Regular Paper

An Anonymous Sealed-bid Auction with a Feature of Entertainment

Kazumasa Omote† and Atsuko Miyaji†

Some works about an electronic *sealed-bid auction* protocol[1),3),5)~10),15),16),18)] have been proposed. An electronic auction scheme should satisfy the following seven properties: (a) Fair of bidders; (b) Bid security; (c) Anonymity; (d) Validity of winning bids; (e) Non-repudiation; (f) Robustness; and (g) Efficient bidding points. Many previous schemes do not realize anonymity for an auction manager. In this paper, we propose a new electronic sealed-bid auction that realizes anonymity for an auction manager, maintaining both computational and round complexity low. We represent a bid efficiently by using binary trees: for 2^k bidding points, the size of the representation of bids is just k. Furthermore, we introduce a new idea of entertainment to the opening phase by decreasing winner candidates little by little. Our notion is very attractive and new since all previous works on a sealed-bid auction aim at "*efficiency*" but not "*entertainment*" seen in *English auction*. The main features of our scheme are: anonymity for a single $\mathcal{AM}$, efficient bidding points and entertainment.

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 enjoys 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 submits a bid to $\mathcal{AM}$ 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 schemes realize a sealed-bid auction[1),3),5)~10),15),16),18)]. We note that all electronic auction aims at efficiency but not a feature of entertainment.

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

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

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

(a) **Fair of bidders:** all bidders can look a proper polling on Internet.
(b) **Bid security:** nobody can forge (falsify) and tap a bid.
(c) **Anonymity:** nobody knows the correspondence of a bidder to a bid even after the opening phase. Note that, in an electronic auction, this does not mean the secrecy of loosing bids. Anonymity 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 she/he submitted the winning bid after the winning 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

† Japan Advanced Institute of Science and Technology

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 English auction. So our scheme reveals only part of distribution of bids but not reveal loosing bids directly.

Various works about an electronic auction have been proposed. The timing when each bidder sends a bid in real-time Internet English auction is considered[12]. Sealed-bid auctions are investigated in some works[1),3),5)~10),15),16),18)] and a *second-price auction* is also discussed[4]. A second-price auction is a kind of sealed-bid auction: a bidder who offers the highest price gets the good in the second price. For anonymity, a bid[3),4),6)] or the opening function[15)] is distributed among $\mathcal{AM}$s by using the secret sharing technique[17]. In this technique, however, anonymity on the correspondence of a bidder to a bid should leak out by a dealer[3),15)] or a collusion of $\mathcal{AM}$s forming a quorum[4),6)]. Usually plural $\mathcal{AM}$s require more communication cost[3),4),6)] or more computation amount[15)]. Although the schemes[5),9)] realize anonymity for $\mathcal{AM}$, all bids are opened after the bidding phase. These schemes do not satisfy secrecy of loosing bids at all. On the other hand, the schemes[7),8),16),18)] do not realize the anonymity for $\mathcal{AM}$. The previous schemes[1),10)] use two kinds of auction servers ($\mathcal{AM}$). However the scheme[1)] does not realize anonymity for one server and discloses a order of all bids for the server. The scheme[10)] is presented in section 2. In this paper, anonymity is realized for a single $\mathcal{AM}$ without directly revealing whole distribution of bids.

Bidding points are usually set up discretely in advance in order to realize secrecy of loosing bids[1),4),6),7),10),15),16),18)]. On the other hand, we use the discrete bidding points in order to realize anonymity for a single $\mathcal{AM}$ like the schemes[5),9)] and not to reveal loosing bids directly.

A one-way hash function instead of a public key cryptosystem is used by introducing the way of "PayWord"[14)], which exceedingly decrease the computational complexity[7),18)]. However, unfortunately the size of representation of bids directly depends on the number of bidding points[6),7),16),18)]: for 2^k bidding points, the size of the representation of bids is just 2^k. Therefore the more bidding points are set up, the more communication or computation amount is required in the bidding or opening phase. Two previous schemes[1),10)] has a fairly efficient opening phase: for 2^k bidding points, the size of the representation of bids is just k.

On the other hand, a bid is efficiently represented as an encryption of a known message[15)], which does not depend on the number of bidding points. Therefore it improves the representation of bids. However 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 the computational and round complexity in the opening phase depends on mainly (probabilistically) k, but not directly on the number of bidders. Our scheme can well handle both tie bids and many bidders, and also represents a bid with the size k for 2^k bidding points.

Up to the present, most auction schemes aim at realizing sealed-bid auction faithfully, whose concern is both "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 for a bidder in the opening phase is negligible low on the average (see Section 6).

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

- **Perfect anonymity with low computational and low round complexity:** Perfect anonymity means that nobody (including $\mathcal{AM}$) can identify a bidder for her/his bid except for a winning bid even after the opening phase. Our scheme 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 a previous scheme. Section 3 explains our basic model and presents two practical schemes, on DLP-based scheme and a one-way-hash-function-based scheme. Section 4 investigates security of our scheme. Section 5 discusses the properties and Section 6 presents performance.

2. Previous Scheme

In this section, we summarize a previous scheme[10] and discuss the weaknesses. This scheme is a sealed-bid auction[☆] that has an efficient opening process similar to our scheme.

2.1 Outline

This scheme has two entities $\mathcal{AI}$ and $\mathcal{AM}$: $\mathcal{AI}$ generates programs for computing a winning bid and $\mathcal{AM}$ is an auction manager as usual. $\mathcal{AI}$ uses a public key encryption. First $\mathcal{AM}$ publishes $L = 2^k$ bidding points and $\mathcal{AI}$'s public key $E_{\mathcal{AI}}$, while $\mathcal{AI}$ publishes $c = g^r (\mathrm{mod}\ p)$ (p is a prime, r is a secret random number and g is a basepoint on which the discrete log problem is hard) and keeps the two kinds of a bidder $\mathcal{B}_i$'s values $m^0_{i,j}, m^1_{i,j}$ ($i \in [1,n], j \in [1,k]$) secret. The values $m^0_{i,j}$ and $m^1_{i,j}$ express the bit 0 and 1, respectively. Each $\mathcal{B}_i$ engages in a 1-out-of-2 proxy oblivious transfer protocol for each bit of her/his bid value M_i. The basic steps is as follows:

(1) $\mathcal{B}_i$ selects her/his secret keys $\{x_{i,j}\}$ and computes $g^{x_{i,j}}$ and $c/g^{x_{i,j}} = g^{r-x_{i,j}}$ ($j \in [1,k]$). $\mathcal{B}_i$ sends both $\{x_{i,j}\}$ and $E_{\mathcal{AI}}(g^{\alpha_{i,j}})$ to $\mathcal{AM}$, where $\alpha_{i,j}$ is either $x_{i,j}$ or $r - x_{i,j}$.

(2) $\mathcal{AM}$ forwards only $E_{\mathcal{AI}}(g^{\alpha_{i,j}})$ to $\mathcal{AI}$, who decrypts $g^{\alpha_{i,j}}$ from $E_{\mathcal{AI}}(g^{\alpha_{i,j}})$.

(3) In return, $\mathcal{AI}$ sends $(g^{\ell_j},\ g^{\alpha_{i,j}\ell_j} \oplus m^0_{i,j},\ (c/g^{\alpha_{i,j}})^{\ell_j} \oplus m^1_{i,j})$ ($j \in [1,k]$) to $\mathcal{AM}$ (ℓ_j is a random number).

(4) $\mathcal{AM}$ can decrypt $m^*_{i,j}$ using $x_{i,j}$ corresponding to $\mathcal{B}_i$. Note that $m^*_{i,j}$ ($j \in [1,k]$) is either $m^0_{i,j}$ or $m^1_{i,j}$. Then $\mathcal{AM}$ inputs $m^*_{i,j}$ ($i \in [1,n], j \in [1,k]$) to a program, which outputs the value M_p corresponding to a winner $\mathcal{B}_p$.

2.2 Weaknesses

There are four weaknesses in the previous scheme.

- Anonymity on the correspondence of a bidder to a bid is not realized if $\mathcal{AI}$ and $\mathcal{AM}$ cooperate.
- If $\mathcal{AM}$ colludes with $\mathcal{AI}$, $\mathcal{AM}$ can get the bid value of all bidders without using a program.
- If $\mathcal{AI}$ colludes with a bidder $\mathcal{B}_i$, $\mathcal{AI}$ can make such a faulty program that $\mathcal{B}_i$ always becomes a winner.
- A winner with her/his winning bid is decided as soon as a program has been conducted. Therefore no bidder can enjoy the opening phase.

3. Our Scheme

We propose an electronic sealed-bid auction scheme which satisfies the perfect anonymity 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. We use the discrete bidding points in order to realize anonymity for a single $\mathcal{AM}$ like the schemes[5),9)] and not to reveal loosing bids directly. Our scheme does not rely on an anonymous channel since any bid is placed anonymously. Our system can be implemented with the public key technology, cryptographic one-way functions and a public bulletin board like Ref. 16). For simplicity, we assume the winners to be the one who places the highest bid among a set of bidding points.

3.1 Explanation of Notations

Notations are defined as follows:

n	:	a number of bidders,
k	:	a number of bits,
L	:	a number of bidding points ($L = 2^k$),
i	:	an index for $\mathcal{B}$ ($i = 1, \cdots, n$),
$r_i, \tilde{r_i}, R_i$	:	a random number for $\mathcal{B}_i$,
x_i	:	a secret key of $\mathcal{B}_i$,
y_i	:	a public key of $\mathcal{B}_i$,
x_C	:	a secret key of $\mathcal{AM}$,
y_C	:	a public key of $\mathcal{AM}$,
$Enc(K, D)$	:	a public key encryption and
$Dec(K, D)$		decryption, which are a probabilistic encryption like ElGamal-encryption[2] ($K : key,\ D : data$),
$\mathbf{M}_i$	:	a bid vector for $\mathcal{B}_i$,
$f(\cdot)$	:	a one-way function (e.g., DLP, a hash function).

[☆] This scheme can also implement the second price sealed-bid auction by changing the program.

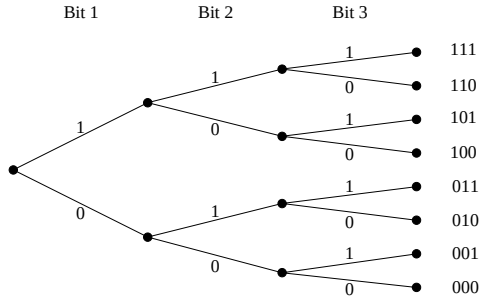


Fig. 1 Example of bidding points.

3.2 Preliminary

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

3.3 Bidding Points

The bidding points are efficiently set up by $\mathcal{AM}$. For example, eight bidding points are given by three bits in **Fig. 1**. Generally, there are 2^k $(= L)$ bidding points for k bits. 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 more bidding points. A binary expression can reduce the probability of bidder's tie of bid since it can set up many bidding points.

3.4 Bid Vector

When $\mathcal{B}_i$ places a bid v_{b_i} (k-bit) to $\mathcal{AM}$, $\mathcal{B}_i$ sends a bid vector $\mathbf{M}_i$. The format of $\mathbf{M}_i$ is defined as follows:

$$\begin{aligned}\mathbf{M}_i &= [\mathrm{bit}_1,\ \cdots,\ \mathrm{bit}_k,\ \mathcal{B}_i\text{'s } ID,\ \mathbf{M}_i\text{'s } ID] \\ &= [M_{i,1}, \cdots, M_{i,k}, M_{i,k+1}, M_{i,k+2}]\,,\end{aligned}$$

$1 \le t \le k$

$$M_{i,t} = \begin{cases} f^{k-t+1}(r_i) \oplus f^{k-t}(r_i) & (\text{if bit}_t = 1) \\ f^{k-t+1}(r_i) \oplus R_{i,k-t} & (\text{otherwise}), \end{cases}$$

$t = k+1$

$$M_{i,k+1} = r_i \oplus x_i,$$

$t = k+2$

$$M_{i,k+2} = Enc(y_C, \tilde{r_i}),$$

where $\oplus$ means the bit-wise exclusive or. Note that a function f satisfies $f^k(r) = f(f^{k-1}(r))$. Here we denote the t-th row of $\mathbf{M}_i$ by $M_{i,t}$ $(1 \le t \le k+2)$.

The bid vector $\mathbf{M}_i$ consists of the values expressing **0** or **1** in each bit. The $\mathcal{B}_i$'s ID and $\mathbf{M}_i$'s ID are embedded in the $(k{+}1)$-th row, and the $(k{+}2)$-th row, respectively. In a representation of a bid, a binary number **1** or **0** expresses whether a bid opens the next bit or not, respectively. The $(k{+}2)$-th row $\mathbf{M}_i$'s ID is used for the purpose of correspondence of a bid vector $\mathbf{M}_i$ to the opening key, and does not reveal the correspondence of $\mathbf{M}_i$ to $\mathcal{B}_i$. The anonymity of $\mathcal{B}_i$ is revealed only by opening the $(k{+}1)$-th row ID_i. ID_i can be opened only if $\mathcal{B}_i$ is a winner candidate. Therefore anonymity except for a winner is satisfied. $\mathbf{M}_i$ is opened from bit 1 to ID_i one by one. By checking ID_i for a winner candidate, we can confirm who places a highest bids.

3.5 Bidding Phase

We explain how $\mathcal{B}_i$ places a bid. For simplicity, $\mathcal{B}_j$ places a bid $v_{b_j} = (\mathbf{1}\cdots\mathbf{1}\overset{t}{\check{\mathbf{0}}}\mathbf{1}\cdots\mathbf{1}\overset{k-1}{\check{\mathbf{0}}}\mathbf{1})$ that both the t-th and the $(k{-}1)$-th bits are **0**. Then bid vector $\mathbf{M}_j$ is as follows:

$$\begin{aligned}\mathbf{M}_j = [&M_{j,1}, \cdots, M_{j,t}, M_{j,t+1}, \cdots, \\ &M_{j,k-1}, M_{j,k}, M_{j,k+1}, M_{i,k+2}] \\ = [&f^k(r_j) \oplus f^{k-1}(r_j), \cdots, f^{k-t+1}(r_j) \oplus \\ &R_{j,k-t},\ f^{k-t}(r_j) \oplus f^{k-t-1}(r_j), \cdots, \\ &f^2(r_j) \oplus R_{j,1},\ f(r_j) \oplus r_j,\ r_j \oplus x_j, \\ &Enc(y_C, \tilde{r_j})]\,,\end{aligned}$$

where $R_{i,k-t}$ is a random number$(R_{i,k-t} \neq f^{k-t}(r_j))$ and x_j is $\mathcal{B}_j$'s secret key.

Step 1: $\mathcal{B}_j$ generates random numbers $R_{j,k-t}, R_{j,1}, r_j$ and $\tilde{r_j}$.

Step 2: $\mathcal{B}_j$ computes $f(r_j), \cdots, f^k(r_j)$ by using a one-way function f and r_j.

Step 3: $\mathcal{B}_j$ encrypts $\tilde{r_j}$ to $Enc(y_C, \tilde{r_j})$ by using $\mathcal{AM}$'s public key y_C.

Step 4: $\mathcal{B}_j$ constructs a bid vector $\mathbf{M}_j$ corresponding to v_{b_j}.

Step 5: $\mathcal{B}_j$ has to keep $\{f(r_j), \cdots, f^k(r_j)\}$ secret, but posses only $\{f^k(r_j), f^{k-t}(r_j), f(r_j)\}$ as opening keys.

Step 6: $\mathcal{B}_j$ sends $\mathbf{M}_j$ and $Enc(y_C, \tilde{r_j})$ to $\mathcal{AM}$, where $\mathbf{M}_j$ does not need to be encrypted, because $\mathcal{B}_j$ keeps the opening key $f^k(r_j)$ secret to conceal the value of v_{b_j}.

Step 7: $\mathcal{AM}$ decrypts $\tilde{r_j}$ from $Enc(y_C, \tilde{r_j})$ by using his secret key x_C, and keep $\tilde{r_j}$ secretly for the purpose of correspondence of $\mathbf{M}_j$ to the

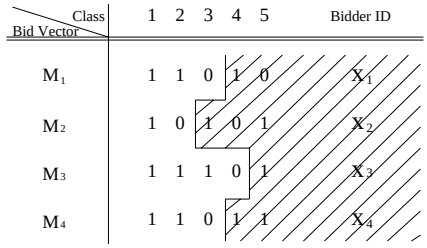


Fig. 2 Opening example.

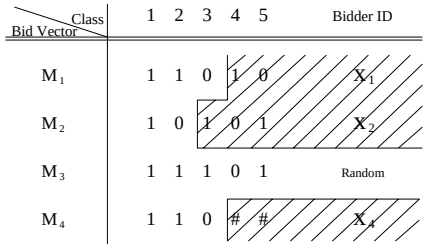


Fig. 3 Examples of invalid bid.

opening key.

Anonymity of the correspondence of a bidder to a bid is satisfied as long as opening keys are kept secret.

3.6 Opening Phase

This section presents the opening phase in our scheme. First $\mathcal{AM}$ publishes both each bid vector $\mathbf{M}_j$ and each public key y_j for bidders on Internet. Note that nobody gets any information about the correspondence of a bid vector to a public key. For simplicity, we assume that a bid v_{b_j} for $\mathcal{B}_j$ is the highest in this auction.

Step 1: $\mathcal{B}_j$ sends the first opening key $f^k(r_j)$ with $Enc(y_C, \tilde{r_j})$ to $\mathcal{AM}$. $\mathcal{AM}$ corresponds $f^k(r_j)$ to $\mathbf{M}_j$ by decrypting $Enc(y_C, \tilde{r_j})$. Then the bid vector $\mathbf{M}_j$ is opened till the t-th row corresponding to "**0**". Everybody can confirm **0** of t-th row in $\mathbf{M}_j$ by checking $f^{k-t+1}(r_j) \neq f(R_{j,k-t})$. As a result, the only values $\{f^k(r_j), f^{k-1}(r_j), \cdots, f^{k-t+1}(r_j)\}$ are opened. Note that the value $f^{k-t}(r_j)$ is not opened.

Step 2: Only bidders $\mathcal{B}_i$ whose bid vectors are opened to the higher bit send the next opening key as winner candidates (e.g., $\mathbf{M}_3$ in **Fig. 2**). $\mathcal{B}_j$, a winner candidate, sends the second opening key $f^{k-t}(r_j)$ with $Enc(y_C, \tilde{r_j})$ to $\mathcal{AM}$. In the same way as **Step 1**, this procedure continues till the last row. Note that $\mathcal{B}_j$'s secret key is not opened as long as $\mathcal{B}_j$ keeps the final opening key r_j 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. Of course, after this auction a winner $\mathcal{B}_j$ has to get another certificate of y'_j by changing x_j into x'_j.

3.7 Schemes Based on a Practical One-way Function

We will present two examples of one-way function f, one is based on DLP[2] and the other is based on a hash function.

DLP: $\mathcal{AM}$ selects a large prime p and $g \in Z_p^*$ with prime order q. Then a one-way function f is set to $f(r) = g^r \ (mod\ p)$. In this case, $f^2(r) = g^{g^r}$.

One-way hash function: Let $h(\cdot)$ be a cryptographically strong hash function such as SHA-1[11] or MD5[13]. Then a one-way function f is set to $f(r) = h(r)$ in the same way as "*PayWord*"[14]. In this case, $f^2(r) = h(h(r))$.

4. Security

This section discusses security of 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:

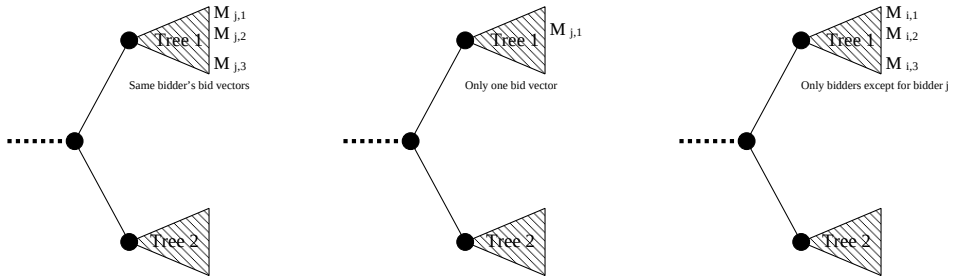
(1) a bidder $\mathcal{B}_i$ does not embed her/his secret key into $\mathcal{B}_i$'s ID bit in a bid vector (Fig. 3-$\mathbf{M}_3$),

(2) a bidder does not embed the proper opening key into a bid vector (Fig. 3-$\mathbf{M}_4$).

First we discuss Case 1. $\mathbf{M}_i$ is $\mathcal{B}_i$'s bid vector. Unless $\mathcal{B}_3$ is a winner candidate, there is no problem: $\mathbf{M}_3$ is simply ignored. If $\mathcal{B}_3$ is a winner candidate like Fig. 3, nobody can identify $\mathcal{B}_3$ because $\mathcal{B}_3$'s secret key is not embedded in $\mathbf{M}_3$. 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 Case 2. Both $\mathcal{B}_1$ and $\mathcal{B}_4$ are winner candidates except for $\mathcal{B}_3$. However, nobody can open the bit 4 of $\mathbf{M}_4$ since $\mathbf{M}_4$ is not embedded into the proper opening key in the 4-th bit. In such a case, $\mathbf{M}_4$ 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 scheme, we cannot identify the invalid bidders in the same way as some works[4),6),7),15),16),18)]. However our scheme 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 sim-



(a) : Case 1 (b) : Case 2 (c) : Case 3

Fig. 4 Bid manipulation.

ply ignored. So our scheme satisfies disturbing resistance, i.e., *robustness*.

4.2 Bid Manipulations

We investigate the multiple bidding by a bidder $\mathcal{B}_j$, who wants to get goods in the lowest price available. For simplicity, let $\{M_{i,1}, M_{i,2}, M_{i,3}\}$ be bid vectors of $\mathcal{B}_i$. There are three cases in bid manipulations seen in **Fig. 4**, which expresses a part of binary tree in bids:

Case 1 (Fig. 4-(a)): there are only $\mathcal{B}_j$'s bid vector $\{M_{j,1}, M_{j,2}$ and $M_{j,3}\}$ in higher trees (Tree 1).

Case 2 (Fig. 4-(b)): there is only one of $\mathcal{B}_j$'s bid vector $M_{j,1}$ in higher trees.

Case 3 (Fig. 4-(c)): there is no $\mathcal{B}_j$'s bid vector but there are other bidder's bid vector $\{M_{i,1}, M_{i,2}$ and $M_{i,3}\}$ in higher trees $(i \neq j)$.

In Case 1, $\mathcal{B}_j$ can get goods in the lowest bid of $M_{j,3}$ by canceling two bids of $M_{j,1}$ and $M_{j,2}$ presented in Ref. 9). But in both Case 2 and Case 3 it is impossible for $\mathcal{B}_j$ to control the winning bid. To sum up, a bidder can control the winning bid only in Case 1. However such bid manipulations have a little influence on the auction proceedings since $\mathcal{B}_j$ cannot necessarily get goods in the lower price than that of $\mathcal{B}_i$ $(i \neq j)$. Furthermore even if $\mathcal{B}_j$ conducts the multiple bidding, this does not affect other bidders.

4.3 Group Collusion

We can treat a group collusion likewise. This is not a serious problem as we have described in Section 4.2.

5. Properties

Our scheme satisfies the following properties:

- **Fair of bidders**—All bidders can look a proper polling on Internet.
- **Bid security**—Bid security 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 $f(r_i) \oplus r_i$ and $r_i \oplus r'_i$ 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, the bidder $\mathcal{B}_i$ can easily notice $\mathcal{B}_i$'s falsified 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 $\mathcal{AM}$) 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 the validity of a bid vector is easily checked by a one-way function and secret key.
- **Non-repudiation**—A winner $\mathcal{B}_i$ cannot deny her/his bid since $\mathcal{B}_i$'s secret key is revealed.
- **Robustness**—Our scheme 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 a

Table 1 Communication amount.

	A bidder (bit)		Server (AM)	
	Bidding	Opening	Opening	#Server
Scheme 1[10]	$1024\log L + 2048$	0	$O(n\log L)$	2
Scheme 2[1]	$1024\log L + 160$	0	$O(n\log L)$	2
DLP	$1024\log L + 1024$	$1024\left(2-\frac{1}{L}\right)$	0	1
Hash	$160\log L + 160$	$160\left(2-\frac{1}{L}\right)$	0	1

feature of entertainment that it does not only decide a winner but also pleases all participants until the winner is decided. In our scheme, 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 though the schemes[3),5),8),9)] do, and what is still better, satisfies anonymity.

6. Performance

In this section, we compare our scheme with two previous schemes[1),10)] from the viewpoint of communication and computation amounts, which are shown in **Table 1** and **Table 2**. Here let the number of bidding points and bidders be $L = 2^k$ and n, respectively. We assume a one-way function f to be DLP (1024-bit) or a 160-bit output one-way hash function, whose output size is denoted by $|f|$.

First we examine the communication amount in Table 1. As for the communication amount in the bidding phase, if we use DLP as a one-way function, the communication amount of our scheme is as efficient as that of the previous schemes. On the other hand, if we use a one-way hash function, the communication amount of our scheme is more efficient than previous schemes. As for the communication amount in the opening phase, the communication between $\mathcal{B}_i$ and $\mathcal{AM}$ is required since we aim at a feature of entertainment. 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 $n/2^t$ bidders in each branch of bit t on the average, and that each bidder sends an opening key in the probability 1/2. Therefore the communication amount for a bidder in the opening is on the average:

$$\frac{1}{n}\cdot|f|\sum_{t=0}^{k}\frac{n}{2^t} = |f|\left(2-\frac{1}{2^k}\right) = |f|\left(2-\frac{1}{L}\right)$$

Table 2 Computation amount

	A bidder	Server (AM)
	Bidding	Opening
Scheme 1[10]	$O(\log L)$	$O(n\log L)$
Scheme 2[1]	$O(\log L)$	$O(n\log L)$
DLP/Hash*	$O(\log L)$	$O(n)$

*Both computation order (DLP, hash) is the same but the unit of computation time is different between hash and DLP. Hash computation is much more efficient.

Both previous schemes have the communication amount between two servers, while our scheme does not have such a communication for a single server.

Next we discuss the computation amount in Table 2. As for the bidding computation, if we use DLP scheme, the communication amount of our scheme is as efficient as that of the previous schemes: all schemes can be conducted in polynomial time of k. Two previous schemes are based on a modular multiplication. Therefore our hash scheme is much more efficient. On the other hand, our computation order for a server is on the average:

$$O\left(\sum_{t=0}^{k}\frac{n}{2^t}\right) = O\left(n(2-\frac{1}{2^k})\right) \simeq O(n),$$
$$\left(0 \le 2 - 1/2^k \le 2\right).$$

Even if the more number of k is set up, the computation amount for a server depends on only n. Note that the computation amount in the opening phase is much more efficient if our scheme uses a one-way hash function.

7. Conclusion

We have proposed an anonymous auction scheme with a single $\mathcal{AM}$. Our scheme realizes the following features:

Perfect anonymity: Nobody can identify a bidder from her/his bid except for a winning bid with low computational and low round complexity 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 scheme can be easily applied to a power auction, which decides the plural winners.

References

1) Cachin, C.: Efficient Private Bidding and Auctions with an Oblivious Third Party, *Proc. 6th ACM Conference on Computer and Communications Security*, pp.120–127 (1999).
2) ElGamal, T.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Trans. Inf. Theory*, Vol.IT-31, No.4, pp.469–472 (1985).
3) Franklin, M. and Reiter, M.: The design and implementation of a secure auction service, *IEEE Trans. Softw. Eng.*, Vol.5, pp.302–312 (1996).
4) Harkavy, M., Tyger, D. and Kikuchi, H.: Electronic Auctions with Private Bids, *Proc. Third USENIX Workshop on Electronic Commerce* (1998).
5) Imamura, Y., Matsumoto, T. and Imai, H.: Electronic Anonymous Bidding Schemes, *Proc. Symposium on Cryptography and Information Security* (1994).
6) Kikuchi, H., Harkavy, M. and Tyger, D.: Multi-round anonymous auction protocols, *Proc. First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp.62–69 (1998).
7) Kobayashi, K., Morita, H., Suzuki, K. and Hakuta, M.: Efficient Sealed-bid Auction by Using One-way Functions, *IEICE Trans. Fundamentals*, Vol.E84-A, No.1, pp.289–294 (2001).
8) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, Vol.E81-A, No.1, pp.20–27 (1998).
9) Nakanishi, T., Fujiwara, T. and Watanabe, H.: An Anonymous Bidding Protocol without Any Reliable Center, *Trans. IPS Japan*, Vol.41, pp.2161–2169 (2000).
10) Naor, M., Pinkas, B. and Sumner, R.: Privacy Preserving Auctions and Mechanism Design, *Proc. ACM Workshop on Electronic Commerce*, pp. 120–127 (1999).
11) NIST: Secure Hash Standard (SHS), FIPS Publication 180-1 (1995).
12) Peng, C.-S., Pulido, M., Lin, J. and Blough, M.: The Design of an Internet-based Real Time Auction Systems, *Proc. First IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp.70–78 (1998).
13) Rivest, R.L.: The MD5 message-digest algorithm, RFC1321 (1992).
14) Rivest, R.L. and Shamir, A.: PayWord and MicroMint: Two Simple Micropayment Schemes, *Proc. Security Protocols*, pp.69–87 (1996).
15) Sako, K.: An Auction Protocol Which Hides Bids of Losers, *Proc. PKC2000*, pp.422–432 (2000).
16) Sakurai, K. and Miyazaki, S.: An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme, *Proc. ACISP2000*, pp.385–399 (2000).
17) Shamir, A.: How to share a secret, *Comm. the ACM*, Vol.22, pp.612–613 (1979).
18) Suzuki, K., Kobayashi, K. and Morita, H.: Efficient Sealed-bid Auction Using Hash Chain, *Proc. ICISC 2000*, pp.189–197 (2000).

(Received December 11, 2000)
(Accepted June 19, 2001)

Kazumasa Omote received the B.E. degree from Osaka Prefecture University, Osaka, Japan in 1997, and received the M. info. Sc. degree from JAIST (Japan Advanced Institute of Science and Technology) in 1999. He is currently pursuing a doctorate degree in the same field at JAIST. His research interests include an electronic auction to design.

Atsuko Miyaji received the B.Sc., M.Sc., and Dr.Sci. degrees in mathematics from Osaka University, Osaka, Japan in 1988, 1990, and 1997 respectively. She joined Matsushita Electric Industrial Co., Ltd. from 1990 to 1998 and engaged in research and development for secure communication. She has been an associate professor at JAIST (Japan Advanced Institute of Science and Technology) since 1998. Her research interests include the application of projective varieties theory into cryptography and information security. She is a member of the International Association for Cryptologic Research and the Information Processing Society of Japan.