An anonymous auction protocol with a single non-trusted center using binary trees

Kazumasa OMOTE† and Atsuko MIYAJI†

School of Information Science
Japan Advanced Institute of Science and Technology,
Asahidai 1-1, Tatsunokuchi, Nomi, Ishikawa, 923-1292 JAPAN
E-mail: {omote, miyaji}@jaist.ac.jp

Abstract. Some works about an electronic auction protocol have been proposed[2, 3, 4, 5, 6, 8, 11, 12]. An electronic auction protocol should satisfy the following seven properties: (a)Fair of bidders; (b)Security of bids; (c)Anonymity; (d)Validity of winning bids; (e)Non-repudiation; (f)Robustness; and (g)Efficient bidding points. As for anonymity, previous protocols assume some entities like a dealer or plural centers to be trusted. In this paper, anonymity is realized without a trusted center, maintaining both computational and round complexity low. Furthermore, we represent a bid efficiently by using binary trees: for 2^k bidding points, the size of the representation of bids is just k. Previous works investigating a *sealed-bid auction* aim at "*efficiency*" but not "*entertainment*" seen in *English auction*[2, 4, 5, 6, 11, 12]. We introduce a new idea of entertainment to the opening phase by decreasing winner candidates little by little. Our protocol has the following three main features in addition to the above seven properties: *perfect anonymity(a single non-trusted center)*, *efficient bidding points* and *entertainment*.

keywords anonymity, sealed-bid auction, bidding points, entertainment, one-way function

1 Introduction

Auction is a price-decision system based on a market principle, but not a fixed price. An auction price would reflect a market price more clearly than a fixed price since it is decided by bidders. There are many different types of auction. An *English auction* is the most familiar type. In an English auction, each bidder offers the higher price for goods one by one, and finally a bidder who offers the highest price gets the goods. Each bidder participates in the price-decision process and enjoy it. So an English auction has a feature of *entertainment* as well as a price-decision system. A *sealed-bid auction* is another type, in which each bidder secretly submit a bid to a center only once. Therefore a sealed-bid auction decides the price more efficiently than an English auction. However, all bidders cannot enjoy the price-decision process. A sealed-bid auction would not have a feature of entertainment. In real(i.e. non-electronic) auction, both types are

held and desired. On the other hand, many electronic auction protocols realize a sealed-bid auction[2, 4, 5, 6, 11, 12]. We note that all electronic auction aims at efficiency but not a feature of entertainment.

There are mainly three entities in an auction, a center($\mathcal{C}$), a vendor($\mathcal{V}$) and a bidder($\mathcal{B}$). This basic component is also used in an electronic auction. Each role is as follows:

- **Center**($\mathcal{C}$)**:** This includes an auctioneer. A center sponsors several auctions.
- **Vendor**($\mathcal{V}$)**:** Vendor wants to sell her/his goods and is registered to a center.
- **Bidder**($\mathcal{B}$)**:** Bidder wants to buy goods and is registered to a center.

$\mathcal{V}$ only requests an auction to $\mathcal{C}$ and communicates with neither $\mathcal{C}$ nor $\mathcal{B}$ while an auction is held. An auction process is conducted between $\mathcal{C}$ and $\mathcal{B}$. The following are seven properties that are required in an electronic auction protocol:

(a) **Fair of bidders:** all bidders can look a proper polling on Internet.
(b) **Security of bids:** nobody can forge(falsify) and tap a bid.
(c) **Anonymity:** nobody know the correspondence of a bidder to a bid even after the opening phase. Note that, in electronic auction, this does not mean the secrecy of loosing bids. Anonymity that dose not reveal which bidder except for a winner has bid at what bid can be realized even if some loosing bids are revealed.
(d) **Validity of winning bids:** a protocol can prove that a winning bid is the highest or the lowest values of all bids.
(e) **Non-repudiation:** a winner cannot deny that he/she submitted the winning bid after the bid is opened.
(f) **Robustness:** even if a bidder sends an invalid bid, the auction process is unaffected.
(g) **Efficient bidding points:** if the bidding points are set up discretely, many bidding points are desirable.

In addition to the above seven properties, a sealed-bid auction requires the following property.

(h) **Secrecy of loosing bids:** a protocol keeps loosing bids secret.

Apparently the secrecy of loosing bids is not required in an English auction since all loosing bids are revealed. Therefore the necessity of secrecy of loosing bids depends on targeting what electronic auction. As we will describe below, we aim at a sealed-bid auction with a feature of an English auction. So our protocol reveals only part of distribution of bids but not reveal loosing bids directly.

Various works about electronic auction have been proposed [2, 3, 4, 5, 6, 8, 11, 12]. In [8], the timing is considered when each bidder sends a bid in real-time electronic auction on Internet. A sealed-bid auction protocol is investigated in [2, 4, 5, 6, 11, 12] and a *second-price auction* protocol is discussed in [3]. A second-price auction is a kind of sealed-bid auction: a bidder who offers the highest price gets goods in the second price. For anonymity, a bid[2, 3, 4] or the

opening function[11] is distributed among centers by using the secret sharing technique[13]. In this technique, however, anonymity on the correspondence of a bidder to a bid should leak out by a dealer[2] or a collusion of centers forming a quorum[3, 4, 11]. On the other hand, the scheme[6] cannot satisfy the anonymity for the center, in which the secret sharing technique is not used. To sum up, the previous protocols assume that some entities like a dealer or centers to be trusted. Usually plural centers require more communication cost[2, 3, 4] or more computation amount[11]. On the other hand, [5, 12] realize anonymity without a trusted center, however unfortunately both computational and round complexity to bidders are rather high in the opening phase. [5] uses not a public key cryptosystem but a one-way hash function by introducing the way of "PayWord"[10], which exceedingly decrease the computational complexity. Although such a technique is used, high round complexity to bidders is required for anonymity without a trusted center. In this paper, anonymity on the correspondence of a bidder to a bid is realized without a trusted center, maintaining both computational and round complexity low. In a sense our protocol realizes "perfect anonymity", and also realizes "non-trusted center".

The bidding points are set up discretely in advance in order to realize an anonymity[3, 4, 5, 11, 12]. Therefore the more bidding points are set up, the less probability of tie decreases. In [4], the size of representation of bids directly depends on the number of bidding points: for k bidding points, the size of the representation of bids is just k. Therefore the more bidding points are set up, the more communication amount is required in the bidding phase. Although the bidding points are expressed rather efficiently by logarithm expression[3], both protocols[3, 4] can handle neither tie bids nor invalid bids well: they cannot specify the winners or how many winners there are if the same winning bids or invalid bids are submitted. On the other hand, in [11] a bid is expressed efficiently as an encryption of a known message, which does not depend on the number of bidding points. Therefore it improves the representation of bids. However, unfortunately it costs much computation time in the opening phase: it repeats n times decryption of ElGamal or RSA cryptosystems until the winning bids are decided, where n is the number of bidders. Apparently it is not suited for handling many bidders. In this paper, a bid is represented efficiently by using binary trees: for 2^k bidding points, the size of the representation of bids is just k. Furthermore, the computational and round complexity in the opening phase depends on only (probabilisticly) k, but not the number of bidders. Our protocol can well handle both tie bids and many bidders, and also represents a bid efficiently for many bidding points.

Up to the present, all auction protocols[2, 3, 4, 5, 6, 8, 11, 12] aim at realizing sealed-bid auction faithfully, whose concern is "anonymity" and "efficiency". Entertainment seen in a real English auction has not been discussed before. In this paper, we introduce a new idea of entertainment to the opening phase by decreasing winner candidates little by little. Our price-decision process looks like a winner-decision process in lottery tickets. Note that the computational and round complexity in the opening phase is negligible low, which depends on

only (probabilisticly) k for 2^k bidding points, but not on the number of bidders.

Our electronic auction protocol satisfies the above seven properties. Main features in our protocol is as follows:

- **Perfect anonymity with low computational and low round complexity (a single non-trusted center):** Perfect anonymity means that nobody(including a center) can identify a bidder for her/his bid except for a winning bid even after the opening phase. Our protocol realizes perfect anonymity with both low computational and low round complexity.
- **Efficient bidding points:** a bid is represented efficiently by using binary trees: for 2^k bidding points, the size of the representation of bids is just k.
- **Entertainment:** Entertainment means that many bidders can enjoy the opening phase by decreasing winner candidates little by little.

This paper is organized as follows. Section 2 summarizes as a previous work. Section 3 explains our basic model and presents two practical schemes, one based on DLP and the other based on a one-way hash function. Section 4 investigates attacks against our scheme. Section 5 discusses the properties of our protocol. Section 6 presents performance of our protocol.

2 Previous Work

In this section, we summarize the outline of [4] and discuss the weaknesses.

2.1 Outline

First $\mathcal{C}$ sets L bidding points $\{v_1, \cdots, v_t, \cdots, v_L\}$ and L encryption function $\{E_1 \cdots, E_t \cdots, E_L\}$ according to each bidding point. $\mathcal{C}$ keeps each inverse function $\{E_t^{-1}\}$. A winner who bids the highest value gets goods in the highest value. We describe how $\mathcal{B}_i$ with an identity information ID_i places a bid v_{b_i}. The bid vector $M_i(t)$ for $\mathcal{B}_i$ is as follows:

$$M_i(t) = \begin{cases} E_t(ID_i) & if\ b_i \leq t, \\ 0 & otherwise. \end{cases}$$

We explain how to find the highest bid from the bid vectors. Given bid-vectors of all bidders, each element in the same bidding point are added to sum-vector $M(t)$:

$$M(t) = \sum_i M_i(t) \qquad (1 \leq t \leq L). \tag{1}$$

If $M(t)$ is zero, it means that nobody bids v_t. The winning bid v_t is given by the first t that $M(t)$ is non-zero. If only one bidder bids v_t(a winning bid), he/she is identified by ID_i using the inverse function E_t^{-1}.

This protocol uses secret sharing technique[13] since $\mathcal{C}$ can know the correspondence of a bidder to a bid from $M_i(t)$. Each bid vector $M_i(t)$ is distributed among centers in order to keep all bids secret against centers.

2.2 Weaknesses

There are four weaknesses in [4].

- Anonymity on the correspondence of a bidder to a bid should leak out by a collusion of centers forming a quorum.
- This protocol can handle neither tie bids nor invalid bids well: they cannot specify the winners or how many winners there are, if the same winning bids or faulty bids are submitted.
- The size of representation of bidding points directly depends on the number of bidding points: for k bidding points the size of the representation of bids is just k.
- A winner is decided as soon as sum-vector M is computed. Therefore any bidders cannot enjoy the opening phase.

3 Our Protocol

We propose an auction protocol which satisfies a perfect anonymity on the correspondence of a bidder to a bid except for a winning bid even after the opening phase, efficient bid representation by using binary trees, and a feature of entertainment in the opening phase. For simplicity, we assume the winners to be the one who bids the highest value among a set of bidding points.

3.1 Explanation of Notations

Notations are defined as follows:

n	: number of bidders
k	: number of bid class
L	: number of bidding points $(L = 2^k)$
i	: an index for $\mathcal{B}$ $(i = 1, \cdots, n)$
r_i, R_i	: a random number for $\mathcal{B}_i$
x_i	: a secret key for $\mathcal{B}_i$
y_i	: a public key for $\mathcal{B}_i$
$\mathbf{M}_i$	: a bid vector for $\mathcal{B}_i$
$f(\cdot)$	: a one-way function (e.g. DLP, a hash function)

3.2 Preliminary

- **Initialization:** $\mathcal{C}$ sets up a one-way function f and publishes f to all $\mathcal{B}$.
- **Requesting by vendor:** $\mathcal{V}$ requests an auction to $\mathcal{C}$ to sell her/his goods.
- **Entry of bidders:** Before starting an auction, bidders which want to buy goods execute the following procedure: first make a pair of secret key x_i and public key y_i, send y_i to $\mathcal{C}$ and get its certificate by a center.
- **Setting up of bidding points:** $\mathcal{C}$ sets up $L = 2^k$ bidding points for goods requested by L.

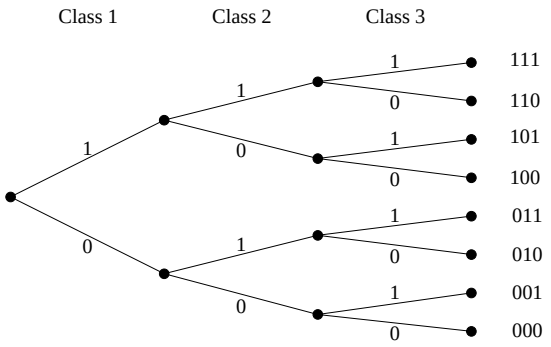

Fig. 1. Example of Bidding Points

3.3 Bidding Points

A binary number denotes the value of a bidding point. For example, we see that eight bidding points are given by three classes in Figure 1. Generally, there are $2^k (= L)$ bidding points for k classes. Note that a bid is represented by a bid vector $\mathbf{M}_i$, whose size depends on only k. As a result, it is possible to handle many bidding points.

In our protocol, bidding points have two properties as follows:

1. In a representation of a bid, a binary number **0** or **1** expresses whether a bid opens the next class or not.
2. A binary expression can set up more bidding points. This can reduce the probability of tie.

3.4 Bidding Phase

A bid sent by $\mathcal{B}_i$ to $\mathcal{C}$ is represented by a bid vector $\mathbf{M}_i$. The format of $\mathbf{M}_i$ is defined as follows:

$$\mathbf{M}_i = [class\ 1, \quad class\ 2, \quad \cdots, \quad class\ k, \quad ID_i].$$

The bid vector $\mathbf{M}_i$ consists of the value expressing **0** or **1** in each class and the identification information of $\mathcal{B}_i$ in the last row. This ID_i cannot be opened unless $\mathcal{B}_i$ is a winner candidate. Therefore anonymity even for $\mathcal{C}$ is satisfied. $\mathbf{M}_i$ is opened from $class\ 1$ to ID_i one by one. By using ID_i, we can confirm who places a highest bids. We explain how $\mathcal{B}_i$ places a bid. For simplicity, $\mathcal{B}_i$ places a bid $v_{b_i} = (\mathbf{1} \cdots \mathbf{1} \overset{t}{\check{\mathbf{0}}}\ \mathbf{1} \cdots \mathbf{11}\ \overset{k-1}{\hat{\mathbf{0}}\mathbf{1}})$ that t-th and $(k-1)$-th bits are **0**. Then bid vector $\mathbf{M}_i$ is as follows:

$$\mathbf{M}_i = \Big[f^k(r_i) + f^{k-1}(r_i),\ \cdots,\ f^{k-t+1}(r_i) + R_{i,k-t},\ f^{k-t}(r_i) + f^{k-t-1}(r_i),\ \cdots,$$
$$f^2(r_i) + R_{i,1},\ f(r_i) + r_i,\ r_i + x_i\Big]$$

Here we denote s-th row of $\mathbf{M}_i$ by $M_{i,s}$ $(1 \leq s \leq k+1)$.

Step 1. $\mathcal{B}_i$ generates a random number r_i and computes $f(r_i), \cdots, f^k(r_i)$ by using a one way function f and r_i.
Step 2. $\mathcal{B}_i$ constructs a bid vector $\mathbf{M}_i$ corresponding to v_{b_i}:

$$(1 \leq s \leq k) \quad M_{i,s} = \begin{cases} f^{k-s+1}(r_i) + f^{k-s}(r_i) & (\text{if } s\text{-th of } v_{b_i} = 1) \\ f^{k-s+1}(r_i) + R_{i,k-s} & (\text{if } s\text{-th of } v_{b_i} = 0), \end{cases}$$
$$M_{i,k+1} = r_i + x_i,$$

where $R_{i,k-s}$ is a random number and x_i is $\mathcal{B}_i$'s secret key.
Step 3. $\mathcal{B}_i$ has to keep $\{r_i, f(r_i), \cdots, f^k(r_i)\}$ secret, but has to posses only $\{f^k(r_i), f^{k-t}(r_i), f(r_i)\}$ as opening keys.
Step 4. $\mathcal{B}_i$ sends $\mathbf{M}_i$ to $\mathcal{C}$, where $\mathbf{M}_i$ does not need to be encrypted, because $\mathcal{B}_i$ keeps the opening key $f^k(r_i)$ secret to conceal the value of v_{b_i}.

Our bid vector has the following features:

1. Anonymity of the correspondence of a bidder to a bid is satisfied as long as opening keys are kept secret.
2. If one opening key is posted, then each row of $\mathbf{M}_i$ is opened one by one till the row corresponding to "**0**" in a bid. However the row next to "**0**" in a bid is never opened as long as the next opening key is kept secret.
3. Everybody can verify the validity of a bid vector by checking $f^{k-s+1}(r_i) = f(f^{k-s}(r_i))$, both of which are open to everybody.
4. Bid vectors for only bidders who place the highest bid are opened one by one till the last row, in which their secret key is set. Furthermore everybody can confirm that the validity of both the highest bid and winners.

3.5 Opening Phase

This section presents the opening phase in our protocol. First $\mathcal{C}$ opens both each bid vector and each public key for bidders on Internet. Note that nobody gets

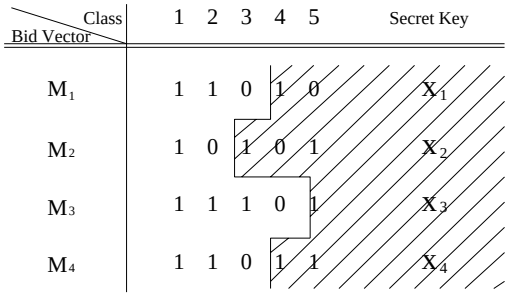

Fig. 2. Opening Example

any information about the correspondence of a bidder to a bid. For simplicity, we assume that a bid v_{b_j} for $\mathcal{B}_j$ in section 3.4 is the highest in this auction.

[**Step 1**] Each $\mathcal{B}_i$ sends the first opening key $f^k(r_i)$ to $\mathcal{C}$. Then each bid vector $\mathbf{M}_i$ is opened till the row corresponding to "**0**", while $f^{k-t+1}(r_i) = f(f^{k-t}(r_i))$ is confirmed. On the other hand, everybody can confirm **0** of t-th row in $\mathbf{M}_i$ by checking $f^{k-t+1}(r_i) \neq f(R_{i,k-t})$.

[**Step 2**] Only bidders $\mathcal{B}_i$ whose bid vectors are opened to the lowest bid send the next opening key (e.g. $\mathbf{M}_3$ in Figure 2). In this case, the next opening key is $f^{k-t}(r_i)$. In the same way as **Step 1**, this procedure continues till the last row. Note that $\mathcal{B}_i$'s secret key is not opened as long as $\mathcal{B}_i$ keeps the final opening key secret.

[**Step 3**] Everybody can confirm that $\mathcal{B}_j$ is the winner of bid vector $\mathbf{M}_j$ by checking a pair of public key y_j and the secret key x_j, which is revealed in the last row.

3.6 Schemes based on a practical one-way function

We will present two examples of one-way function f, one is DLP[1] and the other is hash function.

[**DLP**] $\mathcal{C}$ selects a large prime p and $g \in Z_p^*$ with prime order q. Then a one-way function f is set to $f(r) = g^r \ (mod\ p)$.

[**One-way hash function**] Let $h(\cdot)$ be a cryptographically strong hash function such as SHA-1[7] or MD5[9]. Then a one-way function f is set to $f(r) = h(r)$ in the same way as *"PayWord"*[10].

4 Attacks

This section discusses some attacks against our protocol.

4.1 Invalid bid vector

We investigate that any invalid bid does not have an influence on the auction proceedings. Figure 3 shows two types of invalid bid vector:

1. a bidder does not embed her/his secret key into the last class in a bid vector [Figure 3-$\mathbf{M}_3$],
2. a bidder does not embed the proper opening key into a bid vector [Figure 3-$\mathbf{M}_4$].

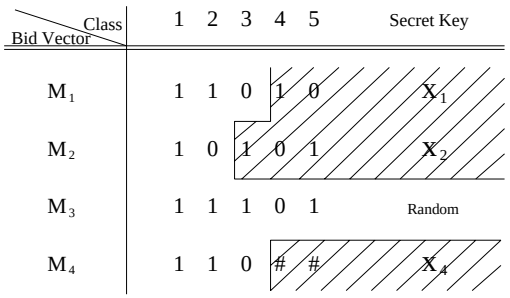

Fig. 3. Examples of invalid bid

First we discuss the case 1. Unless $\mathbf{M}_3$ is a winner candidate, there is no problem: $\mathbf{M}_3$ is simply ignored. If $\mathbf{M}_3$ is a winner candidate like Figure 3, nobody can identify $\mathcal{B}_3$, because $\mathbf{M}_3$ is not embedded $\mathcal{B}_3$'s secret key. In such a case, $\mathbf{M}_3$ is simply removed from this auction as an invalid bid. In our protocol, a bid vector is opened from the highest bid. Therefore the auction proceedings may just continue except for an invalid bid vector.

Next we discuss the case 2. Both $\mathbf{M}_1$ and $\mathbf{M}_4$ are winner candidates except for $\mathbf{M}_3$. However, nobody can open the class 4 of $\mathbf{M}_4$ since $\mathbf{M}_4$ is not embedded into the proper opening key in the class 4. In such a case, $\mathcal{B}_4$ is also ignored. Therefore $\mathbf{M}_1$ is an only winner candidate. The opening phase continues except for $\mathbf{M}_3$ and $\mathbf{M}_4$.

In our protocol, we cannot identify the invalid bidders in the same way as [3, 4, 5, 11, 12]. However our protocol has a feature that each bid vector of bidders is independently opened. Therefore even if an invalid bidder places a bid vector, the auction proceedings will be unaffected: all invalid bids are simply ignored. So our protocol satisfies disturbing resistance, i.e. *robustness*.

4.2 Group Collusion

We investigate group collusion attacks by some bidders: attackers want to get goods in the lowest price available. For simplicity, let $\{I_1, I_2, I_3\}$ be an invalid group. There are three cases of group collusion seen in Figure 4, which expresses a part of binary tree in bids:
Case 1(Figure 4-(a)): there are only plural invalid bidders I_1, I_2 and I_3 in higher trees(Tree 1).
Case 2(Figure 4-(b)): there are only one invalid bidder I_1 in higher trees.
Case 3(Figure 4-(c)): There is no invalid bidder but there are some valid bidders V_1, V_2 and V_3 in higher trees.

In the case 1, attackers can get goods in the lowest bid of I_3 by canceling two bids of I_1 and I_2. However in both case 2 and case 3, it is impossible for attackers to control the winning bid. Furthermore, if an attacker I_1 places the highest bid

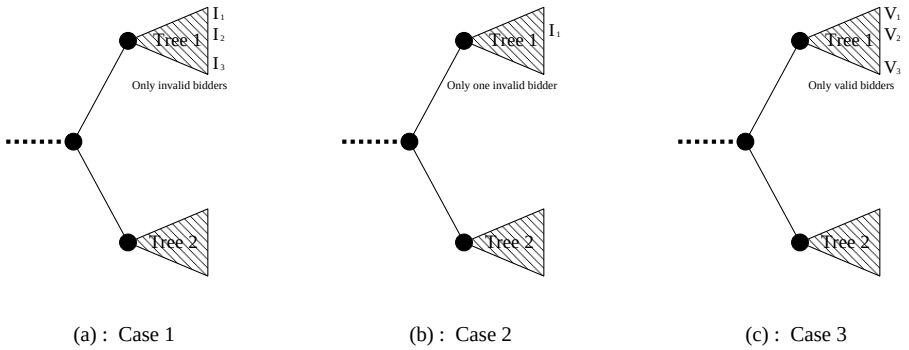

Fig. 4. Group Collusion

of all bid points, then I_1 cannot deny the winning bid after the opening phase. To sum up, attackers can control the winning bid only in the case 1 since attackers cannot get goods in the lower price than that of valid bidders. Therefore such collusion attackers have little influence on the auction proceedings.

$\mathcal{C}$ may solve this group collusion by placing some bids randomly since $\mathcal{C}$ makes it hard for invalid bidders to control a winning bid. Of course $\mathcal{C}$ should place some bids near the winning bid.

5 Properties

Our protocol satisfies the following properties:

- **Fair of bidders** — All bidders can look a proper polling on Internet.
- **Security of bids** — Security of bids means that: 1. Before the opening, a bid cannot be revealed. 2. Any bidder can check whether her/his bid is not forged. In our protocol, each row of a bid vector consists of two random numbers $f(r_i) + r_i$ and $r_i + r'_i$ by using a one-way function f and a random number r_i and r'_i. As for the former, r_i is kept secret as long as $f(r_i)$ is not opened, whose security depends on f. As for the latter, r'_i is chosen randomly, and r_i is kept secret as long as the next row is not opened. Therefore the security also depends on f. The security on attacks of using all row data in a bid vector also depends on f. On the other hand, if a bid is falsified, then the corresponding bidder can easily notice the faulty bid since all bid vectors are opened on Internet.
- **Anonymity** — In our protocol, only a winner's secret key is revealed, which identifies the corresponding bidder. On the other hand, other secret keys are kept secret even after the opening phase. As a result, nobody (including a center) can know the correspondence of a bidder to a bid except for a winner.
- **Validity of winning bids** — Since bid vectors are opened one by one from the higher bid, apparently a winning bid is the highest of all bids. Moreover

Table 1. Performance

	Total communication amount (bit)		Each bidder's computation amount	
	Bidding	Opening	Bidding	Opening
[4]	$1024(2^k-1)mn$	0	$\mathcal{P}\cdot 2^k$	0
DLP	$1024(k+1)n$	$1024\left(2-\frac{1}{2^k}\right)n$	$\mathcal{D}\cdot k$	0
Hash	$160(k+1)n$	$160\left(2-\frac{1}{2^k}\right)n$	$\mathcal{H}\cdot k$	0

the validity of a bid vector is easily checked by a one-way function and secret key.

- **Non-repudiation** — A winner $\mathcal{B}_j$ cannot deny her/his bid since $\mathcal{B}_j$'s secret key is revealed.
- **Robustness** — Our protocol has a feature that each bid is independently opened. Therefore if invalid bids are placed, the auction proceedings will be unaffected: invalid bids are simply ignored.
- **Entertainment** — English auction has an entertainment that it does not only decide a winner but also pleases all participants until the winner is decided. In our protocol, we introduce a feature of entertainment to the opening phase by decreasing winner candidates one by one, which looks like a winner-decision process in lottery tickets. Since we aim at a feature of entertainment, our protocol reveals only part of distribution of bids. However our protocol does not reveal the whole distribution of bids like [2, 6], and what is still better, satisfies anonymity.
- **Tie** — In electronic auction protocol, bidding points are often set discretely[3, 4, 5, 11, 12]. In such a situation, two properties should be required: 1. Winners should be specified even if two or more bidders place the same winning bid. 2. The probability of tie should be reduced by setting many bidding points. As for the former, our protocol can specify the winners in the case of the same winning bids. As for the latter, our protocol can set many bidding points like 2^k, maintaining computational, communicational and round complexity of $\mathcal{B}_i$ or $\mathcal{C}$ low, all which depend on k. Furthermore the probability of tie can be reduced.

6 Performance

In this section, we compare our protocol with [4] from the point of view of communication and computation amount, which are shown in Table 1. Here let the number of bidding points and bidders be 2^k and n, respectively. In [4], plural centers are required, whose number is denoted by m (≥ 2). We assume a one-way function f to be DLP or a 160-bit output one-way hash function, whose output size is denoted by $|f|$. In [4], the communication amount in the bidding phase depends on 2^k and m. On the other hand, in our protocol the communication

amount depends on only k since only a single center is sufficient for anonymity. Therefore the communication amount can be dramatically reduced.

Next we discuss the communication amount in the opening phase. Since we aim at a feature of entertainment, communication between $\mathcal{B}_i$ and $\mathcal{C}$ is required in the opening phase. But we will see in Table 1 that the communication amount in the opening phase is negligible small. For simplicity, we assume that there are $\frac{n}{2^i}$ bidders in each branch of class i on the average, who send an opening key in probability $\frac{1}{2}$. Therefore the communication amount in the opening is at most

$$|f| \left(n + \sum_{i=1}^{k} \frac{n}{2^i} \right) = |f| \left(2 - \frac{1}{2^k} \right) n.$$

Lastly we discuss the computation amount. Let $\mathcal{P}$ be computation amount to compute the distribution information of the secret sharing technique, $\mathcal{D}$ be computation amount to compute a modulus exponent, and $\mathcal{H}$ be computation amount to compute a one-way hash function. In the same discussion as the communication amount, the computation amount of [4] depends on 2^k while that of our protocol depends on only k.

7 Conclusion

We have proposed an anonymous auction protocol with a single non-trusted center. Our protocol realizes the following features:

Perfect anonymity with low computational and low round complexity : Nobody can identify a bidder from her/his bid except for a winning bid even after the opening phase.
Efficient bidding points : For 2^k bidding points, the size of the representation of bids is reduced to just k by using binary trees.
Entertainment : Many bidders can enjoy the opening phase by decreasing winner candidates little by little.
Robustness : Even if a bidder sends an invalid bid vector, the auction process is unaffected.
Application : Our protocol can be easily applied to a power auction, which decides the plural winners.

References

1. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Trans. on Information Theory*, pages 469–472, 1985.
2. M. Franklin and M. Reiter. The design and implementation of a secure auction service. *IEEE Transactions on Software Engineering*, 5:302–312, 1996.
3. M. Harkavy, D. Tyger, and H. Kikuchi. Electronic Auctions with Private Bids. In *Proceedings of the Third USENIX Workshop on Electronic Commerce*, 1998.

4. H. Kikuchi, M. Harkavy, and D. Tyger. Multi-round anonymous auction protocols. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 62–69, 1998.
5. K. Kobayashi and M.Morita. Efficient sealed-bid auction with quantitative competition using one-way functions. *ISEC99-30*, pages 31–37, 1999.
6. M. Kudo. Secure electronic sealed-bid auction protocol with public key cryptography. *IEICE Trans. Fundamentals*, E81-A(1):20–27, 1998.
7. NIST. Secure Hash Standard (SHS). *FIPS Publication 180-1*, April 1995.
8. C-S. Peng, M. Pulido, J. Lin, and M. Blough. The Design of an Internet-based Real Time Auction Systems. In *Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pages 70–78, 1998.
9. R.L.Rivest. The MD5 message-digest algorithm. *Internet Request for Comments*, pages 302–312, April 1992.
10. R.L.Rivest and A.Shamir. PayWord and MicroMint:Two simple micropayment schemes. *To Appear at the RSA '96 Conference*, May 1996.
11. K. Sako. An Auction Protocol Which Hides Bids of Losers. In *Proceedings of PKC2000*, pages 422–432, 2000.
12. K. Sakurai and S. Miyazaki. A Bulletin-board based digital auction scheme with bidding down strategy -towards anonymous electronic bidding without anonymous channels nor trusted centers in Cryptographic Techniques and E-Commerce. In *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce(CryTEC '99)*, 1999.
13. A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

This article was processed using the LaTeX macro package with LLNCS style