Regular Paper

A Second-price Sealed-bid Auction with Public Verifiability

Kazumasa Omote† and Atsuko Miyaji†

A second-price sealed-bid auction is that where a bidder who offers the highest price gets a good in the second highest price. This style of auction solves the problems of both an English auction and a first-price sealed-bid auction. An electronic first-price sealed-bid auction cannot directly be applied to a second-price sealed-bid auction which keeps the highest bid secret. We propose the verifiable discriminant function of the p_0-th root. Our auction scheme satisfies public verifiability of auction results, and also does not have a single entity who knows the highest bid value even after an auction. Furthermore the bidding cost of our scheme is lower than that of the previous one.

1. Introduction

1.1 Background

A *sealed-bid auction* is that each bidder secretly submits a bid to auction manager (AM) only once for an auction. Compared with English auction, a winner is decided more efficiently. In a *first-price sealed-bid auction*, a bidder who offers the highest price gets a good in the highest price. However, a bidder does not have the *dominant strategy* (optimal strategy) in this auction type, so a winning bid may be much higher or much lower. There are many studies on an electronic first-price sealed-bid auction [2),4),7)~9),11)~17)]. On the other hand, in a *second-price sealed-bid auction*, a bidder who offers the highest price gets a good in the second highest price. This style of auction has the *incentive compatibility*. The dominant strategy for each bidder is to place a bid honestly her/his own true value [18)]. So it works the competition principle as well as English auction and a winning bid reflects a market price better than a first-price sealed-bid auction. In our scheme, we electronically realize a second-price sealed-bid auction.

An electronic second-price sealed-bid auction should satisfy the following properties:

(a) **Secrecy of the highest bid:** The scheme should not disclose the exact value of the highest bid. Furthermore, nobody can know the information about the highest bid except that it is placed higher than the second highest bid value. This property is desired for secrecy of winner's bid.

(b) **Anonymity of the second highest bid:** Nobody can identify a bidder who places the second highest bid ($\mathcal{B}_{sec}$). This property is desired because the second highest bid is opened.

(c) **Public verifiability:** Anyone can verify the correctness of an auction.

(d) **Secrecy of loosing bids:** The scheme should keep loosing bids secret. This property is desired in order to keep loser's privacy for the auction managers.

(e) **Robustness:** Any malicious bid can be detected and removed justly by authorities.

(f) **Non-cancelability:** A winner cannot deny that she/he submitted the highest bid after the winner decision procedure.

It is easy to apply a second-price sealed-bid auction to a first-price sealed-bid auction. But a first-price sealed-bid auction cannot directly be applied to a second-price sealed-bid auction which keeps the highest bid secret with public verifiability. This is why we need new techniques for a second-price sealed-bid auction.

1.2 Related Works

We discuss several studies [1),6),12)] as a second-price sealed-bid auction. These schemes set the bidding points discretely. Reference 12) realizes some kinds of sealed-bid auctions using two auction managers AM1 and AM2, which applies the oblivious transfer. But this scheme requires the cut-and-choose technique in order to satisfy public verifiability. Kikuchi [6)] also proposed the (M+1)st-price sealed-bid auction using the verifiable secret sharing technique, where the bidding point is represented by the degree of a polynomial shared by the number of AMs m. In his scheme, there exist some drawbacks: (1) this scheme has a undesirable condition that m is larger than the number of bidding points, so it is difficult to set many bidding points;

† Japan Advanced Institute of Science and Technology

(2) anyone can anonymously disturb an auction by submitting an invalid bid. These problems are solved in our scheme. Abe and Suzuki [1] proposed the (M+1)st-price sealed-bid auction using homomorphic encryption and mix and match technique [5]. Their scheme realizes public verifiability of a winner and the winning bid. However, each bidder must compute K+1 zero-knowledge proofs in bidding, where K is the number of bidding points.

1.3 Our Result

Our second-price sealed-bid auction scheme uses two kinds of auction managers (AM1 and AM2). AM1 treats the bidder registration. AM2 manages the bidding phase in an auction. Only the cooperation of both AM1 and AM2 can decide a winning bid, together with a winner. In the bidding phase, each bid can be verified by AM1 and AM2. In the opening phase, anyone can verify the auction process and the results (a winning bid and a winner) by the techniques of the discriminant function of the p_0-th root, the verifiable w-th power mix, the verifiable ElGamal decryption, and the verifiable decryption mix. Our scheme satisfies the above properties. Nobody can know the information about the highest bid except that it is placed higher than the second highest bid value, but anybody can publicly verify the auction results. There is no single entity who knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values by himself. Furthermore, each bidder does not have to compute the zero-knowledge proofs unlike [1]. So the computational cost of bidder is lower.

The remaining of this paper is organized as follows. Section 2 discusses the effect of a second-price sealed-bid auction from the viewpoints of economics. Section 3 reviews the previous scheme [1] and describes its drawbacks. Section 4 describes our protocol in detail. Section 5 investigates the features of our scheme.

2. Advantages of a Second-price Sealed-bid Auction

2.1 Economic Viewpoints

A second-price sealed-bid auction have been proposed by W. Vickrey, who won the Nobel Economics Prize in 1961 [18]. A second-price sealed-bid auction is that each bidder secretly submits a bid to Auctioneer only once, and a bidder who offers the highest price gets a good in the second highest price. Here we explain why a second-price sealed-bid auction is so outstanding by the following example. Three bidders $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$ participate the car, BMW, auction and their *true values* for it, which means the maximum value that each bidder can spend, are as follows:

- $\mathcal{B}_1$'s true value : \$66,000;
- $\mathcal{B}_2$'s true value : \$64,400;
- $\mathcal{B}_3$'s true value : \$60,900.

If a bidder can buy BMW cheaper than her/his true value, she/he will make a profit. If she/he buys BMW higher than her/his true value, her/his purchase will end in failure. So the true value means the boundary between losses and gains for each bidder.

Suppose that they participate in a first-price sealed-bid auction under the above situation. Then each bidder will never place her/his true value since she/he wants to buy BMW as cheap as possible. In this case, it is often happened for each bidder to tap other bids in order to estimate exactly her/his bid since they can buy it as cheap as possible. If a winning bid is much higher than the second highest price, a winner may want to cancel it. Even if a winner bought a good, she/he will not agree with it.

However, suppose that they participate in a second-price sealed-bid auction. Then each bidder will place her/his true value since she/he cannot reduce her/his cost for BMW by her/his bid. Generally, it is said that a bidder has the *dominant strategy* in a second-price sealed-bid auction.

Dominant strategy: The dominant strategy (optimal strategy) means that the best way for a player exists even if the other players take any strategy.

So it is useless for each bidder to estimate other bids. A winner's bid is decided by other bids. A winner's bid value is not a winning bid value but a datum line to decide a winner. So any bidder will place her/his true value in a second-price sealed-bid auction, which has the following property of *incentive compatibility*.

Incentive compatibility: The incentive compatibility means that the dominant strategy for each bidder is to place a bid honestly her/his own true value [18].

Each bidder can place a bid through mutual agreement. As a result, a bidder will not want to cancel her/his bid. Therefore a second-price sealed-bid auction is superior to a first-price sealed-bid auction from the view points of economics.

Next we compare a second-price sealed-bid

auction with an English auction. A winning bid value in a second-price sealed-bid auction becomes the second highest true value ($64,400) as mentioned above. On the other hand, in an English auction, each bidder places a bid many times until their true value. As a result, $\mathcal{B}_1$ gets BMW in $64,400+$\Delta$ ($\Delta \simeq 0$) since $\mathcal{B}_2$ does not place a bid in more than $64,400. Therefore a winning bid in a second-price sealed-bid auction is almost the same value as one in an English auction. This means that a second-price sealed-bid auction works the competition principle as well as an English auction.

2.2 Bidder Privacy

As for privacy of bidder, it is desired that the correspondence of each bidder to each bid is not revealed for auction manager(s) (AM). In a first-price sealed-bid auction, the correspondence of a winner to her/his bid is revealed for AM. On the other hand, in a second-price sealed-bid auction, the correspondence of winner to her/his bid is not revealed for AM since a winning bid is different from the bid that a winner placed. Therefore a second-price sealed-bid auction protects the privacy of bidder better than a first-price sealed-bid auction.

3. Previous Scheme

Here we summarize a previous scheme [1)] which uses homomorphic encryption and mix and match technique.

3.1 Protocol

There are bidders $\mathcal{B}_1, \ldots, \mathcal{B}_I$, auction manager AM, and the trusted authority TA. The TA generates a secret key and a public key of ElGamal cryptosystem that each bidder uses in the bidding phase. The AM sets the bidding points $\{1, \ldots, K\}$. When a bidder places a bid, she/he generates a bid vector which conceals the bid value by ElGamal encryption E. A bidder must send either $E(1)$ or $E(r)$ as the element of bid vector. The TA can know any bidder's bid value by decrypting the element. In order to conceal the bid values for the TA, this scheme may share the secret key among plural authorities by using a secret sharing technique.

In the opening phase, this scheme uses the following homomorphic property for each bidding point:

$$\overbrace{E(1)\cdots E(1)}^{I-b}\overbrace{E(r)\cdots E(r)}^{b} = E(r^b),$$

where E is an ElGamal encryption and r is public number. Suppose that I is the number of bidders and b is the bidding number in the bidding point k. The mix and much technique can publicly show whether $D^*(E(r^\lambda)) \in \{1, r, r^2, \ldots, r^I\}$ or not, where D^* is the verifiable ElGamal decryption. If $D^*(E(r^\lambda))$ is r^b, b bidders place a bid in the bidding point k. The AM finds the highest bidding point so that $D^*(E(r^\lambda))$ might be r^{M+1}, where M is the number of winners. It becomes the second highest bid (a winning bid value).

3.2 Drawbacks

Since a bidder must send either $E(1)$ or $E(r)$ as the element of bid vector, each bidder must compute $K+1$ zero-knowledge proofs that each element in bid vector is whether $E(1)$ or $E(r)$. So the computational cost for a bidder gets rather large.

4. Our Scheme

4.1 Goals

Our main goals are to realize the following three requirements in an electronic second-price sealed-bid auction, where $\mathcal{B}_{sec}$ is a bidder who places the second highest bid:

(1) The highest bid value are not disclosed for any entity;
(2) Anonymity of $\mathcal{B}_{sec}$ is satisfied for any entity;
(3) Anyone can publicly verify the auction process and results.

The first goal is desired even after winner's decision in order to satisfy a privacy of winner. Our scheme does not disclose the highest bid value as well as the partial range that the highest bid is placed for any entity including both auction managers (AM1 and AM2). The second goal is important because $\mathcal{B}_{sec}$'s bid is revealed as a winning bid. Our scheme realizes anonymity of $\mathcal{B}_{sec}$ without an anonymous channel. The correspondence of each bid to each bidder is also kept secret unless both AM1 and AM2 collude. The third goal ((c) Public verifiability) is important because our scheme secretly computes the auction results.

Furthermore, in our scheme, each bidder does not have to compute the zero-knowledge proofs unlike [1)]. To reduce the computational cost of bidder is one of our goals.

4.2 Authorities

Our scheme uses two kinds of auction managers (AM1 and AM2) in order to eliminate a strong single authority. The role of each auction managers is as follows:

- **AM1:**

- treats the bidder registration;
- publicly computes the winning bid, decides a winner, and show the validity of the results;
- manages AM1's bulletin board system (BBS) which publishes a list of public keys and shows the validity of the results.

• **AM2:**
- manages the bidding phase;
- verifies a bid information;
- publicly multiplies each element in all bid vectors;
- manages AM2's BBS which publishes the computing process of bids.

4.3 Notations

Notations are defined as follows:

I	:	the number of bidders;
i	:	the index of bidders;
$\mathcal{B}_i$	:	a bidder i ($i = 1, \ldots, I$);
$\mathcal{B}_{sec}$	:	a bidder who places the second highest bid;
$\mathbf{V}_i$	:	a bid vector of bidder i;
p_0, p_1	:	small primes but greater in bit size than number of bidders, I (e.g., 100 bit);
p, q, p', q'	:	large primes ($p = 2p_0p' + 1$, $q = 2p_1q' + 1$) which are secret except for the AM1;
n	:	$n = pq$;
g	:	$g \in_R \mathbf{Z}_n$ whose order is $\mathrm{ord}(g) = 2p_0p'p_1q'$ and has neither p_0-th nor p_1-th root;
k	:	the index of bidding points ($k = 1, \ldots, K$);
$t_{i,k}^{(0)}, t_{i,k}^{(1)}$	:	$\mathcal{B}_i$'s secret random numbers generated by the AM1;
x_i	:	$\mathcal{B}_i$'s private key;
y_i	:	$\mathcal{B}_i$'s public key ($y_i = g^{x_i} \ \%n$);
s, w	:	AM2's private keys (w is relatively prime to p_0: $\gcd(w, p_0) = 1$);
Y	:	AM2's public key ($Y = g^s \bmod n$) that has neither p_0-th nor p_1-th root;
$sig_{key}()$	:	a signature by key;
$E_y()$	:	ElGamal encryption with public key g and $y = g^x$ such as $E_y(m) = (G = g^r, M = my^r)$;
$D^*()$	:	verifiable ElGamal decryption
$\mathcal{M}()$	:	the discriminant function of the p_0-th root, where $\mathcal{M}(y)$ is 1 or 0 whether y has the p_0-th root in $\mathbf{Z}_n$ or not, which can be computed only by the AM1.

4.4 Building Blocks

The ElGamal public-key cryptosystem over $\mathbf{Z}_n$ is as secure as the Diffie-Hellman scheme described in 10). In this scheme, we summarize some proofs of knowledge [3] and their applications over $\mathbf{Z}_n$.

Proof of knowledge

We present three kinds of signatures based on a proof of knowledge.

- $SPK[(\alpha) : y_1 = g_1^\alpha \wedge y_2 = g_2^\alpha](m)$: the proof of the equality of two discrete logarithms.
- $SPK[(\alpha, \beta) : y_1 = g_1^\alpha \vee y_2 = g_2^\beta](m)$: the proof of the knowledge of one out of two discrete logarithms.
- $SPK[(\alpha, \beta) : (y_1 = g_1^\alpha \wedge y_3 = g_3^\alpha) \vee (y_2 = g_2^\beta \wedge y_3 = g_3^\beta)](m)$: the proof of the knowledge of one out of two discrete logarithms, which is equal to another discrete logarithm of y_3 to the base g_3. This SPK is given by combining above two SPKs.

The verifiable p_0-th root

Lemma 1 For $n = pq$ ($p = 2p'p_0 + 1, q = 2q' + 1, p', q', p_0$: different primes > 2), $z \in \mathbf{Z}_n$ has the p_0-th root if and only if $z^{2p'q'} = 1 \pmod n$.

Proof. If z has the p_0-th root, there exists x such that $z = x^{p_0}$. Therefore, $z^{2p'q'} = x^{2p'p_0q'} = 1 \pmod n$. Conversely, we can set $z = x^r$ ($r \in \mathbf{Z}_n$) that order of x is $2p'p_0q'$. If $z^{2p'q'} = 1 \pmod n$, then $z^{2p'q'} = x^{2p'q'r} = 1 \pmod n$. So $r = r'p_0$ is necessary ($\exists r' \in \mathbf{Z}_n$). Therefore, $z = x^r = x^{r'p_0} \pmod n$, see, z has the p_0-th root. ∎

$M(z)$ can be computed by only the knowledge of p' and q'. Therefore an authority who knows order of g can publicly prove that z has the p_0-th root by showing

$$SPK[(\alpha) : z^\alpha = 1 \wedge (g^{p_0})^\alpha = 1 \wedge g^\alpha = r](m),$$

for a random number $r \neq 1$. Also, such an authority can publicly prove that z does not have the p_0-th root by showing

$$SPK[(\alpha) : z^\alpha = r \wedge (g^{p_0})^\alpha = 1](m),$$

for random numbers $r \neq 1$. The above two SPKs mean that α is $2p'q'$. Checking whether z has the p_0-th root or not satisfies public verifiability.

Verifiable w-th power mix

A pair of $(c, C = c^w)$ is published, where w is

secret. Let (a, b) and (A, B) be input and output of the verifiable w-th power mix, respectively, where $A = a^w$ and $B = b^w$ $(A \neq B)$. We hide the correspondence of an input to the output, but can show the validity of secret mix by proving the equality of three discrete logarithms of A, B and C. The proof is given by showing

$$SPK[(\alpha) : (A = a^\alpha \wedge B = b^\alpha \wedge C = c^\alpha) \vee (A = b^\alpha \wedge B = a^\alpha \wedge C = c^\alpha)](m).$$

Verifiable ElGamal decryption

We can prove that $m = M/G^s$ is the decryption of $E_Y(m) = (G, M)$ without revealing s by showing

$$SPK[(\alpha) : M/m = G^\alpha \wedge Y = g^\alpha](m).$$

Verifiable decryption mix

Let $(E_Y(a), E_Y(b))$ and (a, b) be input and output of the verifiable decryption mix, respectively, where $E_Y(a) = (G_a, M_a)$ and $E_Y(b) = (G_b, M_b)$. We hide the correspondence of an input to the output, but can show the validity of secret mix. The proof is given by showing

$$SPK[(\alpha) : (M_a/a = {G_a}^\alpha \wedge M_b/b = {G_b}^\alpha \wedge Y = g^\alpha) \vee (M_a/b = {G_a}^\alpha \wedge M_b/a = {G_b}^\alpha \wedge Y = g^\alpha)](m).$$

4.5 Procedure

[Initialization:]

The AM1 selects g, p_0, p_1, p', q', p and q, computes a product $n = pq$, and then publishes (g, p_0, p_1, n) but keeps (p', q', p, q) secret. The AM1 also sets the number K of bidding points for a good. The AM2 computes $Y = g^s \pmod n$ and publishes Y. Note that s is AM2's secret and that both $\gcd(s, p_0) = 1$ and $\gcd(s, p_1) = 1$ hold. The AM1 checks that Y has neither the p_0-th nor p_1-th root and that order of Y is $2p_0p'p_1q'$.

[Bidder registration:]

When Alice $(\mathcal{B}_i)$ participates an auction, she sends her public key y_i with the signature $sig_{x_i}(y_i)$ to the AM1 as a bidder registration. After the AM1 receives her values, he publishes her public key y_i.

[Auction preparation:]

The AM1 chooses her values $t_{i,1}^{(0)}, \ldots, t_{i,K}^{(0)}, t_{i,1}^{(1)}, \ldots t_{i,K}^{(1)} \in \mathbf{Z}_n$, all of which have the p_0-th root, and then secretly sends $\{t_{i,k}^{(0)} \cdot g^{p_0}\}$ and $\{t_{i,k}^{(1)} \cdot g^{p_1}\}$ to $\mathcal{B}_i$. The AM1 shuffles two values in every bidding point:

$$\left(\mathcal{H}(t_{i,1}^{(0)} \cdot g^{p_0}), \mathcal{H}(t_{i,1}^{(1)} \cdot g^{p_1})\right), \ldots, \left(\mathcal{H}(t_{i,K}^{(0)} \cdot g^{p_0}), \mathcal{H}(t_{i,K}^{(1)} \cdot g^{p_1})\right),$$

for $i = 1, \ldots, I$, and places them into AM1's public database. By checking AM1's public database, $\mathcal{B}_i$ can confirm whether her values $t_{i,1}^{(0)} \cdot g^{p_0}, \ldots, t_{i,K}^{(0)} \cdot g^{p_0}, t_{i,1}^{(1)} \cdot g^{p_1}, \ldots, t_{i,K}^{(1)} \cdot g^{p_1}$ are exactly registered. We assume that: nobody except the AM1 knows the correspondence of a bidder to her/his two values; anybody can refer to the data in his public database; but that only the AM1 can alter them.

[Bidding:]

When Alice places a bid at a bidding point $k_i \in \{1, \ldots, K\}$, she generates her bid vector $\mathbf{V}_i$ as follows:

$$\mathbf{V}_i = [E_Y(v_{i,K}), \ldots, E_Y(v_{i,1})],$$

where

$$v_{i,k} = \begin{cases} t_{i,k}^{(1)} \cdot g^{p_1} \pmod n & (k = k_i), \\ t_{i,k}^{(0)} \cdot g^{p_0} \pmod n & (k \neq k_i). \end{cases}$$

She sends $\mathbf{V}_i$ to the AM2. Note that she also sends her reverse bid vector $\mathbf{V}'_i = [E_Y(v'_{i,K}), \ldots, E_Y(v'_{i,1})]$, see, if $v_{i,k} = t_{i,k}^{(0)} \cdot g^{p_0}$, then $v'_{i,k} = t_{i,k}^{(1)} \cdot g^{p_1}$.

[Checking a bid vector:]

The validity of $\mathbf{V}_i$ is checked as follows: (1) The AM2 decrypts $\{E_Y(v_{i,k}), E_Y(v'_{i,k})\}$ by using the verifiable decryption mix; (2) The AM2 computes both $\mathcal{H}(v_{i,k})$ and $\mathcal{H}(v'_{i,k})$ and checks whether or not both values exist in AM1's public database; (3) The AM2 computes

$$\Gamma 1_i = \frac{1}{g^{p_1}} D^* \left(\prod_{k=1}^{K} E_Y(v_{i,k}) \right),$$

and

$$\Gamma 2_i = \frac{1}{g^{Kp_1}} \prod_{k=1}^{K} v_{i,k} v'_{i,k} \qquad (i = 1, \ldots, I)$$

by using the verifiable decryption D^*; (4) The AM1 publicly shows that both $\Gamma 1_i$ and $\Gamma 2_i$ have the p_0-th root. Thanks to this confirmation, any malicious bid vector can be detected by the cooperation of AM1 and AM2. Note that the AM2 does not know whether $v_{i,k}$ and $v'_{i,k}$ have the p_0-th root or not.

[Opening a winning bid:]

First, a winning bid is decided, then a winner is decided by the cooperation of both AM1 and AM2.

Step 1 The AM2 publicly computes the following values for $\mathcal{B}_i$:

$$E_Y(z_{i,K}), E_Y(z_{i,K-1}), \ldots, E_Y(z_{i,1}) = E_Y(v_{i,K}), E_Y(v_{i,K}v_{i,K-1}), \ldots, E_Y\left(\prod_{k=1}^{K} v_{i,k}\right).$$

for $i = 1, \ldots, I$, and then puts them in AM2's BBS.

Step 2 The AM2 publicly computes the following two kinds of values by multiplying $E_Y(z_{i,k})$ of all bidders for a bidding point k,

$$E_Y(Z_k) = \prod_{i=1}^{I} E_Y(z_{i,k}) = \left(g^R, \left(\prod_{i=1}^{I} z_{i,k}\right) \cdot Y^R\right) = (G_k, M_k),$$

$$E_Y(Z'_k) = \left(g^R, \frac{1}{g^{p_1}}\left(\prod_{i=1}^{I} z_{i,k}\right) \cdot Y^R\right) = (G_k, M'_k) \quad k \in \{1, \ldots, K\},$$

where R is the sum of all bidder's random numbers in ElGamal encryption.

Step 3 The AM2 mixes $(E_Y(Z_k), E_Y(Z'_k))$ into $((E_Y(Z_k))^w, (E_Y(Z'_k))^w)$ using w relatively prime to p_0 and the technique of the verifiable w-th power mix, and then publishes the following values:

$$(E_Y(Z_k))^w = E_Y({Z_k}^w) = ({G_k}^w, {M_k}^w),$$
$$(E_Y(Z'_k))^w = E_Y({Z'_k}^w) = ({G_k}^w, {M'_k}^w).$$

The AM1 can publicly show that w is relatively prime to p_0 by using the verifiable p_0-th root technique in 4.4.

Step 4 The AM2 decrypts $E_Y({Z_k}^w)$ and $E_Y({Z'_k}^w)$ into $\mathcal{X}_k = {Z_k}^w$ and $\mathcal{Y}_k = {Z'_k}^w$ using the technique of the verifiable decryption, and publishes $(\mathcal{X}_k, \mathcal{Y}_k)$.

Step 5 The AM1 computes $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$, and publishes a tuple of $(\mathcal{X}_k, \mathcal{Y}_k, \mathcal{M}(\mathcal{X}_k), \mathcal{M}(\mathcal{Y}_k))$. A winning bid value is given by the highest bidding point with both $\mathcal{M}(\mathcal{X}_k) = 0$ and $\mathcal{M}(\mathcal{Y}_k) = 0$.

Since the values $\{t^{(0)}_{i,k}, t^{(1)}_{i,k}\}$ have the p_0-th root, g has neither p_0-th nor p_1-th root, and $\gcd(w, p_0) = 1$ holds, the following three cases are occurred for the values of $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$ in **Fig. 1**:

(1) If no bidder places a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k),\ \mathcal{M}(\mathcal{Y}_k)) = (1, 0)$.

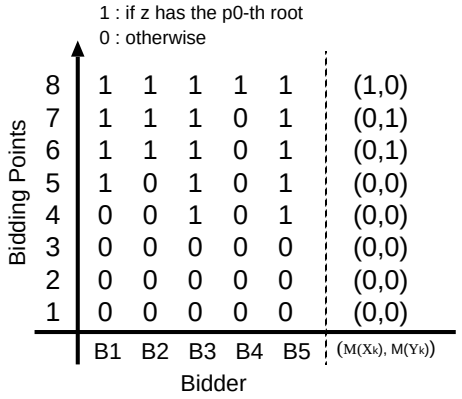

Fig. 1 Opening example.

(2) If only one bidder places a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k),\ \mathcal{M}(\mathcal{Y}_k)) = (0, 1)$.

(3) If more than two bidders place a bid equal to or higher than the bidding point k, then $(\mathcal{M}(\mathcal{X}_k),\ \mathcal{M}(\mathcal{Y}_k)) = (0, 0)$.

Note that we cannot distinguish between case 1 and case 2 because the AM2 uses the technique of the verifiable w-th power mix for $\mathcal{X}_k$ and $\mathcal{Y}_k$.

Public verifiability of a winning bid: The AM1 may rig a winning bid because only the AM1 computes $\mathcal{M}(\mathcal{X}_k)$ and $\mathcal{M}(\mathcal{Y}_k)$. In order to avoid rigging, the AM1 shows the following SPK:

$$SPK[(\alpha) : \mathcal{X}_k^\alpha = r_1 \wedge \mathcal{Y}_k^\alpha = r_2 \wedge \mathcal{X}_{k+1}^\alpha = r_3 \wedge \mathcal{Y}_{k+1}^\alpha = 1](m)$$

for given random numbers r_1, r_2 and r_3 ($r_1, r_2, r_3 \neq 1$). This SPK means that only $\mathcal{Y}_{k+1}$ has the p_0-th root.

Furthermore, the cost of opening bids is $O(\log K)$ by adopting the technique introduced in 4), 6): (1) For a set of bidding points $\{1, \ldots, K\}$, set $k_1 = 1, k_2 = K$ and $k' = \lfloor \frac{k_1+k_2}{2} \rfloor$; (2) If $k' = k_1$ or $k' = k_2$, then output k_2 as the second highest bid value; (3) If $\mathcal{M}(\mathcal{X}_{k'}) = 0$ and $\mathcal{M}(\mathcal{Y}_{k'}) = 0$, then set $k_1 = k'$ and $k' = \lfloor \frac{k_2+k'}{2} \rfloor$, and go to (2). Otherwise set $k_2 = k'$ and $k' = \lfloor \frac{k_1+k'}{2} \rfloor$, and go to (2).

[Winner decision:]

After a winning bid value k (the second highest bid) is decided, the AM2 decrypts all the values $v_{i,k+1}$ ($i = 1, \ldots, I$) using the technique of the verifiable decryption. Anyone can confirm whether or not these values $v_{i,k+1}$ ($i = 1, \ldots, I$) exist in AM1's BBS.

Public verifiability of a winner: In order to decide a winner $\mathcal{B}_j$, the AM1 shows the

following SPK:

$SPK[(\alpha) : (g^{p_0})^{\alpha} = 1 \wedge (v_{j,k+1})^{\alpha} = r_1](m)$

for given random number r_1 ($r_1 \neq 1$). This SPK means that $v_{j,k+1}$ does not have the p_0-th root. A winner $\mathcal{B}_j$'s bid is never revealed. If no bidder places a bidding point $k+1$, more than two winners place a bid at the bidding point k. This means that a winning bid is also k. The AM1 shows the following SPK:

$$SPK[(\alpha) : g^{\alpha} = r_2 \wedge (v_{1,k+1})^{\alpha} = 1 \wedge \cdots \wedge (v_{I,k+1})^{\alpha} = 1](m)$$

for given random number r_2 ($r_2 \neq 1$). This SPK means that all values $v_{i,k+1}$ ($i = 1, \ldots, I$) have the p_0-th root. Note that g does not have the p_0-th root.

5. Consideration

5.1 Features

We discuss the following properties in our protocol.

(a) **Secrecy of the highest bid:** Our scheme keeps the highest bid secret unless both the AMs collude. Nobody can know the information about the highest bid except that it is placed higher than the second highest bid value. Each element $v_{i,k}$ ($z_{i,k}$) has information about whether it has the p_0-th root or not. So only AM1 who knows the products of n realizes the bid values from the values $v_{i,k}$ ($z_{i,k}$). However, such a bid value is encrypted by ElGamal encryption of AM2, and the values $v_{i,k}$ ($z_{i,k}$) themselves are never revealed in the auction procedure. Therefore, AM1 cannot know bid values as long as the ElGamal encryption is secure. Also, AM2 cannot realize bid values because she/he does not know the products of n, even if AM2 knows the values $v_{i,k}$ ($z_{i,k}$). By applying the verifiable w-th power mix to step 3 of the opening phase, the highest bid value can be hidden. Since the AM1 can publicly show that w is relatively prime to p_0, the highest bid value remains correct.

(b) **Anonymity of the second highest bid:** Unless both of the AMs collude, nobody can identify the bidder $\mathcal{B}_{sec}$ even if an anonymous channel is not used. Since all bid vectors are multiplied together before the opening phase, the bidder $\mathcal{B}_{sec}$ is never disclosed. If all bid values are disclosed in the bidding phase, the bidder $\mathcal{B}_{sec}$ is easily decided. As described in (a), each bid value is protected by both hardness of the discriminant of the p_0-th root and the ElGamal encryption. So the identity of $\mathcal{B}_{sec}$ can be protected without using an anonymous channel.

(c) **Public verifiability:** Anyone can publicly verify the correctness of an auction. An auction uses some tools based on the proof of knowledge in order to satisfy public verifiability. As long as the proofs of knowledge are secure, an auction process can be collect. In checking a bid vector, any malicious bid is removed. So a winning bid is decided using only valid bid vectors. By using the technique of verifiable p_0-th root in Step 5 of the opening phase, we can publicly show that a winning bid is valid as well as a winner in an auction.

(d) **Secrecy of loosing bids:** Our scheme keeps loosing bids secret unless both of AMs collude. This feature can be discussed similar to (a).

(e) **Robustness:** Any malicious bid vector can be detected by AM1 and AM2. Unless a bidder uses the valid $v_{i,k}$ and $v'_{i,k}$, anybody notices that $H(v_{i,k})$ or $H(v'_{i,k})$ does not exist in AM1's database. Also, unless a bidder generates the valid V_i, the AM1 notices that $\Gamma 1_i$ and $\Gamma 2_i$ do not have the p_0-th root after the AM2 computes them. So no bidder can disturb the auction system by the malicious bid.

(f) **Non-cancelability:** A winner cannot deny that she/he has submitted the highest bid after the winner decision procedure as long as both (c) and (e) are satisfied. Since the AM1 publicly shows the SPK(s) for the winner decision, a winner is certainly identified.

(g) **Two independent AM's powers:** Our scheme is based on both RSA and ElGamal cryptosystems. Only the AM1 knows the prime factors of n, while only the AM2 knows the secret key of ElGamal encryption. Thanks to separation of two kinds of the cryptosystems, neither AM1 nor AM2 knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values.

5.2 Efficiency

We compare our scheme with the previous scheme [1)] from the viewpoints of the communicational and computational costs in **Table 1**, **2** and **3**. Here let the number of bidding points

Table 1 The communicational costs.

	A bidder ($\mathcal{B}$)	AM		
	Bidding	Preparation	Opening × Round	#AM
[AS02]	$O(K)$	–	$O(1) \times \lceil \log K \rceil$	2
Ours	$O(K)$	$O(IK)$	$O(1) \times \lceil \log K \rceil$	2

Table 2 The computational costs (bidder).

	#Enc	#Proof
[AS02]	K	$K+1$
Ours	$2K$	–

Table 3 The computational costs (AM).

	#Enc	#Proof	#Multiplication	Bid check	#Dec
[AS02]	–	–	$IK + I\lceil \log K \rceil$	$O(IK)$	$2\lceil \log K \rceil + I$
Ours	IK	$I(K+1)$	$2(IK + I\lceil \log K \rceil)$	$O(I)$	$2\lceil \log K \rceil + 2I(K+1)$

and bidders be K and I, respectively.

Table 1 shows the communicational amount of bidding and between the AMs. In both 1) and our scheme, only $\lceil \log K \rceil$ rounds of communication are required in the opening phase because of binary search. In the auction preparation of our scheme, the AM1 must send K ElGamal encryption data to each bidder.

Table 2 and **3** show the computational complexity. In 1), each bidder requires the $K+1$ proofs to avoid the malicious bidding. Such a proof has the large computational amount because it needs both 2-out-of-2 mix and two verifiable decryptions. In our scheme, each bidder does not need to make such proofs, but the AM2 generates $K+1$ proofs for I bidders. In 1), the AM needs the bid checking of the cost $O(IK)$ in order to verify the proofs. In our scheme, the AM2 needs the bid checking of the cost only $O(I)$ because it uses the sum of all bid vectors. The AM1 needs IK ElGamal encryptions for an auction preparation. As for the number of decryption, our scheme requires $2IK$ times in generating proofs, I times in the bid checking, $2\lceil \log K \rceil$ times in the opening phase, and I times in the winner decision phase.

If 1) applies the secret sharing technique for the sake of the TA distribution, both communicational and computational costs becomes larger.

6. Conclusion

We have proposed an electronic second-price sealed-bid auction which mainly satisfies (a) Secrecy of the highest bid, (b) Anonymity of the second-price bid, (c) Public verifiability, and (g) Two independent AM's powers. In our scheme, there is no single entity who knows the highest bid value, a bidder $\mathcal{B}_{sec}$, and loosing bid values. Also, each bidder does not have to compute the zero-knowledge proofs, but the AM computes such proofs. So the computational cost of bidder is lower.

Our scheme may be expanded into the (M+1)st-price sealed-bid auction scheme by modifying our protocol, but we do not consider it here.

References

1) Abe, M. and Suzuki, K.: M+1-st Price Auction Using Homomorphic Encryption, *Proc. 5-th International Workshop on Practice and Theory in Public Key Cryptosystems* (*PKC 2002*), LNCS, pp.115–124, Springer-Verlag (2002).
2) 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).
3) Camenisch, J. and Michels, M.: A Group Signature Scheme with Improved Efficiency, *Advances in Cryptology — ASIACRYPT '98*, LNCS 1514, pp.160–174, Springer-Verlag (1998).
4) Chida, K., Kobayashi, K. and Morita, H.: Efficient Sealed-bid Auctions for Massive Numbers of Bidders with Lump Comparison, *Proc. 4th Information Security Conference* (*ISC 2001*), LNCS 2200, pp.408–419, Springer-Verlag (2001).
5) Jakobsson, M. and Juels, A.: Mix and Match: Secure Function Evaluation via Ciphertexts, *Advances in Cryptology — ASIACRYPT 2000*, LNCS 1976, pp.162–177, Springer-Verlag (2000).
6) Kikuchi, H.: (M+1)st-Price Auction Protocol, *Proc. 5th International Financial Cryptography*

(*FC 2001*), LNCS, page to appear, Springer-Verlag (2001).
7) Kikuchi, H., Harkavy, M. and Tyger, D.: Multi-round anonymous auction protocols, *Proc. 1st IEEE Workshop on Dependable and Real-Time E-Commerce Systems*, pp.62–69 (1998).
8) 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).
9) Kudo, M.: Secure electronic sealed-bid auction protocol with public key cryptography, *IEICE Trans. Fundamentals*, Vol.E81-A, No.1, pp.20–27 (1998).
10) Manbo, M. and Shizuya, H.: A Note on the Complexity of Breaking Okamoto-Tanaka ID-Based Key Exchange Scheme, *IEICE Trans. Fundamentals*, Vol.E82-A, No.1, pp.77–80 (1999).
11) Nakanishi, T., Fujiwara, T. and Watanabe, H.: An Anonymous Bidding Protocol without Any Reliable Center, *Trans. IPS Japan*, Vol.41, No.8, pp.2161–2169 (2000).
12) Naor, M., Pinkas, B. and Sumner, R.: Privacy Preserving Auctions and Mechanism Design, *Proc. ACM Conference on Electronic Commerce*, pp.120–127 (1999).
13) Omote, K. and Miyaji, A.: An Anonymous Auction Protocol with a Single Non-trusted Center using Binary Trees, *Proc. Information Security Workshop* (*ISW 2000*), LNCS 1975, pp.108–120, Springer-Verlag (2000).
14) Omote, K. and Miyaji, A.: An Anonymous Sealed-bid Auction with a Feature of Entertainment, *Trans. IPS Japan*, Vol.42, No.8, pp.2049–2056 (2001).
15) Sako, K.: An Auction Protocol Which Hides Bids of Losers, *Proc. 3rd International Workshop on Practice and Theory in Public Key Cryptosystems* (*PKC 2000*), LNCS 1751, pp.422–432, Springer-Verlag (2000).
16) Sakurai, K. and Miyazaki, S.: An Anonymous Electronic Bidding Protocol Based on a New Convertible Group Signature Scheme, *Proc. 5th Australasian Conference on Information and Privacy* (*ACISP 2000*), LNCS 1841, pp.385–399, Springer-Verlag (2000).
17) Suzuki, K., Kobayashi, K. and Morita, H.: Efficient Sealed-bid Auction Using Hash Chain, *Proc. 3rd International Conference on Information Security and Cryptology* (*ICISC 2000*), LNCS 2015, pp.189–197, Springer-Verlag (2000).
18) Vickrey, W.: Counter Speculation, Auctions, and Competitive Sealed Tenders, *Journal of Finance*, Vol.16, pp.8–37 (1961).

(Received December 4, 2001)
(Accepted June 4, 2002)

Kazumasa Omote received the B.E. degree from Osaka Prefecture University, Osaka, Japan in 1997, and received the M. Info. Sc. and Dr. Info. Sci. degrees from JAIST (Japan Advanced Institute of Science and Technology) in 1999 and 2002. He is currently joining Fujitsu Laboratory and engages in research and development for secure computing. His research interests include the application of information and network security.

Atsuko Miyaji received the B.Sc., the 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. She has joined the computer science department of University of California, Davis since 2002. Her research interests include the application of projective varieties theory into cryptography and information security. She received IPSJ Sakai Special Researcher Award in 2002. She is a member of the Institute of Electronics, Information and Communication Engineers and the Information Processing Society of Japan.