IEICE TRANS. FUNDAMENTALS, VOL.E85–A, NO.5 MAY 2002

PAPER *Special Section on Discrete Mathematics and Its Applications*

A Practical English Auction with Simple Revocation*

Kazumasa OMOTE[†a)], ***Nonmember and*** **Atsuko MIYAJI**[†], ***Regular Member***

SUMMARY An English auction is the most familiar type of auctions. Generally, an electronic auction has mainly two entities, the registration manager (RM) who treats the registration of bidders, and the auction manager (AM) who holds auctions. Before starting an auction, a bidder who wants to participate in English auction is registered to RM with her/his information. An electronic English auction protocol should satisfy the following nine properties, (a) Anonymity, (b) Traceability, (c) No framing, (d) Unforgeability, (e) Fairness, (f) Verifiability, (g) Unlinkability among plural auctions, (h) Linkability in an auction, and (i) Efficiency of bidding. Furthermore from the practical point of view we add two properties (j) Easy revocation and (k) One-time registration. A group signature is adapted to an English auction in order to satisfy (a), (b), and (f) [23]. However such a direct adoption suffers from the most critical drawback of efficiency in group signatures. In this paper we propose more realistic electronic English auction scheme, which satisfies all of these properties without using a group signature. Notable features of our scheme are: (1) both of bidding and verification of bids are done quite efficiently by introducing a bulletin board, (2) both properties (j) Easy revocation and (k) One-time registration are satisfied.

key words: *anonymity, signature of knowledge, bulletin board*

1. Introduction

1.1 Background

An English auction is the most familiar type of auctions. In an English auction, each bidder offers the higher price one by one, and finally a bidder who offers the highest price gets a good. An English auction is used on the Internet as well as the real world. In an English auction through the Internet, it is important to spoil the collusion of bidders, because Internet makes the formation of ring members much easier [19]. Therefore anonymity plays an important role in spoiling the collusion of bidders. It is also important to satisfy anonymity for authorities in order to protect the information of who wants a good and a bidder's history of bidding. In an English auction, all bid values are published and any bidder easily knows the price position of good. A bidder has the *dominant strategy* for bidding, which places a little higher than a current bid value. The competition principle well works, and thus, a winning bid value reflects a market price. This is why an English auction is the most familiar style of auctions. In this paper, we investigate an electronic English auction.

Generally, an electronic auction has mainly two entities, the registration manager (RM) who treats the registration of bidders, and the auction manager (AM) who holds auctions. Before starting an auction, a bidder who wants to participate in an English auction is registered to RM with her/his information. As for studies about an electronic auction, a first-price sealed-bid auction has been often investigated [4], [10]–[13], [17], [18], [21], [22], [24], [26], [28], [29], [31]. A first-price sealed-bid auction is that each bidder secretly submits a bid to AM only once, and a bidder who offers the highest price gets a good. It does not have the dominant strategy for bidding, and thus it has two problems: (1) the competition principle does not work well; (2) a winning bid may be much higher than market one. On the other hand, a second-price sealed-bid auction is that a bidder who offers the highest price gets the good in the second price. It has the dominant strategy, and thus it works the competition principle as well as English auction [32].

In the case of sealed-bid auction, any canceled bid does not affect the valid bidders. However, in the case of English auction, any bid does not allow to be canceled. If a bid can be canceled in an English auction, the highest bid may be insignificant. Therefore, in an electronic English auction, it is the most important to satisfy the following two properties, (a) Anonymity and (b) Traceability. Although any bidder can participate anonymously, it is necessary to identify a winner after a bidding. This means that every bid placed in an English auction must be verified maintaining the bid anonymity. Addition to the above two properties, an electronic English auction should satisfy the following nine properties:

(a) **Anonymity:** nobody can identify a bidder from her/his signature on a bid.
(b) **Traceability:** RM can identify a winner. So a winner cannot deny that she/he submitted the winning bid after the winner decision procedure.
(c) **No framing:** nobody can impersonate a certain bidder.

Manuscript received August 25, 2001.
Manuscript revised November 11, 2001.
Final manuscript received January 20, 2002.

[†]The authors are with the Miyaji Laboratory, Information Science, JAIST, Ishikawa-ken, 923-1292 Japan.
a) E-mail: omote@jaist.ac.jp

*Preliminary version of this paper was presented at ACISP'01 [25].

(d) **Unforgeability:** nobody can forge a bid with a valid signature.
(e) **Fairness:** all bids should be fairly dealt with.
(f) **Verifiability:** anybody can verify a signature on a bid and can confirm whether the bidder is valid or not.
(g) **Unlinkability among plural auctions:** nobody can link the same bidder's bids among plural auctions.
(h) **Linkability in an auction:** anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in an auction.
(i) **Efficiency of bidding:** the computational and communicational amount in both bidding and verifying a bid is practical.

1.2 Related Works

Only a few studies on English auction [19], [20], [23], [25], [30] have been reported as long as we know. On the other hand, many studies on a first-price sealed-bid auction [4], [11]–[13], [17], [18], [21], [22], [24], [28], [29], [31] have been proposed because it can realize fairness more easily than English auction of public auction. These studies [19], [20] do not concern with the security aspect of public auctions but describe those different methods. The scheme [30] also proposed an electronic English auction using reverse hash chains [27] as a bid, which is similar to multiple sealed-bid biddings in order to satisfy fairness. When a bidder participates in an auction, it has two advantages that a valid bidder can place a bid many times by using only one-time signature and that bidder fairness is satisfied for a non-trusted authority. However, in this protocol, the following two problems exist:

1. Since AM knows the bidder's identity, anonymity of bidder is not satisfied for AM after each bidding.
2. The bidding points are set up discretely. For n bidding points, it is necessary for a bidder to compute hash functions n times. Apparently each bidder cannot place a bid as she/he likes.

The scheme [23] proposed an electronic English auction, which keeps a bidder privacy using a slightly modified group signature scheme [6]–[8]. So this protocol suffers from the following drawbacks of group signature schemes. In their scheme, a group manager (GM) works as AM and a group member corresponds to a bidder.

The first problem, which is the most serious, is rather complicated signature generation and verification procedure. In [1], [6]–[8], a membership certificate is used to reduce the data size of public group key [5]: only a group member has the certificate issued by GM. When each member generates a signature on this certificate and a bid, she/he is required the proof of the knowledge. However the proof of the knowledge needs enormous modular multiplication. In an English auction, signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. In an electronic auction, reducing the computational amount of both signature generation and verification are much concerned compared with reducing the group public key size. Therefore we realize an electronic English auction with both fairly simple bidding and verifying procedures by introducing a bulletin board, which is usually used in putting each bid. The important feature of a bulletin board is that anybody can check the correctness of the board easily. In our protocol, the computational cost for both bidding and verifying a bid can be reduced.

The second problem is that it is difficult to revoke a bidder because a membership certificate is distributed to each bidder indicated in [2]. Revocation of bidder is necessary when a bidder wants to withdraw from an auction or RM wants to revoke a certain bidder. Therefore RM should be able to revoke a bidder easily. [3], [15] realize a group signature scheme with a member revocation, both of which do not have to change a public group key. However, these schemes are not so efficient if the member revocation happens frequently like an electronic auction. In our protocol, a revocation of bidder is done easily by using a bulletin board: just remove her/him on it.

1.3 Our Results

Our scheme satisfies above nine properties without using a group signature. Furthermore, our scheme also satisfies the following two properties:

(j) **Easy revocation:** RM can easily revoke a bidder without changing other bidder's public keys.
(k) **One-time registration:** any bidder can participate in plural auctions by only one-time registration. Even if a bidder is identified as a winner, she/he can participate in the next auction without repeating registration, maintaining anonymity for RM, AM, and any bidder.

Our scheme satisfies both (a) and (b) simultaneously by using a combination of both the signature of knowledge and two kinds of bulletin boards. In particular, the computational cost of both bidding and verifying each bid is fairly reduced by introducing a bulletin board. In our protocol, there are two managers RM and AM. RM manages the correspondence of bidder identity to public key, and can identify a winner or a faulty bidder with the help of AM. When a certain bidder is identified after a winner decision procedure or later disputes, AM has only to request RM to identify the bidder.

Our scheme introduces two kinds of bulletin boards

in order to solve the above two problems of group signature. The bulletin boards also play a role of member certificate, and thus our scheme uses two kinds of certificates. Both RM and AM manage their bulletin boards safely.

Notable features of our scheme are as follows:

- Both of bidding and verification of bids are done quite efficiently by introducing a bulletin board.
- Our scheme satisfies both properties (j) Easy revocation and (k) One-time registration.

The remaining of this paper is organized as follows. Section 2 summarizes a basic scheme [23] using group signature. Section 3 describes our protocol in detail. Section 4 considers fairness. Section 5 investigates the properties of our scheme.

2. Related Work

Here we summarize a previous English auction scheme [23] which uses an idea of group signature.

2.1 Group Signature

The concept of group signature was introduced by Chaum and van Heyst [9]. Group signature allows any member to sign on behalf of a group and keeps the member identity secret. The work [8] is the first efficient group signature schemes in that the size of both group's public key and of signatures are independent of the number of group members and that a group's public key remains unchanged if a new member is added to a group. Later, group signature schemes with improved performance and better flexibility are proposed in [1], [6], [7], [14]. [23] is based on these group signatures [6]–[8]. An authority in a group signature scheme is usually divided into two parties, group manager (GM) and escrow manager (EM) by using an idea of identity escrow [14]. In such a scheme, we assume that these two authorities do not collude together.

In an English auction, GM works as auction manager (AM) and a group member corresponds to a bidder. When a bidder places a bid, she/he generates a group signature on a bid. The validity of signature can be verified easily by any participant using a group public key, but any participant does not know who places the bid. EM works to identify a winner at every auction.

2.2 Previous Scheme

This scheme introduces group signature scheme, and thus AM and EM do not collude together.

Setup: AM computes an RSA modulus n, where n is the product of two primes, an RSA key pair (e, d), a cyclic group $G = \langle g \rangle$ of order n over the finite field $\mathbf{Z}_p$ for a prime p, an element $a \in \mathbf{Z}_n^*$ that is of the order $\phi(n)/4$, and an upper bound λ on the length of the private keys: EM chooses $h \in G$ with order n, computes ElGamal-encryption key pair $(\rho,\ Y_E(=h^\rho)) \in \mathbf{Z}_n \times G$, and sets a constant $b \neq 1$. The group public key is $\mathcal{Y} = (n, e, G, g, a, b, \lambda, h, Y_E)$. AM's private key is d and EM's private key is ρ.

Registration: Alice randomly generates a private $x \in \{0, \cdots, 2^\lambda - 1\}$ and sends the value $y = a^x \pmod n$ and $z = g^y$ to AM; AM returns $v = (y + b)^d \pmod n$. Note that AM cannot see the value of x.

Bidding Phase: In order to put a bid m with her signature, she computes the following values $(\tilde{g}, \tilde{z}, d_1, d_2, V_1, V_2, V_3)$:

- $\tilde{g} = g^r$ and $\tilde{z} = \tilde{g}^y$ for $r \in_R \mathbf{Z}_n$;
- $d_1 = {Y_E}^u g^y$ and $d_2 = h^u$ for $u \in_R \mathbf{Z}_n$;
- $V_1 = PK[(\gamma, \delta) : \tilde{z} = \tilde{g}^\gamma \wedge d_2 = h^\delta \wedge d_1 = {Y_E}^\delta g^\gamma](m)$;
- $V_2 = PK[(\beta) : \tilde{z} = \tilde{g}^{a^\beta}](V_1)$;
- $V_3 := PK[(\alpha) : \tilde{z}\tilde{g}^b = \tilde{g}^{\alpha^e}](V_2)$

The notation of a signature of knowledge $(x_1, \cdots, x_k)$ on a message m is as follows:

$$PK[(x_1, \cdots, x_k) : z_1 = f_1(x_1, \cdots, x_k) \wedge \cdots \wedge z_\ell = f_\ell(x_1, \cdots, x_k)](m).$$

The secrets $x_1, \cdots, x_k$ satisfy all ℓ statements: $z_1 = f_1(x_1, \cdots, x_k), \cdots, z_\ell = f_\ell(x_1, \cdots, x_k)$. Assume that computing the discrete logarithm, the double discrete logarithms and the e-th root of the discrete logarithm is infeasible. The concrete algorithm for these signatures is referred to [8]. Alice's group signature consists of a set of $(d_1, d_2, V_1, V_2, V_3)$. If the signature (V_1, V_2, V_3) is valid, anyone confirms that (d_1, d_2) is an encryption of z by using ElGamal encryption function with a EM's public key Y_E, and that Alice knows her private key x and her membership certificate v.

Winner Decision Phase: EM decrypts (d_1, d_2) using his private key ρ and identifies a member Alice from z because he knows the correspondence of z to member's identity.

In this scheme, the signature V_3 is slightly modified using a verifiable group signature sharing scheme in order to satisfy anonymity of bidder.

2.3 Undesirable Properties of the Scheme

This previous scheme satisfies the properties, (a) Anonymity, (b) Traceability, (c) No framing, (d) Unforgeability, (f) Verifiability, and (g) Unlinkability among plural auctions. But there exist some problems as follows.

Efficiency: In applying a group signature to an electronic auction, it is necessary to generate or verify a signature on each bid. A signature generation or verification corresponds to bidding or verification of bids respectively, both of which are required in each bidding. However the computational cost for both signature generation and verification is rather large. Therefore it is not realistic to apply directly a group signature to an electronic auction.

Revocation of Bidder: In an Electronic auction, a revocation of bidder is frequently conducted when a bidder wants to withdraw from an auction or AM wants to revoke a certain bidder. So revocation-procedure should not be complicated. However, in the previous scheme, it is rather difficult to revoke a bidder because a membership certificate has been distributed to each bidder indicated in [2]. Even in the case of [3] or [15], although they realize a revocation of bidders, the computational cost depends on the number of revoked numbers or each bidder must renew her/his key in each revocation of member, respectively.

3. Our Scheme

In this section, we propose a practical electronic English auction. Our scheme satisfies eleven properties mentioned in Sect. 1 without using a group signature. So our scheme can realize more efficient bidding. The secrecy of communication channel is not required because our scheme realizes a public auction.

3.1 Authorities

The authorities of our scheme consist of the registration manager (RM) and the auction manager (AM), where each role of AM and RM is different from that of previous scheme. In our scheme, we assume that these two authorities RM and AM do not collude together. The role of each entity is as follows:

- **RM:**
  - manages the participants of auctions.
  - prepares for auctions.
  - works like Identity Escrow Agency [14] and identifies a certain bidder at the request of AM.
- **AM:**
  - prepares for auctions.
  - sponsors several auctions.
  - manages the current bid value.

GM's roles in the group signature are well divided into two parties RM and AM. Especially the functions of anonymity and Unlinkability are divided into both RM and AM, and are realized by using each bulletin board. That is, in our scheme, two kinds of bulletin boards works as member certificates and also for Unlinkability. Thus it realizes anonymity, Unlinkability and Traceability without using group signature scheme. Furthermore, these bulletin boards make member revocation simple.

In our scheme, there is no single trusted entity, that is, any entity can break neither anonymity nor unlinkability by himself. A protocol with a trusted entity needs the multiple TTP's of the threshold structure. However, our scheme does not need such a threshold structure for auction managers.

3.2 Notations

Notations are defined as follows:

p, q	:	two large primes $(q \mid p-1)$;
g	:	an element $g \in \mathbf{Z}_p$ with order q;
I	:	the number of bidders;
i	:	the index of bidders $(i = 1, \cdots, I)$;
$\mathcal{B}_i$	:	bidder i;
x_i	:	a private key of $\mathcal{B}_i$ $(x_i \in_R \mathbf{Z}_q)$;
y_i	:	a public key of $\mathcal{B}_i$ $(y_i = g^{x_i} \pmod p)$;
r	:	RM's private random number $(r \in_R \mathbf{Z}_q)$;
s	:	AM's private random number $(s \in_R \mathbf{Z}_q)$;
T_i	:	an auction key for $\mathcal{B}_i$;

3.3 Bulletin Board

Our scheme uses two kinds of bulletin boards for RM and AM. A bulletin board is a kind of public communication channel which can be read by anybody, but can be written only by RM or AM.

- RM's bulletin board: $\{p, q, g\}$, a pair of the identities and public keys for bidders, and $\{y_i^r\}$ $(i = 1, \ldots, I)$.
- AM's bulletin board: g^{rs} and $\{y_i^{rs}\}$ $(i = 1, \ldots, I)$, and the current bid value.

3.4 Procedure

Bidder Registration:

A bidder Alice $\mathcal{B}_i$ $(i \in \{1, \ldots, I\})$ registers her public key in the following steps:

1. Alice chooses her private key x_i and computes her public key $y_i = g^{x_i} \pmod p$.
2. She sends y_i to RM, registers her identity and proves that she knows the discrete logarithm x_i of y_i to the base g by showing V_{1i}:
$$V_{1i} = PK[(\alpha) : y_i = g^{\alpha}](m_R),$$
where m_R is a message published by RM.
3. When RM accepts that Alice knows the discrete logarithm, he publishes y_i with her name.

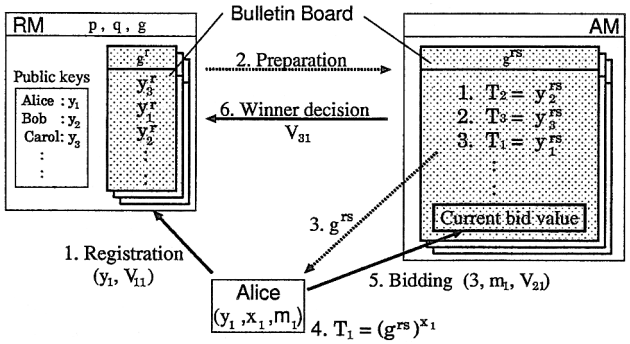

Fig. 1 Overview.

Auction Setup:

When an auction starts, RM computes $y_i^r \pmod p$ $(i = 1, \ldots, I)$ and publishes them with g^r on RM's bulletin board. Note that RM shuffles $\{y_i^r\}$ of all bidders on his bulletin board and keeps her name secretly (Fig. 1).

She can confirm whether there exists her renewal public key y_i^r on RM's board or not by checking $y_i^r \stackrel{?}{=} (g^r)^{x_i}$. Here y_i^r works also as a pseudonym during an auction. Note that the random number r is generated every auction, and so does each user's renewal public key y_i^r.

When a vendor requests AM to hold an auction, AM conducts the following procedure.

1. AM generates a random number $s \in_R \mathbf{Z}_q$ and computes $g^{rs} \pmod p$ by using g^r on RM's bulletin board.
2. AM computes her auction key $T_i = (y_i{}^r)^s \pmod p$ by using the private random number s and y_i^r on RM's bulletin board.
3. AM publishes the shuffled auction key $\{T_i\}$ of all bidders on his bulletin board with g^{rs}.

Note that the random number s is generated every auction, and so does each user's y_i^{rs}. Nobody except for AM can know the correspondence of y_i^r to T_i because y_i^r is concealed by s. On the other hand, AM cannot know the correspondence of y_i to T_i. Therefore neither AM nor RM can identify a bidder from the information on any bulletin board. Furthermore Unlinkability among plural auctions is realized because both the random numbers r and s are changed at every auction.

Each bidder downloads g^{rs} on AM's bulletin board. Alice computes her auction key $T_i = (g^{rs})^{x_i} \pmod p$ for herself. Also, she can easily find her auction key T_i in $\{T_1, \cdots, T_I\}$ published on AM's bulletin board.

Bidding:

When she places a bid, she sends the following bid information (ID_{T_i}, m_i, V_{2i}) to AM.

- the identity ID_{T_i} of auction key T_i
- a bid m_i $(m_i =$ auction identity$||$bid value$)$
- $V_{2i} = PK[(\alpha) : T_i = (g^{rs})^\alpha](m_i)$

Here V_{2i} implies that $\mathcal{B}_i$ knows the value of $\alpha = x_i$ if the signature of knowledge V_{2i} is valid. T_i on AM's bulletin board works like a certificate.

We assume that AM checks the validity of the signature V_{2i} on each bid. Of course, anybody can check the validity. If the signature V_{2i} is invalid signature, AM removes the bid with V_{2i}

Checking the validity of the signature of knowledge V_{2i}, anybody can confirm that $\mathcal{B}_i$ knows her/his private key. Furthermore anybody can accept that the signer is one of the valid bidders if the value ${y_i}^{rs}$ is published on AM's bulletin board.

Winner Decision:

Let Alice's bid (ID_{T_j}, m_j, V_{2j}) be a winning bid. AM publicly must prove that T_j corresponds to ${y_j}^r$ in order for RM to identify Alice. So AM generates the signature of knowledge V_{3j}:

$$V_{3j} = PK[(\alpha) : T_j = ({y_j}^r)^\alpha)](m_R),$$

where m_R is a message published by RM, and publishes V_{3j} with $(T_j, {y_j}^r, m_j, V_{2j})$. Then anybody can confirm the winner by checking the validity of V_{3j} in the following reason.

Theorem 1 *If V_{3j} is a valid signature, then T_j for a winner $\mathcal{B}_j$ is generated by y_j^r.*

Proof. Let $\mathcal{B}_i$'s public key and $\mathcal{B}_j$'s public key be y_i and y_j $(y_j = y_i^z)$, respectively. We assume that nobody knows z. AM can generate $V_{3j} = PK[(\alpha) : T_j = ({y_j}^r)^\alpha)](m_R)$. Here suppose that AM can generate $V_{3j} = PK[(\alpha) : T_j = ({y_i}^r)^\alpha)](m_R)$ $(i \neq j)$. This means that AM can solve the discrete logarithm of T_j to the base y_i^r, which is contradictory to the difficulty of DLP. Therefore AM cannot generate a valid signature V_{3j} using ${y_i}^r$ $(y_i \neq y_j)$. □

When RM received a valid signature V_{3j}, he can identify Alice as a winner for the first time. Note that AM cannot identify a winner Alice in this winner decision.

Winner Announcement:

Only the entity RM knows the winner's identity after the winner decision procedure. This means that all participants including AM cannot identify a winner but can confirm the validity of a winner. If RM informs a vendor of winner's identity after the winner decision procedure, nobody except for RM can identify a winner. Therefore anonymity of a winner is satisfied without

changing her/his public key managed by RM.

Generally, there is a problem of bidder collusion to form a ring. However, in our protocol, even if a winner Alice offers her values of bid, any bidder cannot identify her at the next auction, because both RM and AM change the random number, r and s at every auction.

4. Fairness of Bidder

Fairness of bidder in an electronic auction means that any bid is fairly accepted by AM. Generally, in an electronic English auction, fairness of bidder depends on AM. Note that we do not consider unfairness by network collision here because it can impartially happen to any bidder. There are two unfairness acts by AM:

1. AM repudiates any higher bids than a certain value.
2. AM repudiates any bidding by a certain bidder.

In order to avoid unfairness of case 1, a bidder has to conceal a bid value for AM. In order to avoid case 2, a bidder has only to place a bid anonymously. Our protocol can avoid unfairness of case 2 because the bidding is done anonymously. However, in our protocol, AM can do unfairness act like case 1. Therefore we may use *non-repudiation protocol* [16], [33], [34].

4.1 Outline of Non-repudiation Protocol

The non-repudiation protocol is that Alice sends a message to Bob and then Bob cannot repudiate a receipt of the message from Alice. We summarize the basic procedure.

1. Alice encrypts a message m into C and sends it to Bob.
2. He sends his signature $S_{Bob}(C)$ back to her after receiving C.
3. She sends the decryption key K of C to him after receiving $S_{Bob}(C)$.

Note that if Bob repudiates K after the deadline, she deposits K in TTP (Alice cannot know whether Bob repudiates K or the network between Alice and Bob is broken down). TTP publishes K using public directory service as soon as TTP receives it. Bob cannot deny receiving a message m if the network between Bob and TTP is not permanently broken down.

4.2 Bidding Procedure with Non-repudiation

Fairness of bidder is realized by introducing an idea of non-repudiation protocol as above. Non-repudiation protocol can be added to a bidding procedure of our protocol. Alice and Bob correspond to a bidder $\mathcal{B}_i$ and AM, respectively. RM also plays a role of TTP. In our protocol, both RM and AM use a public bulletin board. A bid m is placed as follows:

1. AM cannot know each bid value because the bid information is encrypted by a bidder.
2. AM publishes his signature $S_{\mathrm{AM}}(C)$ in AM's bulletin board instead of returning it because AM does not know who $\mathcal{B}_i$ is.
3. Even if AM repudiates a receipt of decryption key K from a bidder, he cannot deny getting bid information because RM publishes K in his bulletin board.

5. Consideration

5.1 Features

We discuss the following eleven properties in our scheme.

(a) **Anonymity:** nobody can identify a bidder from her/his signature on a bid. More importantly any bidder can anonymously participate in another auction even if she/he has been identified once.
(b) **Traceability:** RM can open a signature on a bid with the help of AM and can identify a winner. So a winner cannot deny that she/he has submitted the winning bid after the winner decision procedure.
(c) **No framing:** this will be discussed in 5.2.
(d) **Unforgeability:** nobody can forge a bid with a signature V_{2i} because she/he does not know the private key x_i.
(e) **Fairness:** our scheme has fairness of bidder if it applies non-repudiation protocol to bidding. Otherwise AM may decide on which bids to accept. However AM's misbehavior turn out by a bulletin board. A bidder can point out that AM does not accept her/his bid.
(f) **Verifiability:** anybody can verify the signature V_{2i} on a bid. Furthermore anybody can confirm whether a bidder is valid or not by checking her/his auction key in AM's bulletin board.
(g) **Unlinkability among plural auctions:** each auction key is different among plural auctions because the secret values r and s, which are different in every auction, is embedded in y_i^{rs} with a bid. So nobody can link two signatures among plural auctions.
(h) **Linkability in an auction:** a real auction has a linkability in an auction. It is not so important to satisfy unlinkability in an auction of an electronic English auction. An auction becomes active by a certain aggressive bidder who always places a higher bid. Anybody knows how many times a bidder places bids in an auction from the signature because a bidder uses the same y_i^{rs} in an auction.
(i) **Efficiency of bidding:** this will be discussed in 5.3.
(j) **Easy revocation:** this will be discussed in 5.4.

(k) **One-time registration:** any bidder can take part in plural auctions as a valid bidder in one-time registration of public key, maintaining anonymity for RM, AM, and any bidder.

5.2 No Framing

Here we discuss the security against framing attacks such that an entity impersonates another valid bidder.

Theorem 2 *Both RM and AM cannot impersonate a valid bidder.*

Proof. Suppose that they can generates the signature of knowledge V_{2i} to impersonate a bidder $\mathcal{B}_i$. This means that they know the discrete logarithm of y_i^{rs} to the base g^{rs}, that is, the value x_i. This is contradictory to the difficulty of DLP. Therefore they cannot impersonate a valid bidder. □

Even if both RM and AM are colluded, they cannot impersonate a bidder. Of course, other bidders and outsiders cannot also impersonate another valid bidder by Theorem 2.

5.3 Performance

In an English auction, it is required to reduce the time in one bidding because a bidder repeatedly places a bid in real time. Therefore, the computational and communicational costs for one bidding are the most important, compared with the other costs (e.g. the preparation of auction). We estimate the computational and communicational costs for one bidding. We use the definition field of DLP with 1200-bit, and the basepoint with 160-bit order. We assume that [6] uses the same field and the basepoint with about 1200-bit order because it is a RSA-based scheme. This order of basepoint is secret.

Table 1 compares our scheme with the scheme using the efficient group signature scheme [6] from the viewpoints of computational and communicational costs for one bidding by a bidder. Note that English auction scheme applying [6] is much more efficient than [23]. From Table 1, we see that both the computational and communicational costs for one bidding are fairly reduced. As for the efficiency of [6], the signature generation needs 13,000 modular multiplications modulo a 1200-bit modulus in average, and the signature is about 1 kbytes long. On the other hand, in our scheme, the signature generation corresponds to computing the proof of knowledge V_{2i}, and the signature corresponds to V_{2i}. Our signature generation needs 240 modular multiplications modulo a 1200-bit modulus because V_{2i} is the original Schnorr signature, and the signature is about 40 bytes long (160-bit×2) for V_{2i}.

Table 1 The cost for one bidding.

	#Modular multiplication	Communication
[6]	13,000	1000 byte
Our scheme	240	40 byte

Our scheme introduces two kinds of bulletin boards, which play the role of membership certificates. AM has only to check whether the signature V_{2i} is valid or not and whether there exists an auction key is in his bulletin board or not when a bidder places a bid. In this way the computational and communicational costs for one bidding are reduced.

As for the costs of an auction preparation, a bidder needs to download her/his auction key, and both RM and AM need the computational cost of $O(I)$ to renew each bidder's key.

5.4 Easy Revocation

In an electronic auction, a revocation of bidder can be frequently conducted when a bidder wants to withdraw from an auction or RM wants to revoke a certain bidder. Therefore it should be simple and easy. Furthermore the bidding history is kept secret if a bidder is revoked. In the previous schemes including [3], [15], it is not efficient to revoke a bidder because a revocation of bidder frequently happens. In our protocol, it is easy to revoke a bidder: RM has only to delete a bidder from RM's bulletin board.

6. Conclusion

We have proposed an electronic English auction which realize both anonymity of bidders and traceability, maintaining the efficiency of bidding. Main idea of our protocol is that we make use of not group signature but two bulletin boards, which has the feature of public and easy verifiability, and that we well separate the role of biddings into two entities, RM and AM, which also play an important role in the efficiency of bidding. Since we also aim at the functions of a real English auction like Yahoo auction through the internet, our protocol satisfies the features of Linkability in an auction, and Unlinkability among different auctions. However, in some cases where these features are not required, we might need a slight modification in two entities.

We expect that the bidding will be widely conducted by using a limited CPU power terminal such as a portable telephone in the future. Then, our efficient English auction will be more and more required.

References

[1] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik, "A practical and provably secure coalition-registant group signature scheme," Advances in Cryptology—CRYPTO2000, pp.255–270, 2000.

[2] G. Ateniese and G. Tsudik, "Some open issues and new directions in group signatures," Proc. Financial Cryptography'99, pp.196–211, 1999.

[3] E. Bresson and J. Stern, "Efficient revocation in group signatures," Proc. PKC2001, pp.190–206, 2001.
[4] C. Cachin, "Efficient private bidding and auctions with an oblivious third party," Proc. 6th ACM Conference on Computer and Communications Security, pp.120–127, 1999.
[5] J. Camenisch, "Efficient and generalized group signatures," Advances in Cryptology—EUROCRYPT'97, pp.465–479, 1997.
[6] J. Camenisch and M. Michels, "A group signature scheme with improved efficiency," Advances in Cryptology—ASIACRYPT'98, pp.160–174, 1998.
[7] J. Camenisch and M. Michels, "Separability and efficiency for generic group signature schemes," Advances in Cryptology—CRYPTO'99, pp.106–121, 1999.
[8] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups," Advances in Cryptology—CRYPTO'97, pp.410–424, 1997.
[9] D. Chaum and E. van Heyst, "Group signatures," Advances in Cryptology—EUROCRYPT'91, pp.257–265, 1991.
[10] K. Chida, K. Kobayashi, and H. Morita, "Efficient sealed-bid auctions for massive numbers of bidders with lump comparison," Proc. ISC2001, pp.408–419, 2001.
[11] M. Franklin and M. Reiter, "The design and implementation of a secure auction service," IEEE Trans. Software Engineering, vol.5, no.22, pp.302–312, 1996.
[12] Y. Imamura, T. Matsumoto, and H. Imai, "Electronic anonymous bidding schemes," Proc. Symposium on Cryptography and Information Security 11B, 1994.
[13] H. Kikuchi, M. Harkavy, and D. Tyger, "Multi-round anonymous auction protocols," Proc. First IEEE Workshop on Dependable and Real-Time E-Commerce Systems, pp.62–69, 1998.
[14] J. Kilian and E. Petrank, "Identity escrow," Advances in Cryptology—CRYPTO'98, pp.169–185, 1998.
[15] H. Kim, J. Lim, and D. Lee, "Efficient and secure member deletion in group signature schemes," Proc. ICISC2000, pp.150–161, 2000.
[16] K. Kim, S. Park, and J. Baek, "Improving fairness and privacy of ZhouGollmann's fair non-repudiation protocol," Proc. 1999 ICPP Workshops on Security (IWSEC), pp.140–145, 1999.
[17] K. Kobayashi, H. Morita, K. Suzuki, and M. Hakuta, "Efficient sealed-bid auction by using one-way functions," IEICE Trans. Fundamentals, vol.E84-A, no.1, pp.289–294, Jan. 2001.
[18] M. Kudo, "Secure electronic sealed-bid auction protocol with public key cryptography," IEICE Trans. Fundamentals, vol.E81-A, no.1, pp.20–27, Jan. 1998.
[19] M. Kumar and S. Feldman, "Internet auctions," Proc. Third USENIX Workshop on Electronic Commerce, pp.49–60, 1998.
[20] T. Mullen and M. Wellman, "The auction manager: Market middleware for large-scale electronic commerce," Proc. Third USENIX Workshop on Electronic Commerce, pp.49–60, 1998.
[21] T. Nakanishi, T. Fujiwara, and H. Watanabe, "An anonymous bidding protocol without any reliable center," Trans. IPS Japan, vol.41, no.8, pp.2161–2169, 2000.
[22] M. Naor, B. Pinkas, and R. Sumner, "Privacy preserving auctions and mechanism design," Proc. ACM Conference on Electronic Commerce, pp.120–127, 1999.
[23] K. Nguyen and J. Traoré, "An online public auction protocol protecting bidder privacy," Information Security and Privacy (ACISP2000), pp.427–442, 2000.
[24] K. Omote and A. Miyaji, "An anonymous auction protocol with a single non-trusted center using binary trees," Proc. ISW2000, pp.108–120, 2000.
[25] K. Omote and A. Miyaji, "A practical English auction with one-time registration," Proc. ACISP2001, pp.221–234, 2001.
[26] K. Omote and A. Miyaji, "An anonymous sealed-bid auction with a feature of entertainment," Trans. IPS Japan, vol.42, no.8, pp.2049–2056, 2001.
[27] R.L. Rivest and A. Shamir, "PayWord and MicroMint: Two simple micropayment schemes," Proc. Security Protocols, pp.69–87, 1996.
[28] K. Sako, "An auction protocol which hides bids of losers," Proc. PKC2000, pp.422–432, 2000.
[29] K. Sakurai and S. Miyazaki, "An anonymous electronic bidding protocol based on a new convertible group signature scheme," Proc. ACISP2000, pp.385–399, 2000.
[30] S.G. Stubblebine and P.F. Syverson, "Fair on-line auctions without special trusted parties," Proc. Financial Cryptography'99, pp.230–240, 1999.
[31] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient sealed-bid auction using hash chain," Proc. ICISC 2000, pp.189–197, 2000.
[32] W. Vickrey, "Counter speculation, auctions, and competitive sealed tenders," Journal of Finance, vol.16, pp.8–37, 1961.
[33] J. Zhou and D. Gollmann, "A fair non-repudiation protocol," Proc. IEEE Symposium on Security and Privacy, pp.55–61, 1996.
[34] J. Zhou and D. Gollmann, "An efficient non-repudiation protocol," Proc. 10th Computer Security Foundations Workshop (PCSFW). IEEE Computer Society Press, 1997.

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., 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. 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.