Efficient Public Auction with One-Time Registration and Public Verifiability

Byoungcheon Lee, Kwangjo Kim, and Joongsoo Ma

Information and Communications University,
58-4, Hwaam-dong, Yusong-gu, Taejon, 305-732, Korea
{sultan,kkj,jsma}@icu.ac.kr

Abstract. In public auction, all bid values are published, but each bidder participates in auction protocol in anonymous way. Recently, Omote and Miyaji [OM01] proposed a new model of public auction in which any bidder can participate in plural rounds of auction with one-time registration. They have introduced two managers, registration manager (RM) and auction manager (AM), and have used efficient tools such as bulletin board and signature of knowledge [CS97]. In this scheme, even if a bidder is identified as a winner in a round, he can participate in next rounds of auction maintaining anonymity for RM, AM, and any bidder. But a problem of this protocol is that the identity of winner cannot be published. In the winner announcement stage, RM informs the vendor of winner's identity secretly. Therefore RM's final role cannot be verified, and AM and any participating bidder can not be sure of the validity of auction.
In this paper, we propose a new public auction scheme which can solve this problem. In the proposed scheme, both RM and AM execute randomization operation in round setup process which makes the publication of winner's identity be possible while keeping anonymity of winner in next rounds of auction. Moreover, AM provides ticket identifier based on Diffie-Hellman key agreement which is recognized only by the bidder. Our scheme provides real anonymity in plural rounds of auction with one-time registration in a verifiable way.

Keywords: public auction, English auction, anonymity, one-time registration, public verifiability, hash chain, signature of knowledge, anonymous signature scheme

1 Introduction

Electronic auction is an attractive form of electronic commerce and recently many kind of auction services are provided over the Internet. Electronic auction can be classified into sealed-bid auction and public auction according to the way it runs.

In sealed-bid auction [FR96,SKM00,Sako00,OM00,SM00], each bidder secretly submits a bid only once in bidding stage. In opening stage, a bidder who has offered the highest price is announced as a winner. In this type of auction, bid secrecy is of prime concern. Possible problems of sealed-bid auction are that the competition principle does not work well and a winning bid may be much higher than market price. In public auction [OM01,NT00,SS99], also called English auction, all the bid values are published, but each bidder participates in auction protocol in anonymous way. Each bidder offers higher price one by one and can bid multiple times in a round of auction. Finally, a bidder who has offered the highest price becomes a winner. In this case anonymity of bidder is of prime concern. Traditionally, sealed-bid auction and public auction are two different ways of running auction, and one is preferred than the other according to applications. Recently, many online auction services are provided on the Internet and most of them are public auction. In this paper we consider how to improve public auction.

Requirements of public auction can be listed as follows [OM01].

1. Anonymity: Nobody can identify a bidder from a bid.
2. Traceability: A winner who has submitted the winning bid can be traced.
3. No framing: Nobody can impersonate a certain bidder.
4. Unforgeability: Nobody can forge a bid with a valid signature.
5. Non-repudiation: The winner cannot repudiate the fact that he has bidded the winning bid.
6. Fairness: All bids should be dealt with in a fair way.
7. Public verifiability: Anybody can verify the validity of a bidder, the validity of a bid, and the correctness of winner announcement.
8. Unlinkability (among different rounds of auction): Nobody can link the same bidder's bids among different rounds of auction.
9. Linkability (in a round of auction): Anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in a round of auction.
10. Efficiency of bidding: The computation and communication amount in both bidding and verifying should be practical.
11. One-time registration: Bidder can participate in plural rounds of auction anonymously with one-time registration.
12. Easy revocation: RM can revoke certain bidder easily.

Note that we have added the public verifiability and non-repudiation compared with [OM01].

[NT00] proposed a public auction protocol which keeps bidder privacy using group signature scheme. They used the useful property of group signature that a member of a group can sign anonymously on behalf of the group, and the group manager can identify the signer later. But the public auction based on group signature requires complicated signature generation and verification procedure. Moreover the group signature does not satisfy the anonymity for group manager (GM) at all since GM has special power to identify bidders. Revocation of a bidder is also difficult in group signature.

Recently, [OM01] proposed an efficient model of public auction. In their scheme, two managers, registration manager (RM) and auction manager (AM), are introduced to provide the anonymity of bidder. As an anonymous signature scheme, they used the signature of knowledge [CS97] with an anonymous challenge. They made the overall protocol very simple and efficient by using bulletin board as a public communication channel. But a problem of this protocol is that the identity of winner cannot be published. In the winner announcement stage, RM secretly informs the vendor of the winner's identity. Therefore AM and all participating bidders cannot be sure whether RM has executed his role correctly and winner was decided, i.e., the winner announcement is not publicly verifiable. If winner's identity is published (exposed to AM), the anonymity of winner for AM is not satisfied in future rounds of auction because AM uses the same public key in future rounds of auction.

To solve this problem, we propose a new public auction protocol. In our protocol, both RM and AM execute randomization operation in round setup process to prepare auction ticket, so RM or AM alone cannot identify bidders. Moreover winner's identity can be published in the winner announcement stage while keeping the anonymity of winner in future rounds of auction. Therefore, plural rounds of auction with one-time registration is possible in a verifiable way. Moreover, AM provides ticket identifier using Diffie-Hellman key agreement which is recognized only by the bidder.

This paper is organized as follows. First, [OM01] scheme is describe briefly and its problem is discussed in Section 2. Next, cryptographic primitives such as signature of knowledge, hash chain, and Diffie-Hellman key agreement are described in Section 3. Then, the proposed public auction protocol is described in detail in Section 4 and various features of the proposed protocol are discussed in Section 5. Finally, we conclude in Section 6.

2 Omote and Miyaji's Scheme

The public auction scheme proposed by Omote and Miyaji [OM01] is an efficient model of public auction in which bidders can participate in plural rounds of auction with one-time registration. In this scheme, two kind of managers are introduced. Registration manager (RM) secretly knows the correspondence of bidder's identity and bidder's registration key, and works as an identity escrow agency. Auction manager (AM) hosts the auction and prepares auction tickets in each round.

Consider a discrete logarithm based cryptosystem. Let p and q be two large primes satisfying $q|p-1$ and g be a generator of multiplicative group Z_p^* with order q. AM has private key x_A and public key $y_A = g^{x_A}$. The i-th bidder B_i has private key x_i and public key $y_i = g^{x_i}$.

2.1 Procedure

Bidder registration: A bidder B_i registers his public key y_i to RM as follows. He chooses a random number t_i and sends (y_i, t_i) with a proof that he knows the private key x_i (discrete logarithm of y_i to the base g). When RM accepts the proof, he publishes (y_i, t_i) on his bulletin board and keeps bidder's identity B_i secretly in his secure database.

AM's round setup: Assume that AM holds the k-th round of auction. She gets (y_i, t_i) of every participating bidders B_i from RM's bulletin board. She computes shared secret keys $y_i^{x_A}$ for every bidders B_i by using Diffie-Hellman key agreement technique. She generates random numbers r_i for every bidders and keeps them secretly. She computes the following auction keys T_i for B_i

$$T_i = (Enc^k(y_i^{x_A}, t_i), y_i^{r_i}, g^{r_i})$$

where $Enc^k(y_i^{x_A}, t_i) = Enc(y_i^{x_A}, Enc^{k-1}(y_i^{x_A}, t_i))$ is the k-time encryption of t_i using a shared key $y_i^{x_A}$. She publishes the auction keys T_i of all bidders on her bulletin board in a shuffled way.

Bidding: Bidder B_i who wants to participate in the k-th round of auction can easily find his auction key T_i from AM's bulletin board because he can compute $Enc^k(y_i^{x_A}, t_i)$ in advance by using $y_A^{x_i} = y_i^{x_A}$. When he places a bid, he sends the following bid information $(m_i, y_i^{r_i}, g^{r_i}, V_2)$ to AM.

– a bid m_i (m_i = auction ID || bid value)
– $y_i^{r_i}$ and g^{r_i} published by AM
– $V_2 = SK[\alpha : y_i^{r_i} = (g^{r_i})^{\alpha}](m_i)$

Here V_2 is a signature of knowledge [CS97] on message m_i and implies that B_i knows the value $\alpha = x_i$.

Winner decision and announcement: Assume that m_j be a winning bid. AM proves to RM that the public information $y_j^{r_j}$ added to a winning bid m_j corresponds to the public key y_j by sending r_j^{-1}. Then, RM informs a vendor of winner's identity secretly after the winner decision procedure.

2.2 Problem of this Scheme

This scheme is a very efficient public auction in the sense that the bidding and verifying procedures are very simple and each bidder can participate in plural rounds of auction with one-time registration. But a problem of this scheme is that the winner announcement stage is not publicly verifiable. AM's proof to RM (sending r_j^{-1}) and RM's secret identification of the winner to a vendor are not published at all. This kind of secret proof is not a good way in public auction over a distributed network like the Internet. In the winner announcement stage, every bidders can just recognize what the highest bid value is, but they cannot verify whether two managers have executed their job correctly and who the winner is. They just have to trust the honesty of two managers. In AM's point of view, she sends r_j^{-1} to RM, but cannot verify whether RM gives proper identification of winner to the vendor. Therefore this kind of auction protocol that cannot be verified publicly cannot be used in real application and it does not have the one-time registration property.

The reason that winner's identity cannot be published is that anonymity of winner for AM is not provided in future rounds of auction. Since AM uses the same key material y_i for every rounds of auction, she can identify the winner easily in future rounds of auction. So fairness and unlinkability are not provided.

In this paper we propose a new public auction protocol which can solve this problem. The basic idea is that RM executes an additional randomization operation in round setup procedure such that the winner's identity can be published in the winner announcement stage and the winner anonymity for AM is kept in future rounds of auction.

3 Cryptographic Primitives

3.1 Signature of Knowledge

We use the signature of knowledge (SK) of discrete logarithm introduced by Camenisch and Stadler [CS97] as an anonymous signature scheme. Let x be a private key of a signer and $y = g^x$ be the corresponding public key. A pair $(c, s) \in \{0,1\}^l \times Z_q$ satisfying $c = h(m||y||g||g^s y^c)$ where l is a security parameter of hash function, is a signature of knowledge of the discrete logarithm of the element $y \in Z_p$ to the base g on the message m. Such a signature of knowledge can be computed if the private key $x = \log_g y$ is known, by choosing a random number $k \in Z_q$ and computing

$$c = h(m||y||g||g^k) \quad \text{and} \quad s = k - cx \bmod q.$$

It is verified by checking $c \stackrel{?}{=} h(m||y||g||g^s y^c)$. We denote this signature of knowledge as

$$V = SK[x : y = g^x](m).$$

SK represents both the proof of knowledge of the private key x and a signature on message m.

This scheme can be used as an anonymous signature scheme if (y^r, g^r) are challenged for a secret random number $r \in Z_q$ instead of (y, g). The signer computes (c, s) satisfying $c = h(m||y^r||g^r||(g^r)^s(y^r)^c)$ for challenged (y^r, g^r). We denote this signature as

$$V = SK[x : y^r = (g^r)^x](m).$$

3.2 Hash Chain

Assume that a bidder B_i and RM are sharing secret bidder information t_i. In each round k, they compute a special hash chain

$$h^k(t_i) \equiv h(t_i, h^{k-1}(t_i))$$

which can be computed only by the bidder B_i and RM who know t_i. If $h()$ is a collision-resistant cryptographic hash function, computing $h^k(t_i)$ without knowing t_i is infeasible even though all $h^j(t_i)$ for $j < k$ are known.

This is a kind of secure channel between B_i and RM. Using this primitive, a bidder can easily identify his round key generated by RM while keeping the anonymity of the round key against any other party including AM.

3.3 Diffie-Hellman Key Agreement

Assume that a bidder B_i has a key pair (x_i, y_i) and AM has a key pair (x_A, y_A). B_i and AM can share a secret key $K_i = y_i^{x_A} = y_A^{x_i}$ using Diffie-Hellman key agreement technique. Using the shared secret key K_i, bidder B_i can easily identify his auction ticket generated by AM, while AM does not know which is B_i's auction ticket.

4 Proposed Public Auction Scheme

In this Section, we describe the proposed public auction scheme which is a modification of [OM01] such that RM executes an additional randomization operation in round setup procedure and winner's identity is published on bulletin board.

4.1 System Set-up

The entities of our scheme consists of the registration manager (RM), the auction manager (AM), and n bidders B_i $(i = 1, ..., n)$. The role of each entity is as follows:

RM
- He is in charge of the one-time registration process and has secret database to keep secret user information.
- He participates in round key setup process to publish round keys in shuffled way on his bulletin board.
- He publishes winner specific information on his bulletin board in the winner announcement stage.

AM
- She prepares auction tickets in each round of auction using a random number and round keys. She publishes them on her bulletin board in a shuffled way. She has secret database to keep random numbers.
- She publishes winner specific information on her bulletin board in the winner announcement stage.
- She has private key x_A and public key $y_A = g^{x_A}$.

Bidder (B_i where $i = 1, ..., n$)
- Bidder has to register to RM to participate in auction.
- He participates in a round of auction using his auction ticket.
- He has private key x_i and public key $y_i = g^{x_i}$.

In [OM01], winner's identity is secretly informed to the vendor by RM, therefore vendor is an important entity. But in our scheme the vendor of auction does not have any role because winner's identity is published on bulletin board. In this setting we assume that RM and AM do not collude each other to open the anonymity of bidder. If they collude, they can identify any bidder.

In our scheme, five bulletin boards are used, i.e., bulletin boards for registration, round key, auction ticket, bidding, and winner announcement. Bulletin board is a kind of public communication channel which can be read by anybody, but can be written only by legitimate party in an authentic way. All communications are executed publicly via bulletin boards except the one-time registration message of bidder to RM. The registration and round key boards are written only by RM and the auction ticket board is written only by AM. The information posted on each bulletin board is as follows.

Registration board (written by RM)
- RM publishes the identities and public keys of registered bidders.

Round key board (written by RM)
- RM computes round keys for every registered bidders and publishes them in a shuffled way.

Auction ticket board (written by AM)
- AM computes auction tickets for every valid bidders listed in round key board of RM and publishes them in a shuffled way.

Bidding board (written by bidder)
- Each bidder posts his bidding information on this board. Only higher bid than the previous highest one can be posted. Posting of a bid cannot be prevented by anybody.

Winner announcement board (written by AM and RM)
- In the winner announcement stage, AM publishes the winner dependent secret random number.
- In the winner announcement stage, RM publishes the winner dependent secret information.

To identify a winner in the winner announcement stage, RM and AM should keep bidder dependent secret information. Therefore, the following two secret databases are used.

User information DB (managed by RM)
- RM maintains secret user information for registered bidders.

Random number DB (managed by AM)
- AM maintains secret random numbers used to generate auction tickets in each round of auction.

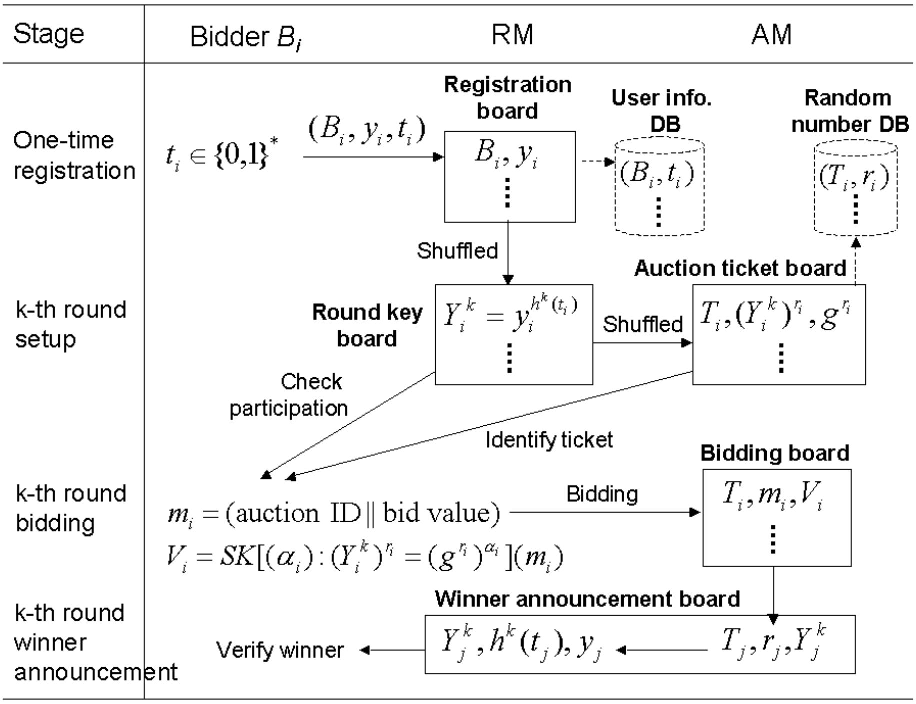

Fig. 1. Public auction protocol

4.2 Public Auction Protocol

The proposed public auction protocol consists of the following 5 stages. Registration of bidder is only one-time in the auction protocol, but other 4 stages are executed in each round of auction. We depict the overall auction protocol in Figure 1.

Stage 1. One-time registration:
A bidder B_i registers to RM as follows:

1. B_i chooses his private key $x_i \in_R Z_q$ and computes his public key $y_i = g^{x_i}$ (Or a certified key with certificate can be used).
2. B_i chooses a random string $t_i \in \{0,1\}^*$ and keeps it secretly.
3. B_i sends (B_i, y_i, t_i) to RM secretly and proves his knowledge of the private key x_i in zero-knowledge.
4. If RM accepts B_i's registration, he publishes (B_i, y_i) on his registration board and keeps (B_i, t_i) secretly in his secure user info DB.

Stage 2. RM's round key setup (k-th round auction):

Now assume that RM, AM and all n bidders are involved in the k-th round of auction. RM computes n round keys $Y_i^k = y_i^{h^k(t_i)}$ for all n bidders using y_i and t_i. Then he shuffles and publishes them on his round key board. Note that a bidder B_i can check easily whether his round key is listed on the round key board because he can also compute round key Y_i^k. But anybody except RM and B_i does not know the correspondence between y_i and Y_i^k. If RM wants to revoke a bidder, then he just removes the bidder from the registration board and removes the round key from the round key board.

Stage 3. AM's auction ticket preparation (k-th round auction):
AM gets the list of all the round keys Y_i^k of n valid bidders from RM's round key board. Then she executes the following steps.

1. She chooses n random numbers $\{r_1, ..., r_n\} \in_R Z_q$.
2. She computes the auction keys $(Y_i^k)^{r_i}, g^{r_i}$.
3. She computes the ticket identifiers $T_i = h((Y_i^k)^{x_A})$.
4. She shuffles and publishes the auction tickets $(T_i, (Y_i^k)^{r_i}, g^{r_i})$ on the auction ticket board.
5. She keeps (T_i, r_i) secretly in her secure random number DB.

Note that a bidder B_i can find the ticket identifier T_i easily as he can compute $T_i = h(y_A^{h^k(t_i)x_i}) = h(K_i^{h^k(t_i)})$ in advance, while AM and RM cannot identify B_i from T_i.

Stage 4. Bidding (k-th round auction):
A bidder B_i who wants to participate in the k-th round of auction executes the following steps.

1. He computes his round key as $Y_i^k = y_i^{h^k(t_i)}$ and checks whether his round key is listed in RM's round key board. If his round key is not listed, he complains to RM.
2. He computes his ticket identifier as $T_i = h(Y_A^{h^k(t_i)x_i})$ and gets his auction ticket $(T_i, (Y_i^k)^{r_i}, g^{r_i})$ from the auction ticket board. If his auction ticket is not listed in the auction ticket board, he complains to AM.
3. He checks the validity of his auction ticket by $(g^{r_i})^{h^k(t_i)x_i} \stackrel{?}{=} (Y_i^k)^{r_i}$. If it does not hold, he complains to AM.
4. He prepares his bid information (T_i, m_i, V_i) as follows and posts them on the bidding board.
   - m_i=(auction ID $||$ bid value), or any relevant information can be included.
   - $V_i = SK[\alpha_i : (Y_i^k)^{r_i} = (g^{r_i})^{\alpha_i}](m_i)$ where $\alpha_i = h^k(t_i)x_i$.

The bid value should be higher than the previous highest one. Note that only the bidder B_i who knows $\alpha_i = h^k(t_i)x_i$ (knows both t_i and x_i) can compute the signature of knowledge V_i.

Stage 5. Winner announcement (k-th round auction):

Assume that a bid m_j of bidder B_j is the highest bid at the end of the bidding stage. AM and RM jointly publish the winner on the winner announcement board as follows.

1. AM announces that (T_j, m_j, V_j) is a winning bid.
2. AM posts (T_j, r_j, Y_j^k) on the winner announcement board which reveals the correspondence between Y_j^k and $(Y_j^k)^{r_j}$.
3. RM posts $(Y_j^k, h^k(t_j), y_j)$ on the winner announcement board which reveals the correspondence between $Y_j^k = y_j^{h^k(t_j)}$ and y_j. It shows that B_j is the winner.
4. Anyone verifies that B_j is the winner using the published values r_j and $h^k(t_j)$.

Although $h^k(t_j)$ is published, t_j is not revealed because of the one-wayness of hash function. $h^{k+1}(t_j)$ cannot be computed from $h^l(t_j)$ for $l \leq k$ without knowing t_j.

The ticket identifier T_i can be recognized only by B_i who knows both t_i and x_i. B_i recognizes the correspondence between y_i and Y_i^k using t_i and recognizes the correspondence between Y_i^k and T_i using x_i. Anybody else including RM and AM cannot identify the two correspondence together. Therefore anonymity of bidder is provided while giving an efficient ticket identifier.

Public verifiability of winner is provided by publishing r_j and $h^k(t_j)$ together. r_j can be published safely after the bidding is finished because it is a random number chosen by AM in a round of auction. $h^k(t_j)$ can also be published safely after the bidding is finished, because $h^{k+1}(t_j)$ is not exposed if t_j is kept secretly.

5 Features

We discuss various features of the proposed public auction protocol according to the list of requirements.

1. Anonymity: We assume that RM and AM do not collude to break the anonymity of bidders. If they collude, they can identify any bidder. They corporate only for winning bid in a public way.
   - Anonymity for RM: RM cannot identify B_i from the auction tickets $(T_i, (Y_i^k)^{r_i}, g^{r_i})$ published by AM on the auction ticket board or bidding information (T_i, m_i, V_i) posted by B_i on bidding board. Identifying Y_i^k from $(Y_i^k)^{r_i}$ is a discrete logarithm problem. Without knowing the secret shared key K_i between B_i and AM, RM cannot identify B_i from T_i. RM also cannot identify B_i from V_i because of the zero-knowledge property of SK.

– Anonymity for AM: AM cannot identify B_i from the round key Y_i^k published by RM without knowing t_i. Identifying y_i from $Y_i^k = y_i^{h^k(t_i)}$ is a discrete logarithm problem. Although AM knows the previous values of $h^l(t_i)$ for $l < k$, she cannot compute $h^k(t_i)$ because of the collision-resistance of the cryptographic hash function $h()$. AM also cannot identify B_i from V_i because of the zero-knowledge property of SK.

2. Traceability: A winner's identity B_j can be identified with the corporation of AM (publishing r_j) and RM (publishing $h^k(t_j)$) together as shown in the winner announcement stage.
3. No framing: Nobody can impersonate a bidder B_i because the signature of knowledge V_i can be computed only with $\alpha_i = h^k(t_i)x_i$ and the bidder B_i is the only person who knows α_i. Even though RM and AM collude, they cannot impersonate B_i.
4. Unforgeability: Anybody including RM and AM cannot forge a valid bid of a bidder B_i with a signature V_i.
5. Non-repudiation: The winner B_j cannot repudiate his bidding because it contains his valid signature V_j.
6. Fairness: Because all bids are anonymous and are posted on the bidding board by the bidder, all bids are dealt with in a fair way.
7. Public verifiability: Because all the relevant information is published on bulletin board, anybody can verify the validity of a bid (by signature of knowledge V_i), the validity of bidder (by round key and auction ticket), and the correctness of winner announcement (by r_j and $h^k(t_j)$).
8. Unlinkability (among different rounds of auction): Because the auction ticket is generated by two randomization operations by RM (round key generation) and AM (auction ticket generation), the auction ticket cannot be linked to a bidder. Therefore, nobody can link the same bidder's bids among plural rounds of auction.
9. Linkability (in a round of auction): Because the same auction ticket is used in a round of auction, anybody can link which bids are placed by the same bidder and knows how many times a bidder places a bid in a round of auction.
10. Efficiency of bidding: In our protocol, most of communication is executed in very simple way, posting on public bulletin boards. Only one exception is that a bidder transmits (B_i, y_i, t_i) to RM through a secure channel in the one-time registration stage. Any complex protocol such as non-repudiation protocol as introduced in [OM01] is not required because a bidder posts his bid on the bidding board. Any secure channel between RM and vendor is not required. The overall computation for one-time registration to RM (1GSK+1VSK), round key generation by RM (1E), auction ticket generation by AM (3E), computing bidding information by bidder (2E+1GSK), and verifying the winner announcement (2E+1VSK) are very efficient, where E, GSK, and VSK represent modular exponentiation, generation of signature of knowledge, and verification of signature of knowledge, respectively.
11. One-time registration: Although the winner's identity in a round of auction is published, the anonymity of auction ticket is maintained in next rounds

of auction. Therefore, bidders can participate in plural rounds of auction anonymously with one-time registration.
12. Easy revocation: When a bidder wants to withdraw from an auction or RM wants to revoke a bidder, RM can simply delete the bidder from his registration board and the round key from the round key board.

We compare the features of proposed protocol with [OM01] in Table 1. In [OM01] AM can distinguish winner's public key although she does not know winner's identity because the same public keys are used by AM repeatedly. Therefore, anonymity for AM, fairness, and unlinkability are not satisfied. As discussed in Section 2, public verifiability and one-time registration are not satisfied in [OM01]. But the proposed scheme satisfies all these requirements. In terms of computational load, the proposed scheme requires a little more exponentiation than [OM01], but both systems are very practical for real application. In communication model, our scheme does not require any non-repudiation protocol because bidding information is posted on bidding board by the bidder.

Table 1. Comparison of proposed public auction scheme with [OM01]

Features	[OM01]	Proposed
Anonymity for RM	O	O
Anonymity for AM	X	O
Traceability	O	O
No framing	O	O
Unforgeability	O	O
Non-repudiation	O	O
Fairness	X	O
Public verifiability	X	O
Unlinkability	X	O
Linkability	O	O
One-time registration	X	O
Easy revocation	O	O
Registration	1GSK+1VSK	1GSK+1VSK
Round setup by RM	–	1E
Round setup by AM	2E	3E
Bidding	1E+1GSK	2E+1GSK
Winner announcement	1E+1VSK	2E+1VSK
Non-repudiation protocol	required	not required

6 Conclusion

We have pointed out the problem of [OM01], lack of public verifiability in the winner announcement stage, and proposed a new public auction scheme which solves this problem. In our scheme both RM and AM execute randomization operations in each round setup process such that RM or AM alone cannot identify bidders, which makes the publication of winner's identity be possible. An efficient ticket identifier is provided such that only a legitimate bidder can identify his auction ticket easily while any other party cannot identify it.

Compared with [OM01], our scheme has following advantages.

1. All the stages of public auction including the winner announcement stage are publicly verifiable because all the relevant information is published on bulletin boards.
2. The overall communication is more efficient. In our scheme winner's identity is published on bulletin boards while it is secretly informed to vendor by RM in [OM01]. Therefore, secure channel is not required in winner announcement stage and non-repudiation protocol for fairness is not required.
3. Plural rounds of auction with one-time registration is possible in a verifiable way.

One drawback of our scheme compared with [OM01] is that the round setup process is executed by two entities, RM and AM, but it is an essential cost to provide public verifiability together with anonymity in one-time registration.

References

[CS97] J. Camenisch and M. Stadler, "Efficient group signature schemes for large groups", In *Crypto'97*, pages 410–424, 1997.

[FR96] M. Franklin and M. Reiter, "The design and implementation of a secure auction service", In *IEEE Transactions on Software Engineering*, pages 302–312, 1996.

[NT00] K. Nguyen and J. Traore, "An online public auction protocol protecting bidder privacy", In *ACISP'2000*, pages 427–442, 2000.

[OM00] K. Omote and A. Miyaji, "An anonymous auction protocol with a single non-trusted center using binary trees", In *ISW'2000*, pages 108–120, 2000.

[OM01] K. Omote and A. Miyaji, "A practical English auction with one-time registration", In *ACISP'2001*, pages 221–234, 2001.

[Sako00] K. Sako, "An auction protocol which hides bids of losers", In *PKC'2000*, pages 422–432, 2000.

[SKM00] K. Suzuki, K. Kobayashi, and H. Morita, "Efficient sealed-bid auction using hash chain", In *ICISC'2000*, pages 189–197, 2000.

[SM00] K. Sakurai and S. Miyazaki, "An anonymous electronic bidding protocol based on a new convertible group signature scheme", In *ACISP'2000*, pages 385–399, 2000.

[SS99] S. G. Stubblebine and P. F. Syverson, "Fair online auctions without special trusted parties", In *Financial Cryptography'1999*, pages 230–240, 1999.