Available online at www.sciencedirect.com
ScienceDirect
The Journal of Systems and Software 81 (2008) 113–119
The Journal of Systems and Software
www.elsevier.com/locate/jss

Bidder-anonymous English auction scheme with privacy and public verifiability

Yu Fang Chung [a], Kuo Hsuan Huang [a], Hsiu Hui Lee [b], Feipei Lai [a,b], Tzer Shyong Chen [c,*]

[a] Department of Electrical Engineering, National Taiwan University, Taiwan
[b] Department of Computer Science and Information Engineering, National Taiwan University, Taiwan
[c] Department of Information Management, Tunghai University, Taiwan

Received 18 May 2006; received in revised form 12 February 2007; accepted 20 March 2007
Available online 28 March 2007

Abstract

This work studies the English auction protocol, which comprises three interactive parties—the Registration Manager, the Auction Manager and the Bidder. The registration manager confirms and authenticates the identities of bidders; the auction manager issues the bidding rights and maintains order in holding the auction. The proposed scheme provides the following security features—anonymity, traceability, no framing, unforgeability, non-repudiation, fairness, public verifiability, non-linkability among various auction rounds, linkability within a single auction round, bidding efficiency, single registration, and easy revocation. The scheme developed herein can effectively reduce the load on the registration and auction managers by requiring the end server to derive the key. It also eliminates the need for bidders to download the auction key and the auction certificate. Hence, the time complexity of processing data is clearly reduced and the best interests of the bidders can be achieved. Accordingly, the scheme is consistent with the actual practice of online transactions.

Keywords: English auction; Anonymity; Unforgeability; Public verifiability

1. Introduction

Online auction protocols presently applied over the Internet include the sealed-bid auction (Omoto and Miyaji, 2000; Franklin and Reiter, 1996; Chida et al., 2001; Kobayashi et al., 2001; Kudo, 1998; Omote and Miyaji, 2001a; Juang et al., 2005) and the public-bid auction, also called the English auction (Kumar and Feldman, 1998; Mullen and Wellman, 1998; Nguyen and Traore, 2000; Wu et al., 2002; Omote and Miyaji, 2001b; Stubblebine and Syverson, 1999; Omote and Miyaji, 2002; Lee et al., 2001). In public-bid auction related works, many researchers proposed various types of auction protocols (Chang and Chang, 2003; Jiang et al., 2005; Hwang et al., 2002; Liaw et al., 2006) focused on the maintenance of bidder's anonymity and the fairness during bidding. However, in these protocols, the auctioneer must verify the identity and bid price of all bidders one by one during the bidding stage to ensure the legality of a bidder and the integrity of the bid price. This type of auction protocol will constitute a heavy calculation load for the server at the auctioneer's end. So, to reduce the calculation load of the entire auction, Omote and Miyaji (2001b) initially developed the use of the bulletin board method for verifying information. Their concept was based on the one proposed by Nguyen and Traore (2000), who suggested the use of group signature technology in the English auction protocol. However, the method of Omote and Miyaji does not publicize bidder information because publishing such information compromises privacy, including anonymity, fairness, and non-linkability among various auction rounds, etc. Later, Lee et al. (2001) proposed a new English auction method that reformed the problem in Omote and Miyaji's method; it allowed information on bidder's identity to be publicized but not to

* Corresponding author. Tel.: +886 4 23590121 3592; fax: +886 2 23504930.
E-mail address: arden@thu.edu.tw (T.S. Chen).

0164-1212/$ - see front matter © 2007 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2007.03.029

the extent as to compromise the anonymity of the bidder in the next round of auction, achieving true one-time registration that lets a bidder repeatedly participate in auctions after registering only once. In the methods proposed by Omote and Miyaji (2001b) and Lee et al., during the auction, the auctioneer must choose a secret parameter for each bidder, and calculate its corresponding public information. Suppose there are n bidders participating in the auction, then the information load that is to be published by the auctioneer on the information verification bulletin board is $3n$; so the greater the number of bidders, the higher the cost of calculation at the auctioneer's end server. Subsequently, Wu et al. (2002) took Omote and Miyaji's method as a prototype and proposed an improvement method that raises efficiency. First, it reduced the information load on the bulletin board from $3n$ to n. Second, it eliminated the need for the auctioneer to choose a secret parameter r for each bidder. Even so, the method could not avert the security concerns that originally existed in Omote and Miyaji's method. Therefore, this work investigates the security compromises of related research approaches, their causes and remedies, and the satisfaction of the requirements (Lee et al., 2001) of the English auction protocol.

(1) Anonymity: No one shall be able to identify the bidder during the auction.
(2) Traceability: The winning bidder must be identifiable at the end of the auction.
(3) No framing: No one shall participate in the auction as the identity of another bidder.
(4) Unforgeability: No one shall falsify a valid bidding price.
(5) Non-repudiation: Bidders cannot deny their bid after the winning bidder has been announced.
(6) Fairness: Bidding must be justly handled by the auction manager.
(7) Public verifiability: Anyone can confirm the identities of bidders and the validity of their bids.
(8) Non-linkability among various auction rounds: No one can access results that enable a bidder to be identified having been involved in various auction rounds.
(9) Linkability within a single auction round: During a single auction round, anyone can determine the number of times a bidder has bid, and tell a bid that is submitted by a particular bidder.
(10) Bidding efficiency: The number of operations and transmissions during the auction must be minimized.
(11) Single registration: A bidder needs only register once, and then can participate in all auctions.
(12) Easy revocation: The register manager can easily revoke the bidding rights of a particular bidder.

This work consists of the following six parts, as follows: brief introduction to auction protocols; operation of the proposed English auction scheme; discussion of security; analysis of performance and operations of the system; comparisons with other methods; conclusions.

2. Proposed English auction scheme

The system has seven stages—initialization, bidder registration, auction key generation, auction setup, bidding, verification, and winning-bidder announcement stages. There are three system participants which are the Registration Manager (RM), the Auction Manager (AM) and the Bidder (B). The system parameters are as follows.

System parameters

p, q	big prime numbers, satisfying $q\|p-1$
g	an element $g \in Z_p$ with order q
B_i	the bidder indexed i
$k_i, t_{1,i}, t_{2,i}$	secret parameters chosen by B_i ($k_i, t_{1,i}, t_{2,i} \in_R Z_q$)
SK_i	B_i's private key ($SK_i \in_R Z_q$)
RK_i	B_i's registration key
SK_{AM}	AM's private key ($SK_{AM} \in_R Z_q$)
PK_{AM}	AM's public key
$Y_{i,j}$	RM with regard to B_i's auction key produced in the jth round of auction
r_j	a secret parameter chosen uniformly at random from Z_q by AM in the jth round of auction
g_j	a generative number published by AM in the jth round of auction
$C_{i,j}$	AM with regard to B_i's auction certificate produced in the jth round of auction
h	a collision-resistant cryptographic hash function h: $\{0,1\}^* \to \{0,1\}^{160}$. In each round of auction, taking the jth for example, h satisfies the conditions $h^j(x) = h(x, h^{j-1}(x))$ and $h^0(x) = x$
$\|\|$	a concatenate operation notation

2.1. Initialization stage

RM and AM work together to establish the system parameters, as follows:

Step 1: RM establishes a read-only bulletin board, on which are posted the two types of information given below. Only RM may write on and update this board.
  (1.1) The identities and the corresponding registration keys of all bidders.
  (1.2) The auction keys of bidders in the jth round of auction.
Step 2: RM declares p, q, g and h publicly.
Step 3: Along with AM, RM establishes a read-only bulletin board for a winning bidder. At the end of each auction, AM and RM together post the winning bidder's information on the board, and allow others to confirm it. Only AM and RM may write on and update this board.

Step 4: AM establishes a read-only bulletin board, and posts all bidders' auction certificates on it. Only AM may write on and update this board.

Step 5: AM randomly selects an integer $SK_{AM} \in {}_RZ_q$ as the private key, and determines the corresponding public key PK_{AM} using Eq. (1)

$$PK_{AM} = g^{SK_{AM}} \bmod p \tag{1}$$

Step 6: Along with RM, AM establishes a read-only bulletin board for a winning bidder. At the end of each auction, RM and AM together post the winning bidder's information on the board, and allow others to confirm it. Only AM and RM may write on and update this board.

2.2. Bidder registration stage

A new bidder, B_i, joining the auction follows the following steps to register:

Step 1: Randomly select an integer $SK_i \in {}_RZ_q$ as the private key and determine the corresponding registration key RK_i using Eq. (2)

$$RK_i = g^{SK_i} \bmod p \tag{2}$$

Step 2: Randomly select an integer $k_i \in Z_q$ and keep it secret.

Step 3: Randomly select an integer $t_{1,i} \in Z_q$ to determine the verification information of RK_i, γ_i and ε_i, using Eqs. (3) and (4)

$$\gamma_i = h(g^{t_{1,i}} \bmod p) \tag{3}$$

$$\varepsilon_i = (t_{1,i} + SK_i \cdot \gamma_i) \tag{4}$$

Step 4: Transmit $\{RK_i, k_i, \gamma_i \text{ and } \varepsilon_i\}$ to RM over a secure channel.

Step 5: After receiving $\{RK_i, k_i, \gamma_i \text{ and } \varepsilon_i\}$, RM validates it using Eqs. (5) and (6)

$$\gamma_i' = h((g^{\varepsilon_i} \cdot RK_i^{-\gamma_i}) \bmod p) \tag{5}$$

$$\gamma_i \stackrel{?}{=} \gamma_i' \tag{6}$$

If Eq. (6) holds, then RK_i is identified as a valid registration key, and B_i is confirmed to exhibit the private key SK_i, which corresponds to RK_i. Conversely, if Eq. (6) does not hold, such a request for registration is refused.

Step 6: RM posts the information on the relation between B_i's identity and RK_i on the RM's bulletin board.

Step 7: RM stores the information on the relation between B_i's identity and the secret parameter k_i in the secret database.

2.3. Auction key generation stage

Consider the jth round of auction. Let the set of registered bidders be $U = \{B_1, B_2, \ldots, B_n\}$. According to Eq. (7) below, RM generates n auction keys, $Y_{i,j}$, for each bidder B_i, then shuffles all $Y_{i,j}$ completely and randomly, and posts them on the RM's bulletin board

$$Y_{i,j} = RK_i^{h^j(k_i)} \bmod p \tag{7}$$

Simultaneously, each B_i determines the auction key $Y_{i,j}$ using the same equation, and verifies that the key is publicly declared on the RM's bulletin board. If B_i cannot find his auction key on the board, then he appeals to RM.

2.4. Auction setup

Consider the jth round of auction, AM generates n auction certificates $C_{i,j}$ for all valid bidders using their auction keys $Y_{i,j}$ on the RM's bulletin board, as follows:

Step 1: Randomly select an integer $r_j \in Z_q$ to determine the public parameter g_j using Eq. (8), and post it on the AM's bulletin board

$$g_j = g^{r_j} \bmod p \tag{8}$$

Step 2: Generate the secret parameter $S_{i,j}$ for each B_i to determine the auction certificate $C_{i,j}$ using Eq. (9), completely shuffle all auction certificates $C_{i,j}$ using Eq. (10), and post $C_{i,j}$ on the AM's bulletin board

$$S_{i,j} = Y_{i,j}^{SK_{AM}} \bmod p \tag{9}$$

$$C_{i,j} = Y_{i,j}^{r_j \cdot S_{i,j}} \bmod p \tag{10}$$

2.5. Bidding stage

The B_i participates in the jth round of auction following the steps below:

Step 1: Generate $S_{i,j}$ using the AM's public key PK_{AM} and Eq. (11)

$$S_{i,j} = PK_{AM}^{h^j(k_i) \cdot SK_i} \bmod p \tag{11}$$

Step 2: Determine the auction certificate $C_{i,j}$ using $S_{i,j}$ and the personal private key SK_i, based on Eq. (12)

$$C_{i,j} = g_j^{h^j(k_i) \cdot S_{i,j} \cdot SK_i} \bmod p \tag{12}$$

Also, check whether $C_{i,j}$ is publicly declared on the AM's bulletin board; if not, appeal to AM.

Step 3: Randomly select an integer $t_{2,i} \in Z_q$ and determine $bid_{i,j}$ to generate the corresponding signature $\{\alpha_{i,j}, \beta_{i,j}\}$ following the Schnorr-like signature scheme (Schnorr, 1990) as shown in Eqs. (13) and (14)

$$\alpha_{i,j} = h(g_j^{t_{2,i}} \bmod p \| bid_{i,j}) \tag{13}$$

$$\beta_{i,j} = (t_{2,i} + \alpha_{i,j} \cdot h^j(k_i) \cdot S_{i,j} \cdot SK_i) \tag{14}$$

Step 4: Post the bidding information $\{C_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ on the bidders' bulletin board. Each bidder is enabled to write on and update the board.

2.6. Verification stage

After bidders have posted their individual bidding information on the bidders' bulletin board, any verifier can validate the bidding information thereon, as follows:

Step 1: Confirm the auction certificate $C_{i,j}$, based on Eqs. (15) and (16)

$$\alpha'_{i,j} = h((g_j^{\beta_{i,j}} \cdot C_{i,j}^{-\alpha_{i,j}} \bmod p) \| bid_{i,j}) \quad (15)$$

$$\alpha_{i,j} \stackrel{?}{=} \alpha'_{i,j} \quad (16)$$

Only if Eq. (16) holds, $C_{i,j}$ is identified as a valid auction certificate, and B_i offers the bidding information attached to $C_{i,j}$.

Step 2: Check the AM's bulletin board to determine whether a valid bidder submitted the auction certificate RM.

2.7. Winner-bidder announcement stage

Following the bidding, the bidder who has submitted the highest bid is the winner. For others to verify the winning bidder, AM and RM together post the relevant information on the winning bidder's bulletin board, as follows:

Step 1: AM posts the winning bidder's information $\{C_{i,j}, (r_j \cdot S_{i,j}), Y_{i,j}\}$ on the winning bidder's bulletin board. Hence, any verifier can confirm the relation between $C_{i,j}$ and $Y_{i,j}$, given by the equation below

$$C_{i,j} = Y_{i,j}^{r_j \cdot S_{i,j}} \bmod p$$

Step 2: According to the information $Y_{i,j}$ posted by AM, RM determines the winning bidder's identity and the corresponding registration key RK_i, and posts $\{Y_{i,j}, h^j(k_i), \mathrm{RK}_i\}$ on the winning bidder's bulletin board. Therefore, any verifier can confirm the existing relation between RK_i and $Y_{i,j}$, according to the equation below, and thus determines the winning bidder's identity from the RM's bulletin board, by comparing with RK_i

$$Y_{i,j} = \mathrm{RK}_i^{h^j(k_i)} \bmod p$$

3. Security analysis

The security requirements (Lee et al., 2001) of an English auction scheme are explained as follows:

(1) Anonymity: Unless AM and RM are colluding, no one can identify the bidders during the auction.
  (1.1) Anonymity in the case of RM: AM uses the random number r_j to generate the auction certificate $C_{i,j}$, so RM cannot identify a bidder by comparing $C_{i,j}$ with the corresponding $Y_{i,j}$.
  (1.2) Anonymity in the case of AM: RM generates the auction key $Y_{i,j}$ using the secret parameter k_i chosen by B_i and the mutual operation of $h^j(k_i)$, so RM provides AM a different $Y_{i,j}$ for each B_i in each round of the auction. Additionally, $h^j(k_i)$ is kept secret to AM. Hence, AM can neither determine RK_i that corresponds to $Y_{i,j}$ nor identify the bidder that corresponds to $Y_{i,j}$.

(2) Traceability: Throughout the entire auction process, all bidders bid anonymously with the help of the auction certificate $C_{i,j}$ issued by AM. Therefore, to the bidders, the most important thing at the end of the auction when the winning bidder is finally announced is the ability to confirm the identity of the winning bidder, and verify his legality. Besides, the owner of the auctioned goods can also directly deliver the goods to the winning bidder, completing the transaction and preventing compromise of the winning bidder's rights in the case that RM fails to announce the winning bidder. So, at the end of the auction, AM and RM each make public the partial information they hold on the winning bidder's identity for any person to verify. As described in the winner-bidder announcement stage, any verifier can look up the winning bidder's auction key $Y_{i,j}$ through the winning bidder's information $\{C_{i,j}, (r_j \cdot S_{i,j}), Y_{i,j}\}$ announced by AM, and then through the winning bidder's information $\{Y_{i,j}, h^j(k_i), \mathrm{RK}_i\}$ announced by RM obtain the registration key RK_i that corresponds to the winning bidder's auction key. Then, by comparing RK_i, the verifier can obtain from the bulletin board the true identity of the winning bidder.

(3) No framing: Unless an attacker obtains B_i's private key SK_i, no one can forge a valid signature, $\{\alpha_{i,j}, \beta_{i,j}\}$, and participate in the bidding in B_i's name. If an attacker seeks to determine the private key SK_i from the public information, then he must use one of the two following methods:
  (3.1) The attacker derives from RK_i the computation complexity of SK_i as the difficulty of solving the discrete logarithm problem (DLP).
  (3.2) First obtain the $t_{1,i}$ in Eq. (3) or the $t_{2,i}$, in Eq. (13), then use Eq. (4) or Eq. (14) to obtain SK_i; the attacker shall face the difficulty of breaking Schnorr's signature scheme (Schnorr, 1990).
  According to the above analyses, the following conclusion is obtained: the attacker cannot derive SK_i via those two methods because no one can impersonate B_i to generate his valid bidding information $\{C_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$.

(4) Unforgeability: Based on the following analyses, the proposed scheme confirms that attackers cannot generate a valid auction certificate $C_{i,j}$ or forge any valid bidder information.
  (4.1) An attacker cannot obtain SK_i, $S_{i,j}$ and k_i.
  (4.2) If an attacker intends to determine $(h^j(k_i) \cdot S_{i,j} \cdot \mathrm{SK}_i)$ from $C_{i,j}$, he must initially handle the

difficulty of solving the discrete logarithm problem.

(4.3) $h^j(k_i)$ evolves with each round of the auction. Hence, each bidder is assigned different auction key $Y_{i,j}$ and auction certificate $C_{i,j}$ in each round of the auction.

(5) Non-repudiation: According to the analysis on "No framing", signature $\{\alpha_{i,j}, \beta_{i,j}\}$ can be generated only by the bidder himself. If the validity of $\{\alpha_{i,j}, \beta_{i,j}\}$ passes verification, then the winning bidder cannot deny his bid price.

(6) Fairness: Bidders bid anonymously and post the bidding information on the bidders' bulletin board by themselves. Hence, AM is bound to justly handle all bidding information.

(7) Public verifiability: All participants can test and verify the legitimacy of the bidders and the winners.

(7.1) The bidding stage: B_i posts bidding information $\{C_{i,j}, bid_{i,j}, \alpha_{i,j}, \beta_{i,j}\}$ on the bidders' bulletin board. Any bidder can use Eqs. (15) and (16) to test and verify the legitimacy of $\{C_{i,j}, bid_{i,j}\}$, and through the information posted on the AM's bulletin board, confirm whether the certificate $C_{i,j}$ has been issued by AM or not, and also whether the bidder is authorized to participate in the auction.

(7.2) The announcement of the winner: The winner is announced through the bulletin board shared by AM and RM, by posting the information $\{C_{i,j}, (r_j \cdot S_{i,j}), Y_{i,j}\}$ and $\{Y_{i,j}, h^j(k_i), \mathrm{RK}_i\}$. The identity of the winner is available to all.

(8) Non-linkability among various auction rounds: In each auction round, RM causes $Y_{i,j}$ to differ, and AM also causes $C_{i,j}$ to differ using a different random number r_j. That is, unless AM and RM conspire, no one can determine the linkability of the same bidder among various rounds of auctions.

(9) Linkability within a single auction round: During an auction, a bidder uses a single auction certificate $C_{i,j}$ to bid. Hence, how many times a bidder bids in the same round of auction can be determined, along with which bids are made by which bidder.

(10) Bidding efficiency: A more detailed discussion is presented in Section 4.

(11) Single registration: Bidders bid anonymously during the auction. Therefore, bidders need only register once with RM, and still keep themselves anonymous in any subsequent round of the auctions.

(12) Easy revocation: RM needs only remove the information about B_i, including the secret parameter k_i from the database, and related information on the bulletin board. Then, he can revoke B_i's bidding rights.

On the method by Omote and Miyaji, Wu et al. (2002) refined it by reducing the load associated with verifying the content of the bulletin board, and increased the efficiency of the system. However, this method does not allow posting of the identity of the winner for verification because the registration key is not renewed with each round of auction. Consider that a past winner participates in a subsequent auction. AM might compare this bidder's key to the registration key issued by RM; he can thus determine the actual identity. This case leads to unfair bid handling for the requirements of anonymity and non-linkability among various auction rounds become inapplicable to AM. To maintain anonymity, the winner is forced to create a new registration key and register it with RM. Such a device ensures anonymity, but undermines the efficiency requirement of single registration. The security analysis is in contrast to the method presented below, in which "Yes" indicates that the requirement is satisfied, and "No" indicates that the requirement is not satisfied. The details can be referred to Table 1.

Table 1
Analysis of security requirement for auction schemes

Comparison items	Contrast method (Wu et al., 2002)	The proposal
Anonymity in the case of RM	Yes	Yes
Anonymity in the case of AM	No	Yes
Traceability	Yes	Yes
No framing	Yes	Yes
Unforgeability	Yes	Yes
Undenialability	Yes	Yes
Fairness	No	Yes
Public verification	No	Yes
Non-linkability among various auction rounds	No	Yes
Linkability within a single auction round	Yes	Yes
Bidding efficiency	Yes	Yes
Single registration	No	Yes
Easy revocation	Yes	Yes

4. Analysis and discussion of performance

Time complexity is used for comparison to estimate the cost of executing operations. The given symbols are defined as follows.

The time complexity of modulus addition operation is very low, so it is neglected in the calculation of the cost of computation. The details can be referred to Table 2.

Table 3 below presents the required computation complexity for the contrast method (Wu et al., 2002) and the proposal, based on the above information. The values in Table 3 are the result of the summing the number of times

Table 2
Definition of operation symbols

Symbol	Definition
T_{MUL}	Time complexity of modulus multiplication operation
T_{EXP}	Time complexity of modulus exponentiation operation
T_{INV}	Time complexity of modulus inverse element operation
T_{H}	Time complexity of one-way hash function operation
T_{S}	Time complexity of searching for a key on the bulletin board

Table 3
Computation complexity for processing

Computation complexity	The contrast method	The proposal
Bidder registration	$4T_{EXP} + 2T_{MUL} + 2T_H$	$4T_{EXP} + 2T_{MUL} + 2T_H$
Auction key generation	–	$nT_{EXP} + nT_H$
Auction setup	$(2n+1)T_{EXP} + 3nT_{MUL} + nT_{INV} + nT_H$	$(2n+1)T_{EXP} + nT_{MUL}$
Bidding	$4T_{EXP} + 3T_{MUL} + 2T_H$	$3T_{EXP} + 6T_{MUL} + 1T_H$
Verification	$2T_{EXP} + 3T_{MUL} + 1T_{INV} + 1T_H + 1T_S$	$2T_{EXP} + 1T_{MUL} + 1T_H$

the various operations were used in different stages of auction. The comparison table shows drops in the number of the modulus multiplication operations, modulus exponentiation operations, modulus inverse element operations and one-way hash function operations in the auction setup stage of the proposed scheme.

From Table 3, it can be seen that the computation complexity required for the bidder registration stage in these two methods is similar. In the bidder registration stage, each bidder creates a registration key associated with related verification information, and the required computation complexity is $1T_{EXP}$ for Eq. (2) and $1T_{EXP} + 1T_H + 1T_{MUL}$ for Eqs. (3) and (4). Also, RM has to validate the registration key using Eqs. (5) and (6), which employs $2T_{EXP} + 1T_{MUL} + 1T_H$. Therefore, the total computation complexity is $4T_{EXP} + 2T_{MUL} + 2T_H$ in the registration stage.

Assume that there are n bidders in the auction key generation stage, then what costs for RM to launch an auction key to each bidder using Eq. (7) is $nT_{EXP} + nT_H$. Although the proposed scheme additionally employs an auction key generation stage, the extra stage is worth the effort from the perspective of security. For instance, the requirements, such as anonymity, fairness, public verifiability, non-linkability among various auction rounds, single registration, are thus met.

For the auction setup stage in the proposed method, AM firstly generates the public parameter g_j using Eq. (8), which takes $1T_{EXP}$. Then, AM generates n auction certificates for all bidders, and spends nT_{EXP} for Eq. (9) and $nT_{EXP} + nT_{MUL}$ for Eq. (10). Thus, the total computation complexity is $(2n+1)T_{EXP} + nT_{MUL}$. Instead, the contrast method employs $(2n+1)T_{EXP} + 3nT_{MUL} + nT_{INV} + nT_H$. Obviously, the proposed method runs more efficiently than the contrast one.

In the bidding stage, the expense of creating the auction certificate for each bidder is $1T_{EXP} + 1T_{MUL}$ in Eq. (11) and $1T_{EXP} + 2T_{MUL}$ in Eq. (12); also, the expense of assigning the signature for the bidding is $1T_{EXP} + 3T_{MUL} + 1T_H$ in Eqs. (13) and (14). Consequently, the total computation complexity for the proposed method is $3T_{EXP} + 6T_{MUL} + 1T_H$, and for the contrast one is $4T_{EXP} + 3T_{MUL} + 2T_H$. Despite double modulus multiplication operations, the former saves one time of modulus exponentiation operation and one-way hash function operation.

For the verification stage, anyone can validate the bidding information, which only costs $2T_{EXP} + 1T_{MUL} + 1T_H$ for Eqs. (15) and (16). However, the contrast method takes $2T_{EXP} + 3T_{MUL} + 1T_{INV} + 1T_H + 1T_S$.

To summarize, the proposed method forces the operating load down in the prerequisite of reasonable security, making the load and capital for the auctioneer server lower. It also significantly reduces the waiting time for the bidders to download the bidder information.

5. Conclusions

This work develops approaches that satisfy the security requirements of the English auction scheme, identifying causes or problems and providing solutions, while reducing the time complexity of bidder verification and auction setup. The proposed scheme improves bidding efficiency, and the effectiveness and convenience of the auction. The scheme proposed by this paper assumes a wired network. To free the scheme from the hardware constraints of a wired network environment, we hope to be able to expand the protocols for use on wireless communication platforms in the future, so as to bring about an electronic auction protocol that is more portable and more convenient.

Acknowledgement

This work was supported by the National Science Council, Taiwan, under Contract No. NSC 95-2221-E-029-024.

References

Chang, C.-C., Chang, Y.-F., 2003. Efficient anonymous auction protocols with freewheeling bids. Computers and Security 22 (8), 728–734.

Chida, K., Kobayashi, K., Morita, H., 2001. Efficient sealed-bid auctions for massive numbers of bidders with lump comparison. In: Proceeding of ISC 2001, pp. 408–419.

Franklin, M., Reiter, M., 1996. The design and implementation of a secure auction service. IEEE Transactions on Software Engineering 5 (22), 302–312.

Hwang, M.-S., Lu, E.-J., Lin, I.-C., 2002. Adding timestamps to the secure electronic auction protocol. Data and Knowledge Engineering 40 (2), 155–162.

Jiang, R., Pan, L., Li, J.H., 2005. An improvement on efficient anonymous auction protocols. Computers and Security 24 (2), 169–174.

Juang, W.-S., Liaw, H.-T., Lin, P.-C., Lin, C.-K., 2005. The design of a secure and fair sealed-bid auction service. Mathematical and Computer Modelling 41 (8–9), 973–985.

Kobayashi, K., Morita, H., Suzuki, K., Hakuta, M., 2001. Efficient sealed-bid auction by using one-way functions. IEICE Transactions Fundamentals E84-A (1), 289–294.

Kudo, M., 1998. Secure electronic sealed-bid auction protocol with public key cryptography. IEICE Transactions Fundamentals E81-A (1), 20–27.

Kumar, M., Feldman, S., 1998. Internet auctions. In: Proceeding of the Third USENIX Workshop on Electronic Commerce, pp. 49–60.
Lee, B., Kim, K., Ma, J., 2001. Efficient public auction with one-time registration and public verifiability. In: Proceeding of the International Conference on INDOCRYPT 2001, pp. 162–174.
Liaw, H.-T., Juang, W.-S., Lin, C.-K., 2006. An electronic online bidding auction protocol with both security and efficiency. Applied Mathematics and Computation 174 (2), 1487–1497.
Mullen, T., Wellman, M., 1998. The auction manager: market middleware for large-scale electronic commerce. In: Proceeding of the Third USENIX Workshop on Electronic Commerce, pp. 49–60.
Nguyen, K., Traore, J., 2000. An online public auction protocol protecting bidder privacy. In: Proceeding of Australasian Conference on Information Security and Privacy 2000, pp. 427–442.
Omoto, K., Miyaji, A., 2000. An anonymous auction protocol with a single non-trusted center using binary trees. In: Proceeding of Information Security Workshop 2000, pp. 108–120.
Omote, K., Miyaji, A., 2001a. An anonymous sealed-bid auction with a feature of entertainment. Transactions IPS Japan 42 (8), 2049–2056.
Omote, K., Miyaji, A., 2001b. A practical English auction with one-time registration. In: Proceeding of Australasian Conference on Information Security and Privacy 2001, pp. 221–234.
Omote, K., Miyaji, A., 2002. A practical English auction with simple revocation. IEICE Transactions Fundamentals E85-A (5), 1054–1061.
Schnorr, C.P., 1990. Efficient identification and signatures for smart cards. Advances in Cryptology: Crypto'89. In: Lecture Notes in Computer Science, 435. Springer Verlag, Berlin, pp. 339–351.
Stubblebine, S.G., Syverson, P.F., 1999. Fair on-line auction without special trusted parties. In: Proceeding of Financial Cryptography'99, pp. 230–240.
Wu, T.-C., Chen, K.-Y., Lin, Z.-Y., 2002. An English auction mechanism for Internet environment. In: Proceeding of ISC 2002, pp. 331–337.

Yu Fang Chung received a B.A. degree in English Language and Literature from Providence University, Taiwan, in 1994, an M.S. degree in CSIE from Da-Yeh University, Taiwan, in 2003, respectively, and a Ph.D. degree in the Electrical Engineering Department of National Taiwan University, Taiwan, in 2007. Her current interests focus on Information Security and Network Security.

Kuo Hsuang Huang received a B.S. and M.S. degree in Computer Science and Information Engineering, both from Da-Yeh University, Taiwan, in 2001 and 2003 respectively. He is a Ph.D. candidate in the Electrical Engineering Department of National Taiwan University. His current interests focus on information security and medical information.

Hsiu-Hui Lee received the B.S. and the M.S. degrees in electrical engineering in 1980 and 1982, respectively, and the Ph.D. degree in computer science and information engineering in 1992, all from National Taiwan University (NTU), Taipei, Taiwan.

In 1982, she was an instructor at the Department of Computer Science and Information Engineering of Tamkang University. Since 1983, she has been on the faculty and currently is an associate professor of the Department of Computer Science and Information Engineering at NTU. From August 2003 to July 2005, she also served as the Chief of the Information Management Division of the Computer & Information Networking Center at NTU and the Vice Director of the Information Systems Office of National Taiwan University Hospital. Her research interests include distributed object system, temporal database, and medical information system.

Feipei Lai received a B.S.E.E. degree from National Taiwan University in 1980, and M.S. and Ph.D. degrees in computer science from the University of Illinois at Urbana-Champaign in 1984 and 1987, respectively.

He is a professor in the Graduate Institute of Biomedical Electronics and Bioinformatics, the Department of Computer Science & Information Engineering and the Department of Electrical Engineering at National Taiwan University. He is a vice superintendent of National Taiwan University Hospital. He is the chairman of Taiwan Network Information Center. He was a visiting professor in the Department of Computer Science and Engineering at the University of Minnesota, Minneapolis, USA. He was also a guest Professor at University of Dortmund, Germany and a visiting senior computer system engineer in the Center for Supercomputing Research and Development at the University of Illinois at Urbana-Champaign. Dr. Lai holds 6 Taiwan patents and 3 USA patents currently. His current research interests are SOC low power computing, Medical Information System.

He is one of the founders of the Institute of Information & Computing Machinery. He is also a member of Phi Kappa Phi, Phi Tau Phi, ACM, Chinese Institute of Engineers. He is the chairman of Taiwan Internet Content Rating Foundation. He received the Taiwan Fuji Xerox Research award in 1991. He is a senior member of IEEE and included in "Who's Who in Science and Engineering" and "Who's Who in the World."

Tzer Shyong Chen received a B.S. degree in Computer and Information Science from Tunghai University, Taiwan, in 1989, an M.S. degree in Computer and Information Science from National Chiao-Tung University, Taiwan, in 1991, and a PhD. degree in Electrical Engineering Department from National Taiwan University in 1996. Currently, he is a professor in the Department of Information Management at Tunghai University, Taiwan. His current research interests focus on Information Security, Cryptography, and Network Security.