$ unjustly, a bidder notices this misbehave since the bidder owns one of his $W_{ij}$. Therefore, the auctioneer who has the authority to collect $W_{ij}$ can not misbehave either.

It should be noted that in a general protocol of electronic double auction, auctioneer can find out identity of all bids. A construction of a system using the proposed protocol will be studied in future work.

# References


[1] William E. Johnston et al."Grids as Production Computing Environments :The Engineering Aspects of NASA's Information Power Grid", *Proceedings of 8th IEEE Symposium on High Performance Distributed Computing*, IEEE Press, 1999.

[2] H. Kikuchi et al. "Multi-round Anonymous Auction Protocols", *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, June, pp. 62-69, 1998.

[3] D. Chaum et al."Multi-party unconditionally secure protocols", *Proceedings of ACM STOC '88*, pp. 11-19, 1988.

[4] A. Shamir. "How to share a secret", *Communication of the ACM*, Vol. 22, No.11, pp. 612-613, 1979.